SyncServer® S6x0 Release 5.0 User Guide

Introduction

This user guide describes the installation and configuration processes of SyncServer® S600/S650 v5.0.

SyncServer® S600

The Microchip SyncServer S600 provides accurate, secure, and reliable time services that are required by all modern networks. 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 that meet needs of your network and business operations.

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 eight BNC connectors comes standard with the most popular timing I/O signals (IRIG B, 10 MHz, 1 PPS, and so on). When more flexibility is required, the unique Microchip FlexPort™ technology option enables six of the BNCs to output any supported signal (time codes, sine waves, programmable rates, and so on), all configurable in real time through 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 also. 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 without degradation in the precise quality of the coherent signals.

SyncServer® S650i

The Microchip SyncServer S650i is a S650 base chassis without a GNSS receiver.

Table of Contents

1. Overview

This section provides the SyncServer features, physical and functional descriptions, and the configuration options using key Keypad interface, Web interface, or Command Line interface.

1.1 SyncServer S6x0 Key Features

- < 15 ns 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, 10 MHz, 1 PPS, and so on) available for S650.
- Four GbE ports standard with NTP hardware time stamping
- Ultra-high bandwidth NTP time server
- Stratum 1 operation through GNSS satellites
- DoS detection/protection (optional)
- Web-Based management with high security cipher suite.
- BlueSky™ Jamming/Spoofing protection
- TACACS+, RADIUS, LDAP, and more (optional)
- –20 ℃ to 65 ℃ 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

1.1.1 Software Options

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

- **Security Protocol License Option**: SyncServer S600/S650 can be seriously hardened from both an NTP perspective and an authentication perspective through this option. This license option includes the following.
  - NTP Reflector
  - High capacity and accuracy
  - Per port packet monitoring and limiting
- **FlexPort Timing License Option**: The FlexPort technology option enables the six 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 two 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 Server Output License Option**: This option enables PTP default profile, PTP Enterprise profile and PTP Telecom-2008 profile server functionality.
- **PTP Client License**: This option enables PTP client operations to be configured on an Ethernet port.

- **1 PPS TI Measurement License**: This license enables 1 PPS 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 and spoofing detection, protection, and analysis features.

See 7.7. 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 through LAN1 port to gain access to the licensed software options web page.

1.1.2 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 S6x0 while remaining services can be disabled. Advanced authentication services, such as TACACS+, RADIUS, and LDAP are optionally available.

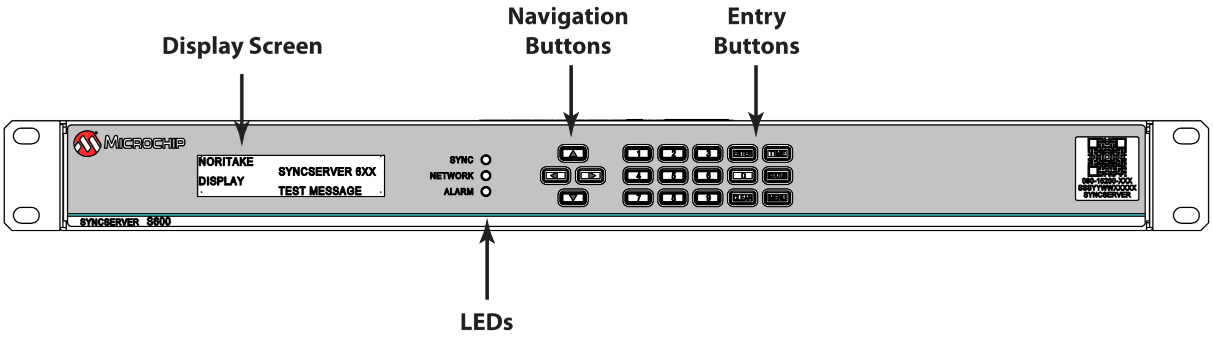
The combined four standard GbE ports and the two optional 10 GbE ports easily handle more than 10,000 NTP requests per second using hardware time stamping and compensation (360,000 is maximum capacity for NTP reflector, 13,000 is maximum capacity for NTPd). All traffic to the S6x0 CPU is bandwidth-limited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

1.2 Physical Description

SyncServer S6x0 consists of a 19-inch (48 cm) rack-mountable chassis, plug-in modules (S650 only), and hardware. All connections for SyncServer S6x0 are on the rear panel.

The following figure shows a front view of the SyncServer S600 version with LEDs, display screen, navigation buttons, and entry buttons.

Figure 1-1. SyncServer S600 Front Panel



The following figures show the single AC versions of SyncServer S600.

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

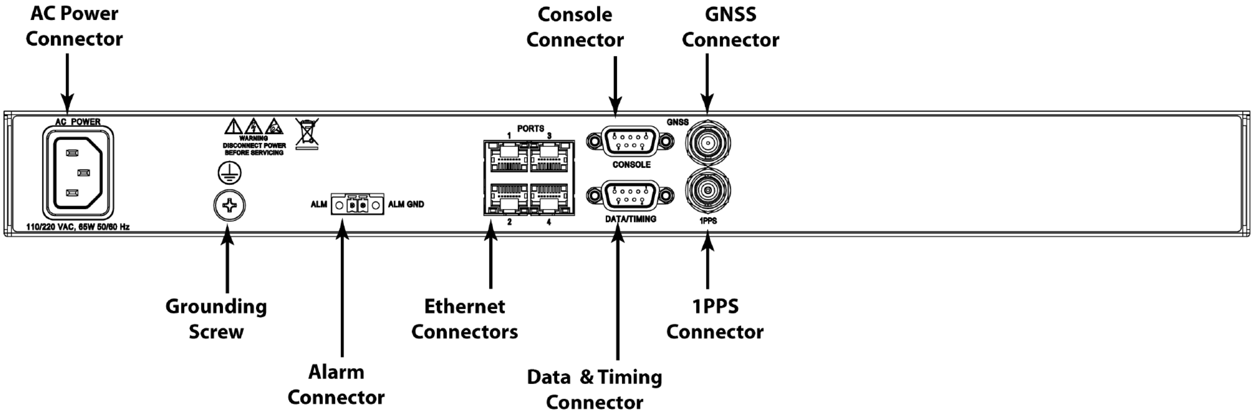
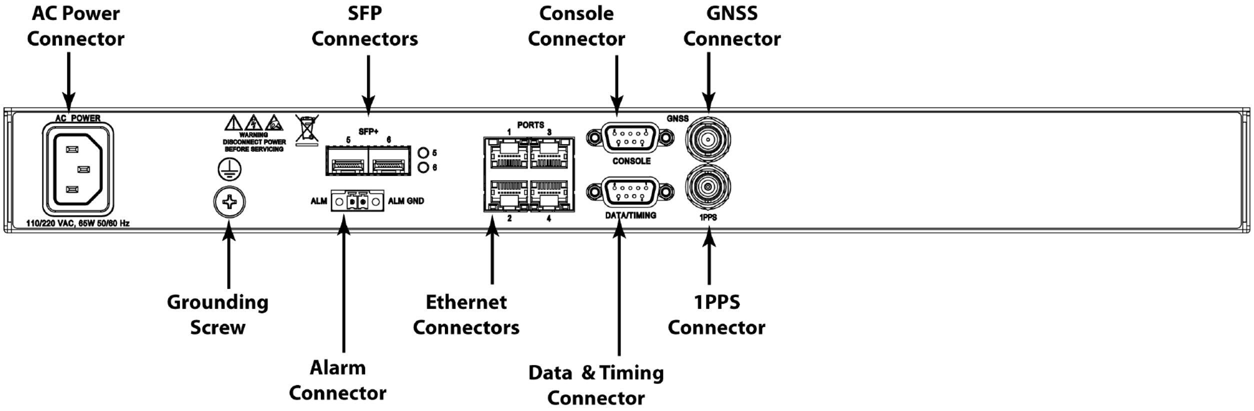


Figure 1-3. SyncServer S600 Rear Panel—Single AC Version with 10 GbE



The following figures show rear panel connections for the dual AC versions of SyncServer S600.

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

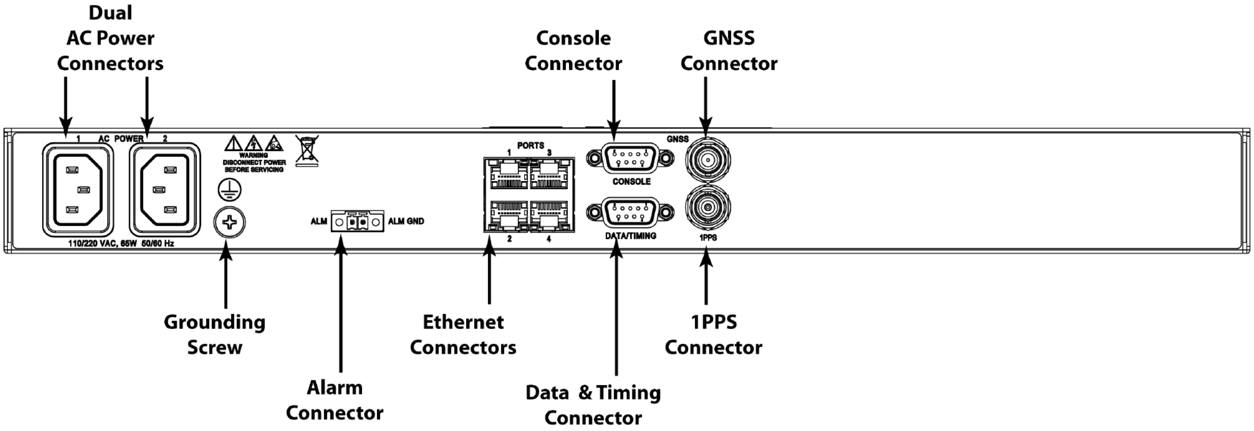
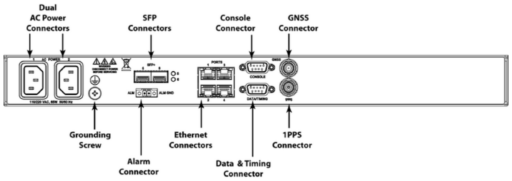


Figure 1-5. SyncServer S600 Rear Panel—Dual AC Version with 10 GbE



The following figures show rear panel connections for the dual DC versions of SyncServer S600.

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

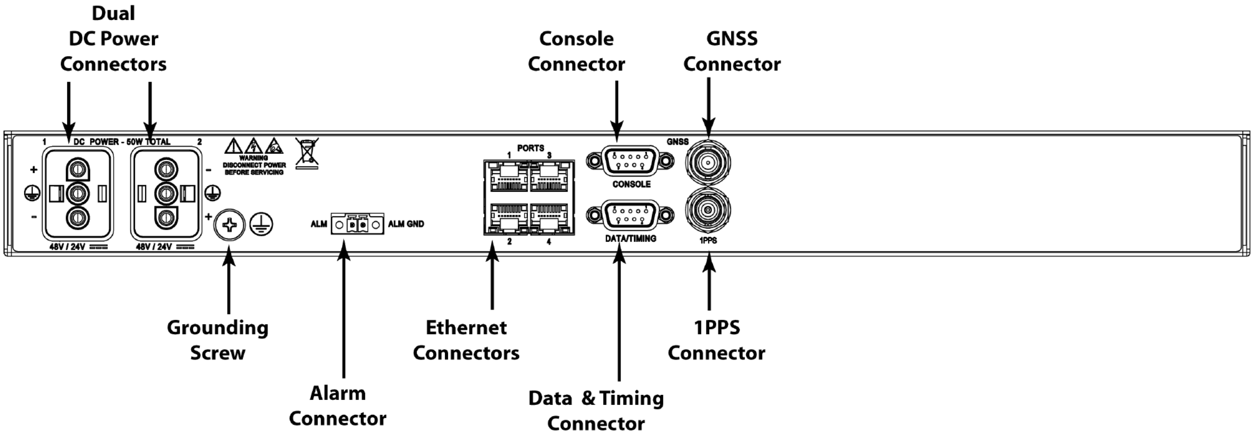
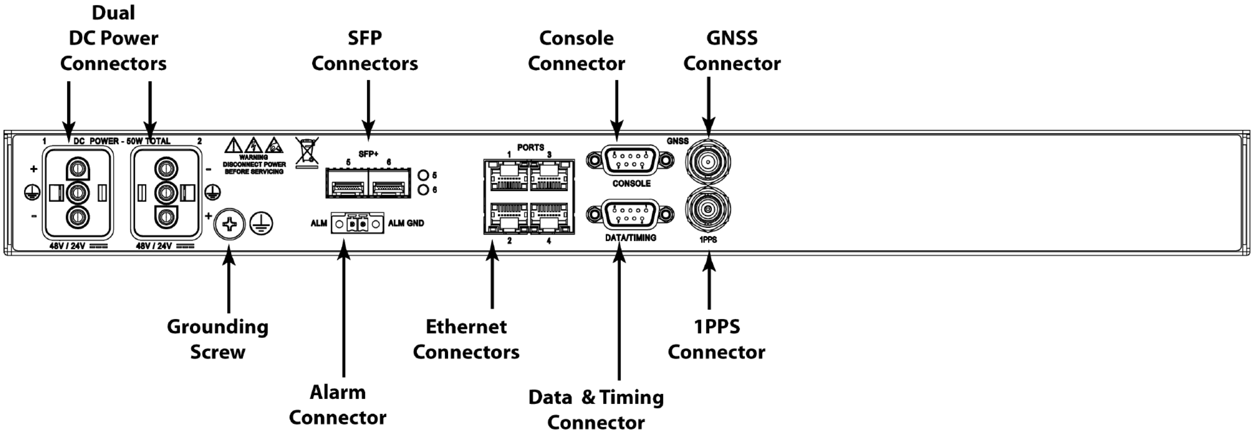
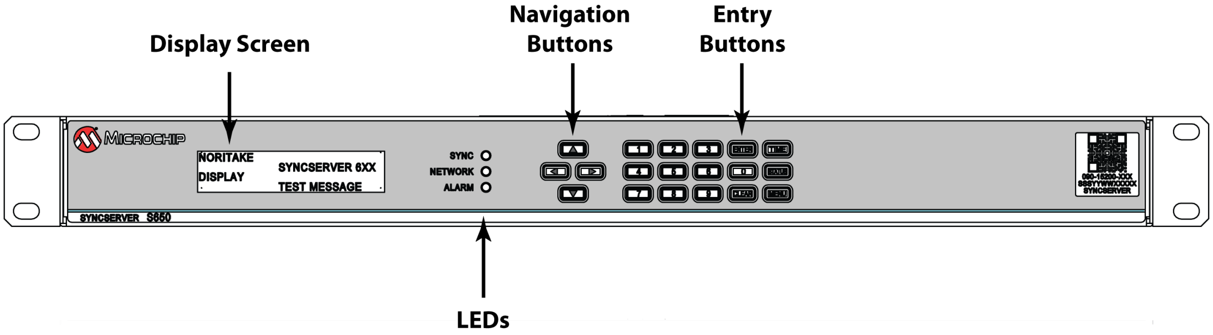


Figure 1-7. SyncServer S600 Rear Panel—Dual DC Version with 10 GbE



The following figure shows front view of SyncServer S650 version with LEDs, display screen, navigation buttons, and entry buttons.

Figure 1-8. SyncServer S650 Front Panel



The following figures show rear panel connections for the single AC versions of SyncServer S650.

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

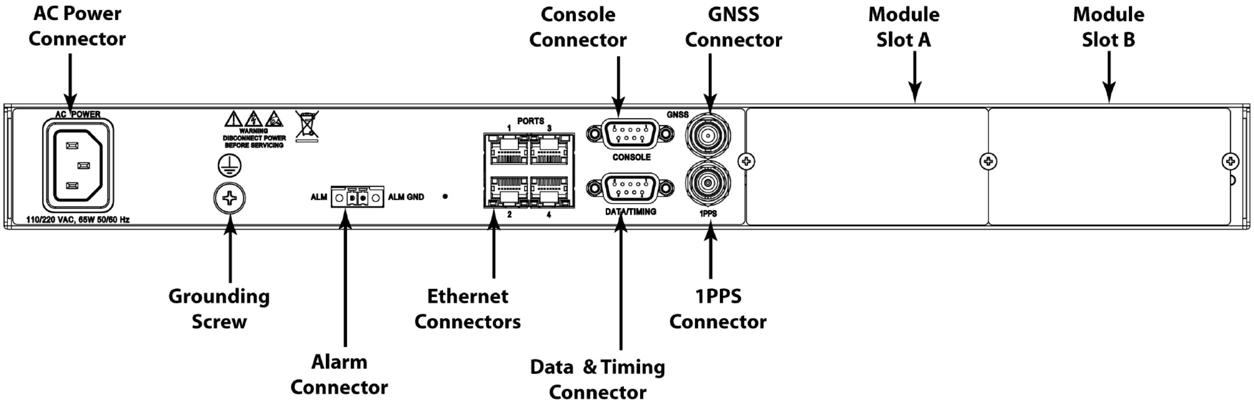
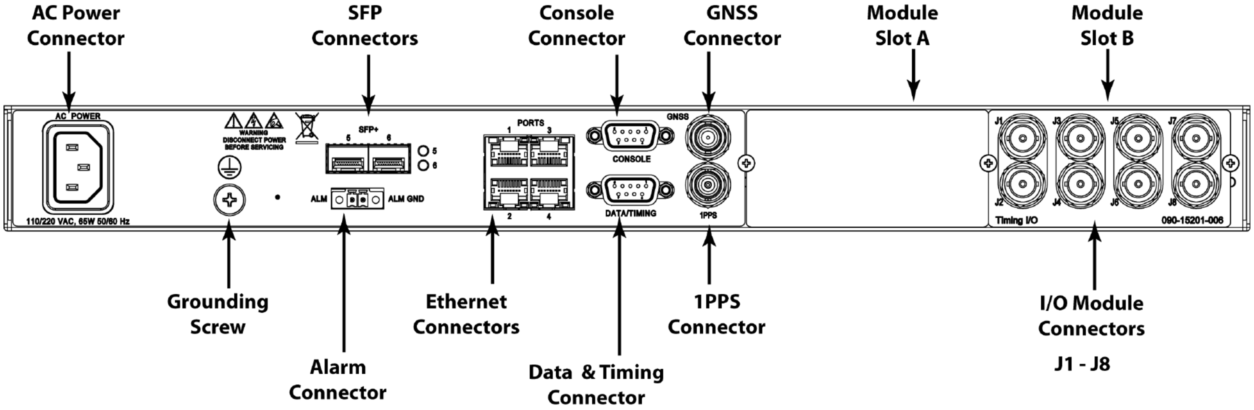


Figure 1-10. SyncServer S650 Rear Panel—Single AC Version with 10 GbE and a Timing I/O Module



The following figures show rear panel connections for the dual AC versions of SyncServer S650.

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

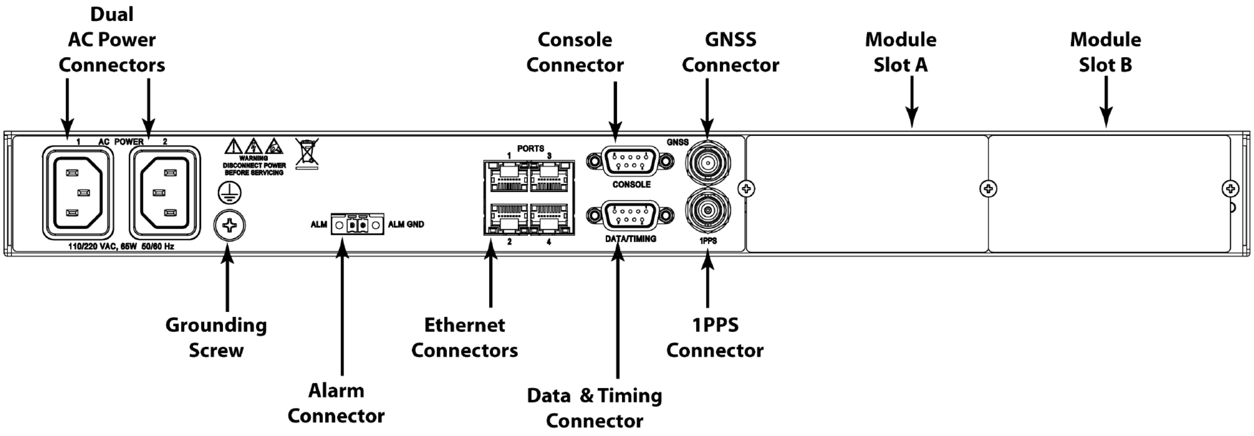
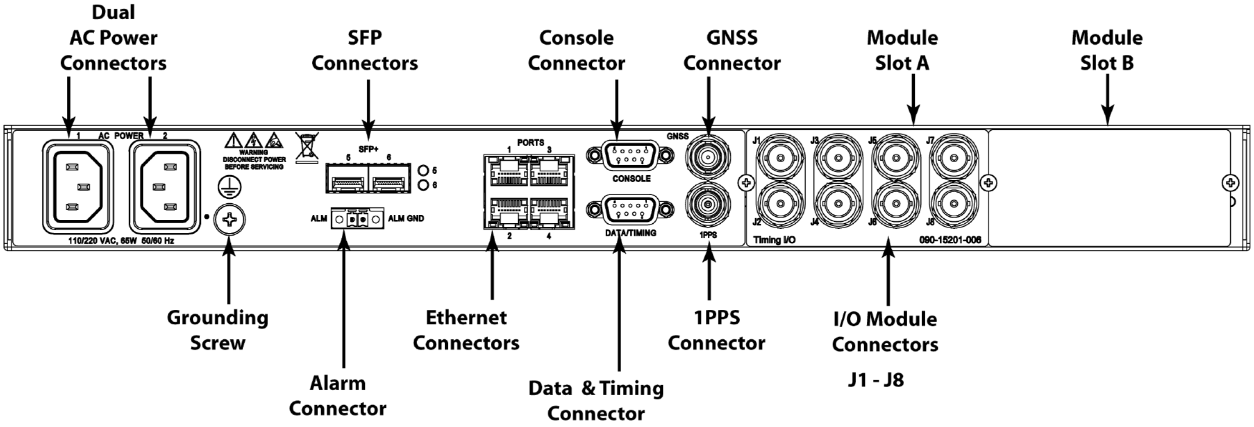


Figure 1-12. SyncServer S650 Rear Panel—Dual AC Version with 10 GbE and a Timing I/O Module



The following figures show rear panel connections for the Dual DC versions of SyncServer S650.

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

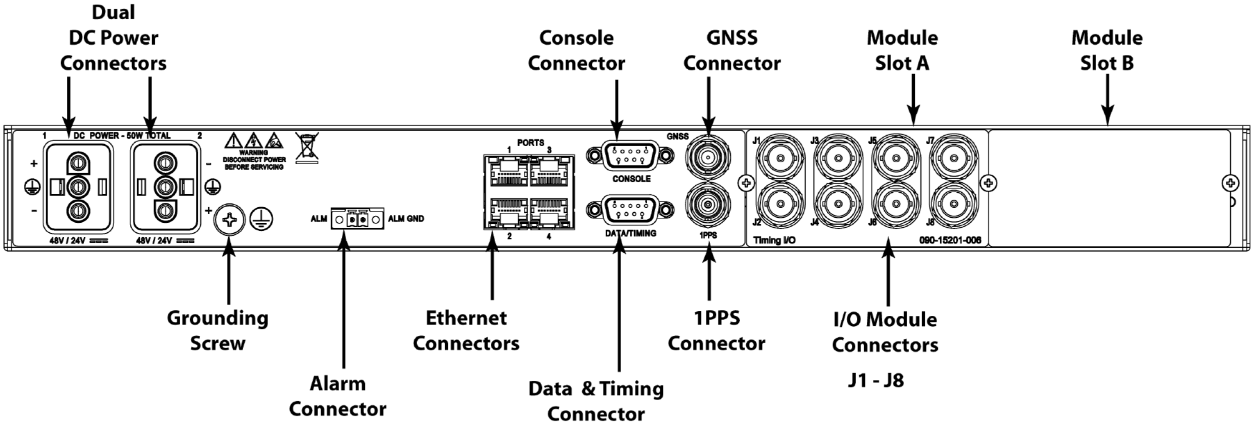
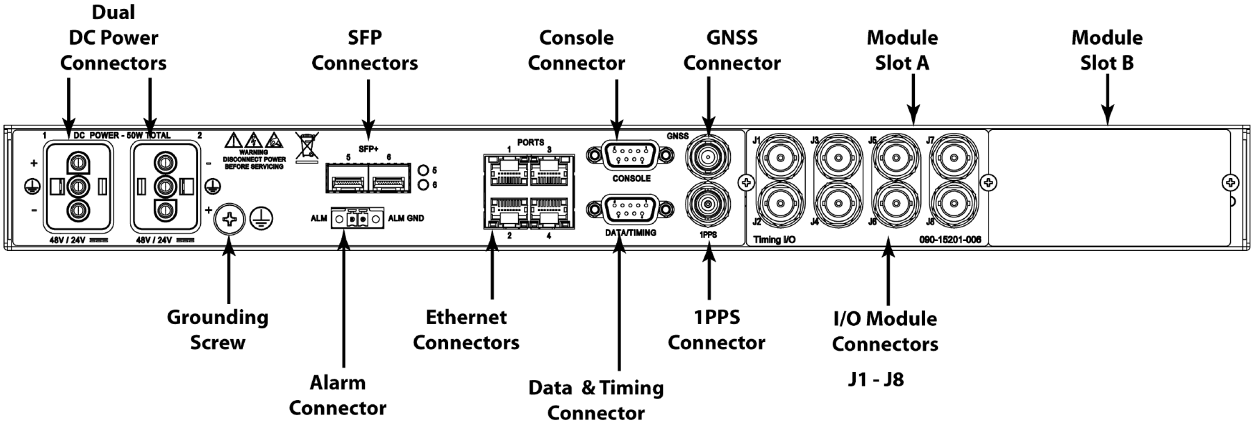
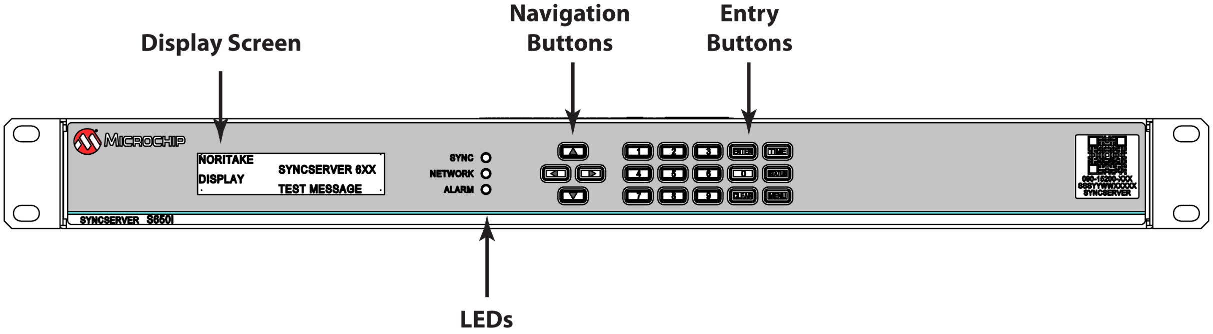


Figure 1-14. SyncServer S650 Rear Panel—Dual DC Version with 10 GbE and a Timing I/O Module



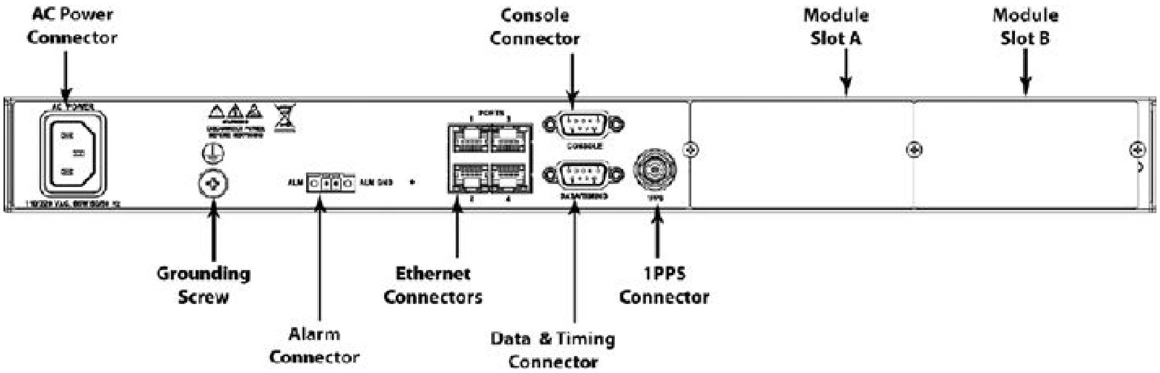
The following figure shows front view of SyncServer S650 version with LEDs, display screen, navigation buttons, and entry buttons.

Figure 1-15. SyncServer S650i Front Panel



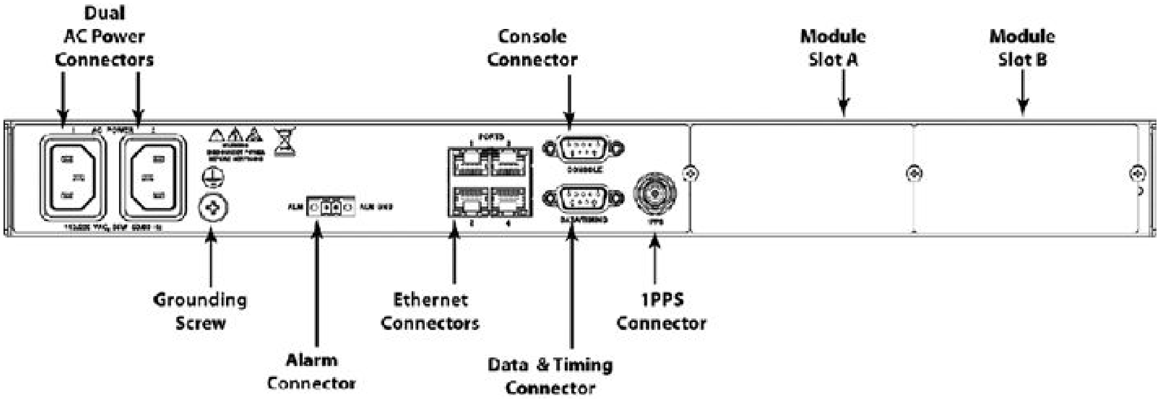
The following figure shows rear panel connections for the single AC version of SyncServer S650i.

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



The following figure shows rear panel connections for the dual AC version of SyncServer S650i.

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



1.2.1 Communications Connections

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

1.2.1.1 Ethernet Management Port—LAN1

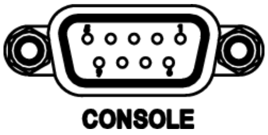
Ethernet port 1 is the management port that is used to access the web interface. This port is located on the rear panel of SyncServer S6x0 and is a standard 100/1000 Base-T shielded RJ45 receptacle. To connect SyncServer S6x0 to an Ethernet network, use a standard twisted-pair Ethernet RJ45 cable (CAT5 minimum). Configurable to 100_Full or 1000_Full or Auto: 100_Full/1000_Full.

1.2.1.2 Serial Console Port

The serial port connection is made through a DB-9 female connector on the rear panel of 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 and Response mode). The following figure shows the DB-9 female connector for the serial port.

Figure 1-18. Serial Port Connector

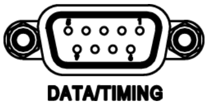


1.2.2 Output Connections

1.2.2.1 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 figure. 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.

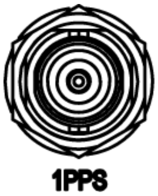
Figure 1-19. Serial Data/Timing Connection



1.2.2.2 1 PPS Output Connection

The following figure shows the SyncServer S6x0 providing a BNC female.

Figure 1-20. 1 PPS Output Connection

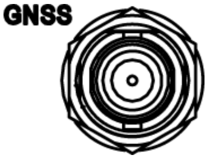


1.2.3 Input Connections

1.2.3.1 GNSS Connection

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 section 10.1. Antenna Kits Overview, Installing GNSS Antennas). This connector is not present on SyncServer S650i.

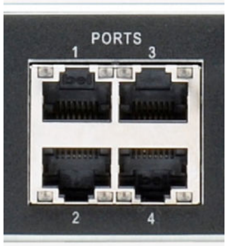
Figure 1-21. GNSS Input Connection



1.2.3.2 NTP Input/Output Connections

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 section 12. Port Details for information on Ethernet port isolation and management port rules.

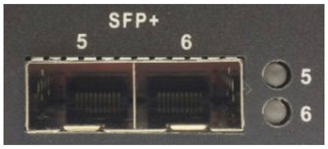
Figure 1-22. NTP Input/Output Connections



1.2.3.3 10 GbE Input/Output Connections

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

Figure 1-23. 10 GbE Input/Output Connections



1.2.4 Alarm Relay

SyncServer S6x0 features a Phoenix connector for an alarm relay output, as shown in the following figure. Figure 1-25 shows that the relay is open when the configured alarm classes occur. If SyncServer S6x0 is not powered, then the alarm relay is open. The relay is energized (shorted), when 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

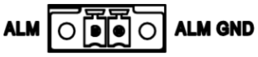
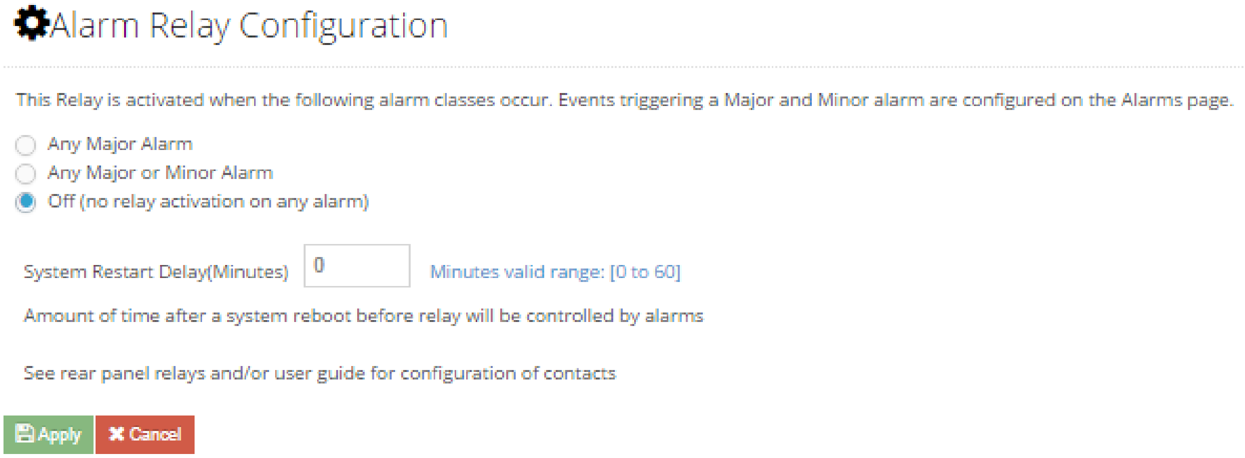


Figure 1-25. Alarm Relay Configuration Web GUI



Alarm Relay Configuration

This Relay is activated when the following alarm classes occur. Events triggering a Major and Minor alarm are configured on the Alarms page.

○ Any Major Alarm
○ Any Major or Minor Alarm
● Off (no relay activation on any alarm)

System Restart Delay(Minutes) 0 Minutes valid range: [0 to 60]

Amount of time after a system reboot before relay will be controlled by alarms

See rear panel relays and/or user guide for configuration of contacts

1.2.5 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 Figure 1-26). 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 1 PPS or IRIG B AM-In, 10 MHz-In, IRIG AM and IRIG DCLS-Out, and 1 PPS-Out and 10 MHz-Out.

The FlexPort technology option enables the six 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. Similarly, the two 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.

Figure 1-27 shows signal types for the standard configuration and the configuration with the FlexPort option.

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

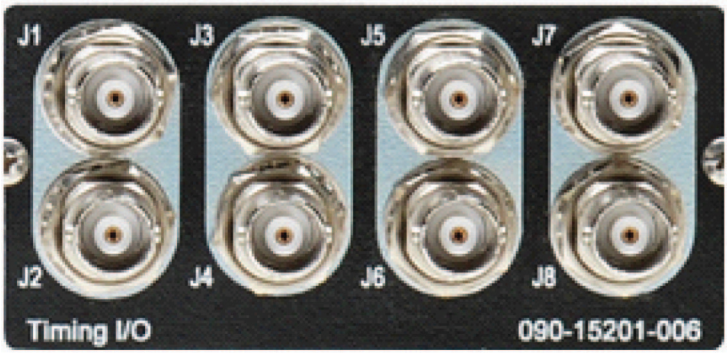
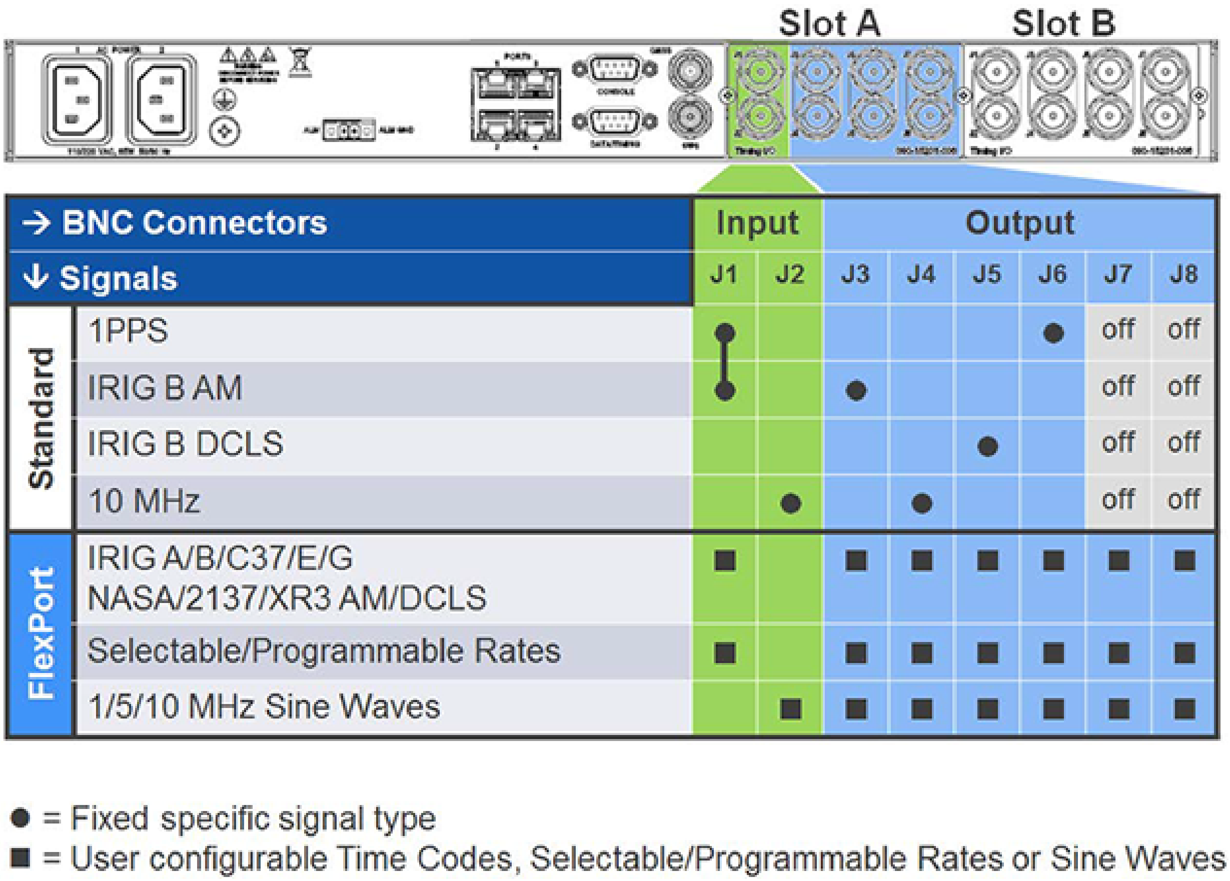


Figure 1-27. Signal Types for Timing I/O Module


Slot A
Slot B

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

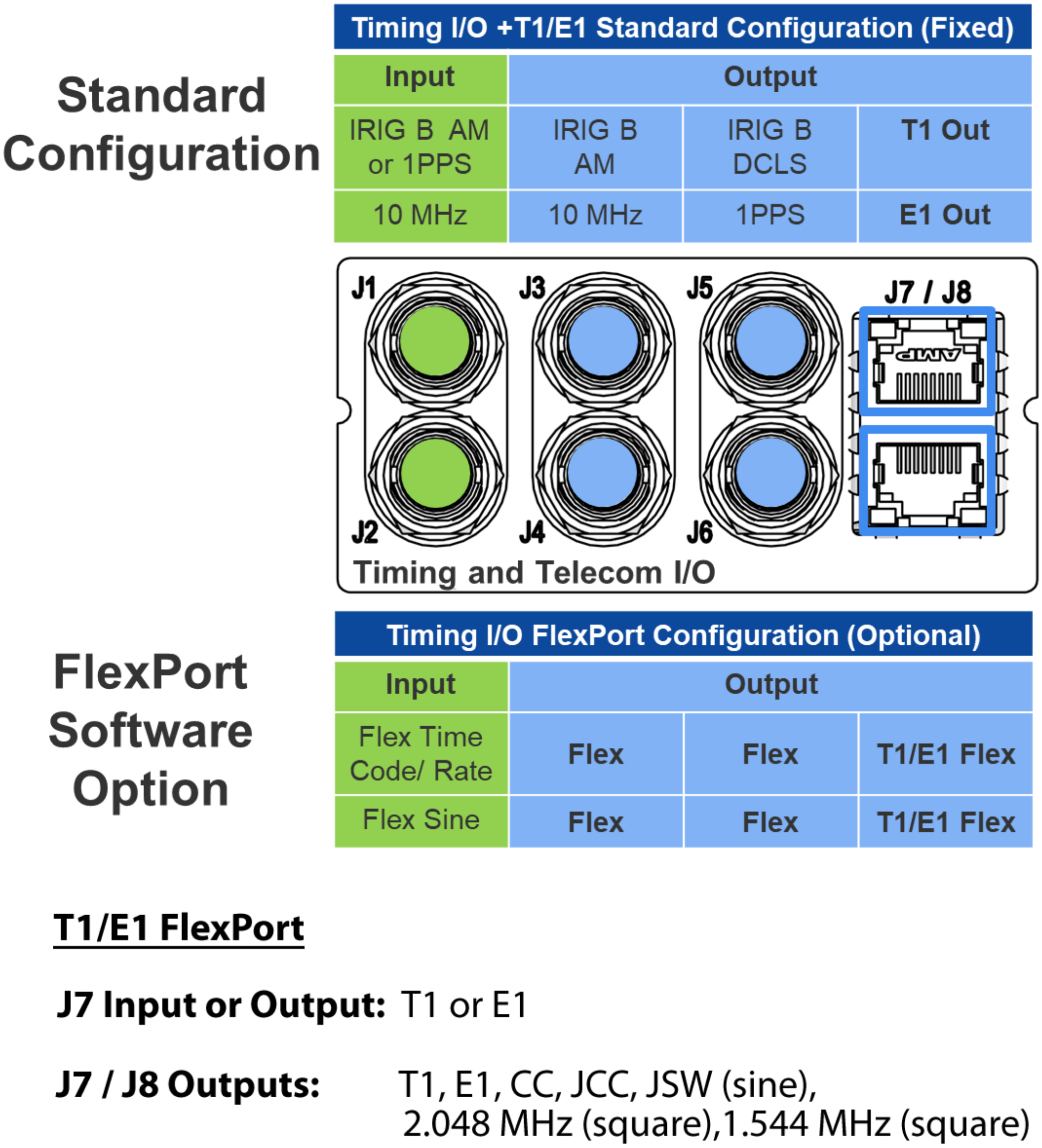
● = Fixed specific signal type
■ = User configurable Time Codes, Selectable/Programmable Rates or Sine Waves

1.2.5.1 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 following figure. The standard configuration for the RJ48c ports is J7 = T1 Output and J8 = E1 Output.

The following figure shows that the ports are individually configurable for the signal formats, 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



Standard Configuration

Timing I/O +T1/E1 Standard Configuration (Fixed)

Input	Output		
IRIG B AM or 1PPS	IRIG B AM	IRIG B DCLS	T1 Out
10 MHz	10 MHz	1PPS	E1 Out

FlexPort Software Option

Timing I/O FlexPort Configuration (Optional)

Input	Output		
Flex Time Code/ Rate	Flex	Flex	T1/E1 Flex
Flex Sine	Flex	Flex	T1/E1 Flex

T1/E1 FlexPort

J7 Input or Output: T1 or E1

J7 / J8 Outputs: T1, E1, CC, JCC, JSW (sine),
2.048 MHz (square),1.544 MHz (square)

Ports J1–J6 have identical functionality to the basic Timing I/O module. See Figure 1-27 for details about configuration choices.

Table 1-1. J7 and J8 Connector Pin Assignments—Timing I/O Module with Telecom I/O Connections

Pin	Signal
1	Rx ring (not supported on J8)

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

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

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

The Timing I/O with HaveQuick/PTTI module (090-15201-012) adds support to 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 is pre-installed on a system containing a HaveQuick/PTTI module.

For details on HaveQuick input support on J1 and J2, see 6.4.5. Provisioning HaveQuick Input on Timing I/O HaveQuick/PTTI Module.

For details on HaveQuick output support on J3 through J8, see 6.8.11. Provisioning Outputs on Timing I/O HaveQuick/PTTI Module.

Figure 1-29. HaveQuick/PTTI Module Connections

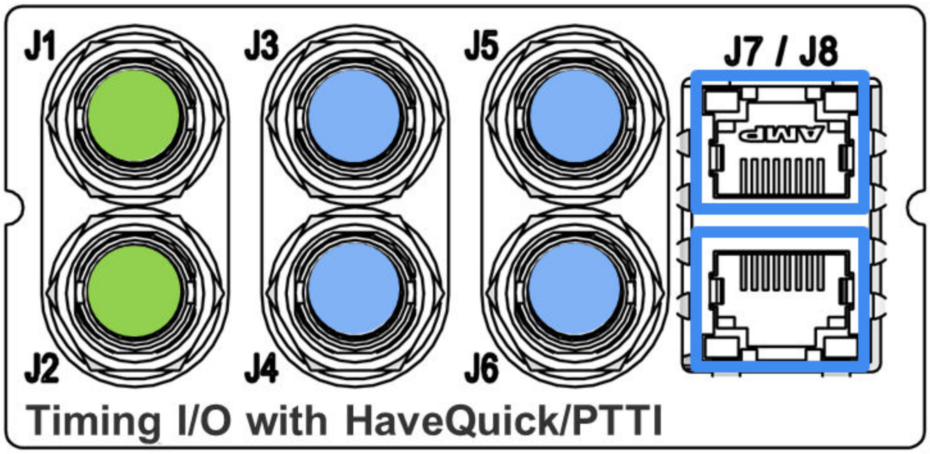


Table 1-2. HaveQuick/PTTI Module Port Descriptions

Port	Description
J1	Input same as Timing I/O module with FlexPort functionality always On, Supports TTL and 5V HaveQuick Input.

...........continued	
Port	Description
J2	Input same as Timing I/O module with FlexPort functionality always On, used for 1 PPS 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 RJ48.
J8	RS422 PTTI Output on RJ48.

Table 1-3. J7 and 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	1 PPS/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

1.2.5.2.1 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

1.2.5.2.2 PTTI Binary Coded Decimal (BCD)

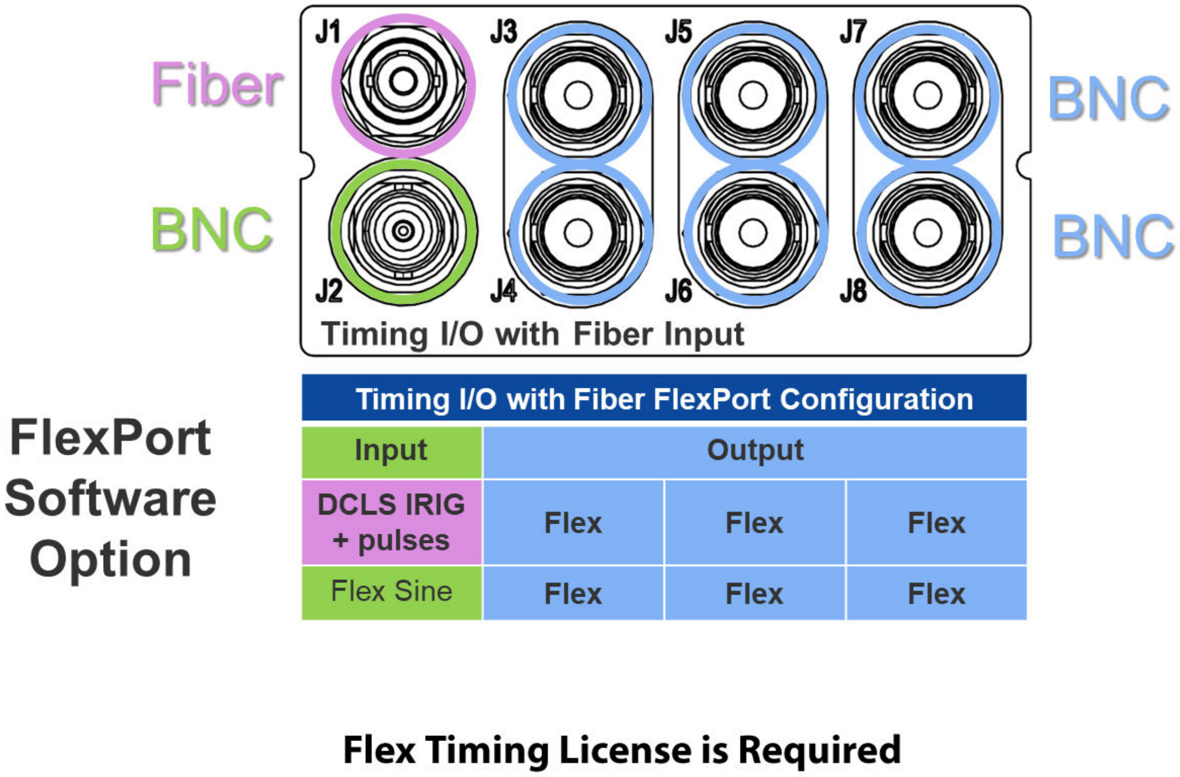
The following formats are supported:

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

1.2.5.3 Timing I/O Modules with Fiber Connectors

There are two variations on the Timing I/O module with fiber connectors. The 090-15201-013 model has three output BNC multimode fiber connectors: J3, J5, and J7. The 090-15201-014 model has a single multimode fiber connector: the J1 input.

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

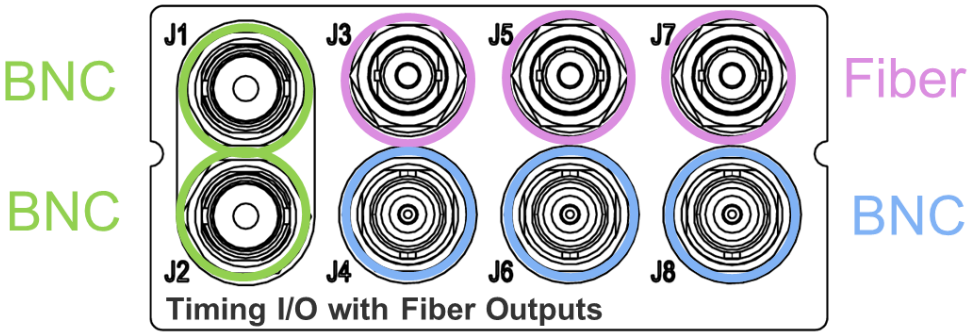


FlexPort Software Option

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

1.2.5.4 Low Phase Noise Module Connections

The module has eight 10 MHz Low Phase Noise (LPN) outputs (J1–J8). Two different LPN modules are available with different performance specifications.

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

Figure 1-32. LPN Module Connections

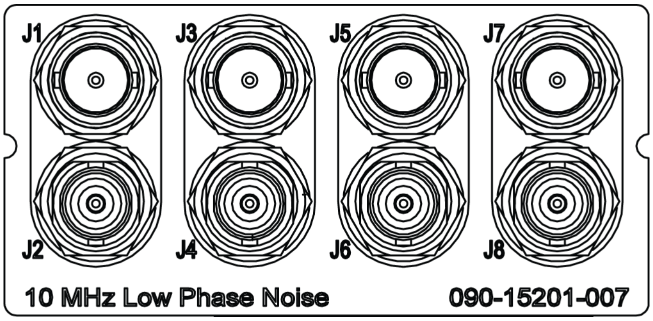
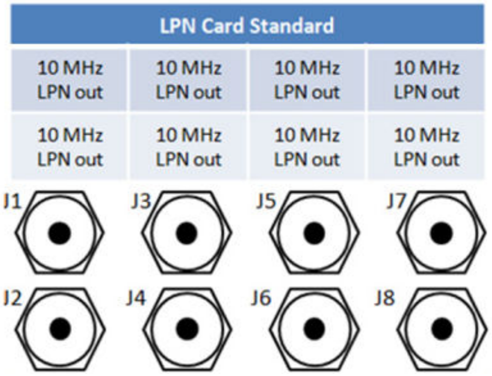


Figure 1-33. LPN Module Signal Types



LPN Card Standard			
10 MHz LPN out	10 MHz LPN out	10 MHz LPN out	10 MHz LPN out
10 MHz LPN out	10 MHz LPN out	10 MHz LPN out	10 MHz LPN out

1.2.6 Power and Ground Connections

SyncServer S6x0 is available with either single or dual 120/240 VAC power, or dual DC power. SyncServer S6x0 is not equipped with a Power switch. AC power is controlled by the unplugging the AC power cord. Frame ground connections on SyncServer S6x0 are made on the grounding stud located on the left side of the rear panel, as identified with the international Ground marking, shown in Figure 1-34 and Figure 1-35.

⚠ **CAUTION** 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

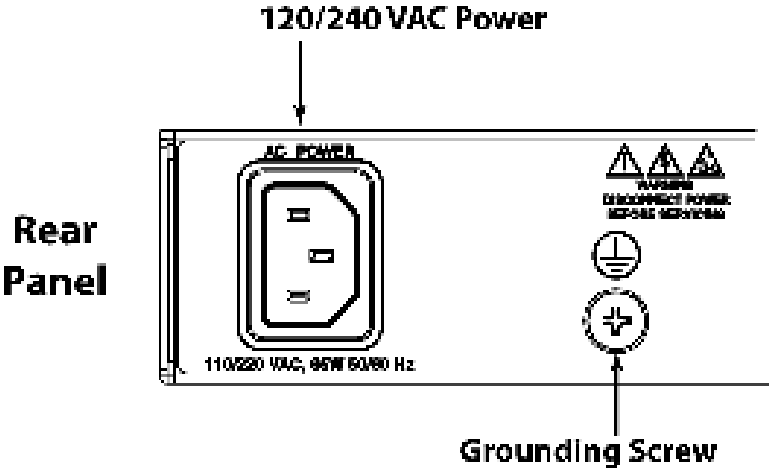


Figure 1-35. SyncServer S6x0 Dual AC Version Power and Ground

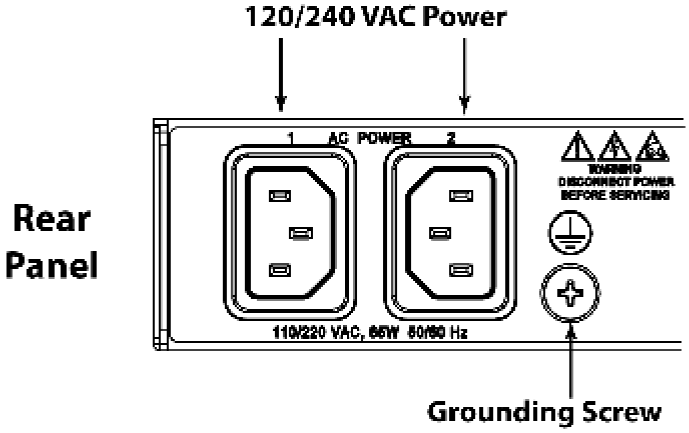
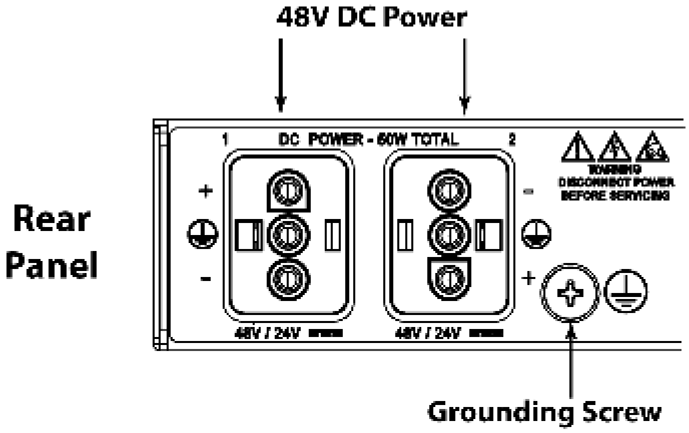


Figure 1-36. SyncServer S6x0 Dual DC Version Power and Ground



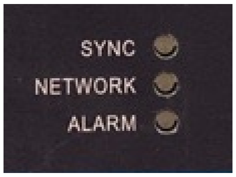
1.3 Functional Description

1.3.1 LEDs

The following figure shows three LEDs provided by SyncServer S6x0 on the front panel that indicate the following:

- Sync status
- Network status
- Alarm status

Figure 1-37. LEDs for SyncServer S6x0



See Table 2-5 for details about the LEDs.

1.3.2 Communication Ports

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

1.3.2.1 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.

1.3.2.2 Local Console Serial Port

The serial port supports very limited local control; you can configure 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

1.3.3 Time Inputs

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 RJ45 (2–4). The IRIG signal uses a BNC connector (J1) on the optional Timing I/O module on the rear panel, as listed in Table 1-4.

1.3.4 Frequency Inputs

SyncServer S6x0 can use either 1 PPS, 10 MPPS, 10 MHz, 5 MHz, or 1 MHz as external frequency input references. The 1 PPS/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 listed in Table 1-4.

1.3.5 Frequency and Timing Outputs

SyncServer S6x0 can provide NTP, 10/5/1 MHz, 1 PPS, 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 1 PPS output is also available using a BNC connector (1 PPS) 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 1 PPS	10 MHz	IRIG B AM 124	10 MHz	IRIG B B004 DCLS	1 PPS	off	off
FlexPort option	A000/A004/A130/A134B000/B001/B002/B003B004/B005/B006/B007B120/B121/B122/B123B124/B125/B126/B127E115/E125C37.118.1a-2014IEEE-1344 Rates:1 PPS 10 MPPS	1 MHz 5 MHz 10 MHz	Pulse: Fixed rate—10/5/1MPPS, 100/10/1kPPS, 100/10/1/0.5 PPS, 1 PPM, 1 PPS falling edge. Programmable period: 100 ns to 86400s, 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: 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 is always zero, and the encoded IRIG time is UTC (if using an input 1344 IRIG as the reference the 2014 rules are applied to get that value). Therefore, any code receiving S6x0 IRIG 1344 output must work regardless of which version they are decoding (as there is nothing to add or subtract).

1.4 Configuration Management

SyncServer S6x0 can be configured using the Keypad interface, Web interface, or Command Line interface.

1.4.1 Keypad/Display Interface

The Keypad/Display interface displays time and system status. It performs the following functions:

- Configures and enables/disables the LAN1 network port
- Sets the time and enters Freerun mode
- Adjusts the brightness
- Locks the keypad
- Shuts SyncServer

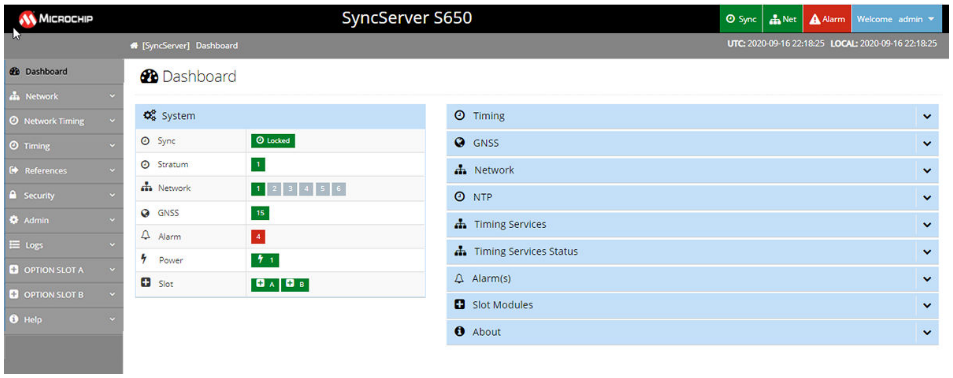
1.4.2 Web Interface

SyncServer S6x0 also allows the user to access information through 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 SyncServer S6x0, when prompted.

1.4.2.1 Dashboard View

The following figure shows an example of the dashboard status screen.

Figure 1-38. Web Interface—Dashboard



SyncServer S650

[SyncServer] Dashboard

UTC: 2020-09-16 22:18:25 LOCAL: 2020-09-16 22:18:25

Dashboard

System	
Sync	Locked
Stratum	1
Network	1 2 3 4 5 6
GNSS	15
Alarm	4
Power	1
Slot	A B

1.4.3 Command Line Interface

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

Note: Before communication with SyncServer S6x0 through an Ethernet connection, you must first configure the Ethernet port using the serial connection or front panel. For details, see 6.3. Provisioning the Ethernet Ports.

1.5 Alarms

SyncServer S6x0 uses alarms to notify 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, Web GUI status, CLI status, alarm connector (configurable), SNMP trap (configurable), message log (configurable), and email (configurable). For details, see 6.10. Provisioning Alarms and 8. System Messages.

2. Installing

This section describes the procedures for installing SyncServer S6x0.

2.1 Getting Started

If you encounter any difficulties during the installation process, contact Microchip Frequency and Time Systems (FTS) Services and Support. See 16. Technical Support for telephone numbers. Contact Microchip FTS Services and Support for technical information and Customer Service for information about your order, RMAs, and other information.

2.1.1 Security Considerations for SyncServer S6x0 Installation

SyncServer S6x0 must be installed in a physically secure and restricted location.

When possible, SyncServer S6x0's Ethernet ports must be installed behind the company's firewall to prevent public access.

2.1.2 Site Survey

SyncServer S6x0 can be installed in a variety of locations.

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

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

SyncServer S6x0 is installed into a rack. The AC power connection must be made to a 120 or 240 VAC power receptacle of following local codes and requirements. An external Surge Protective Device must be used with the AC version of 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 wh while installing SyncServer S6x0. Electromagnetic interference can adversely affect the operation of nearby equipment.

2.1.3 Installation Tools and Equipment

The following tools and equipment are required to install SyncServer S6x0:

- Standard tool kit
- Cable ties, waxed string, or acceptable cable clamps
- 1 mm²/16 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

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

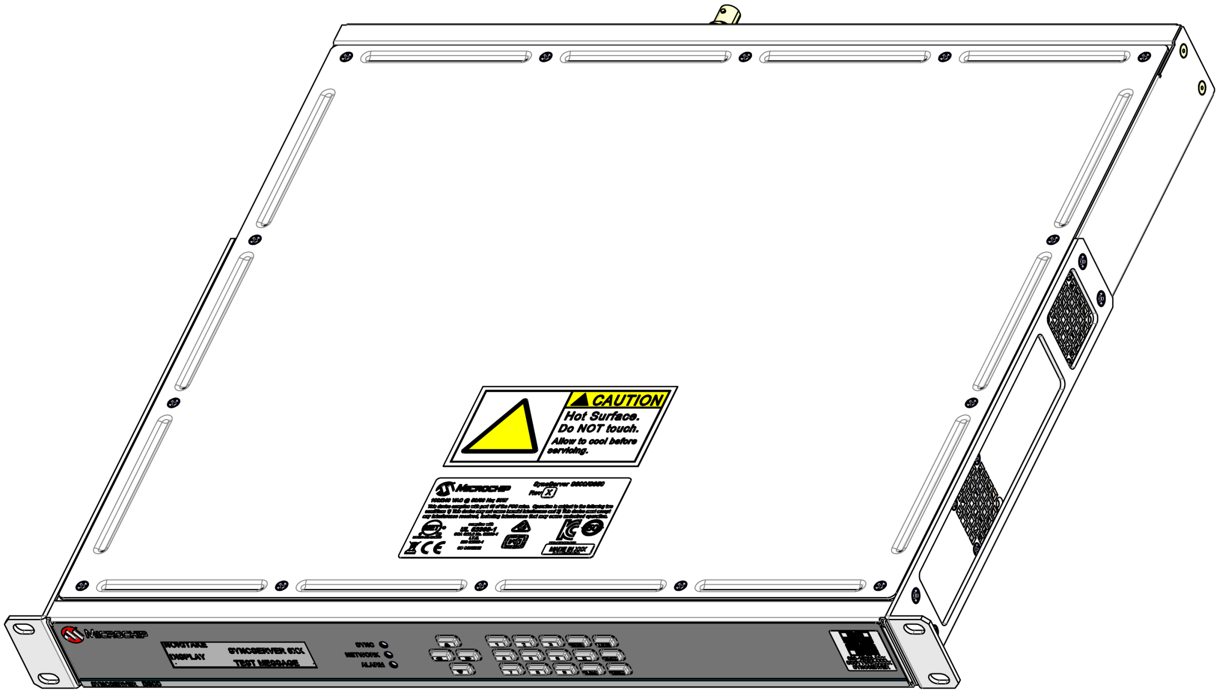
Note: To avoid ESD damage to parts that are packaged with SyncServer S6x0, observe the following procedures.

Perform the following steps to unpack and inspect the unit:

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. Be 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 matches the model and item number on the equipment. The item number can be found on a label affixed to the top of the unit. The following figure shows the location of the label on SyncServer S6x0. Contact your Microchip distributor if the model or item number do not match.

For a complete list 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

This section provides general guidelines for installing 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 Figure 2-3. Use the proper screws for the equipment rack.

Figure 2-2. Dimensions for SyncServer S6x0

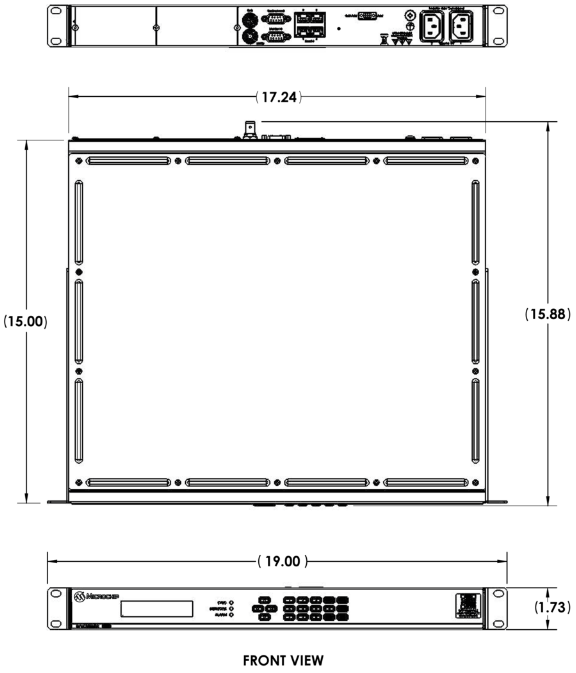
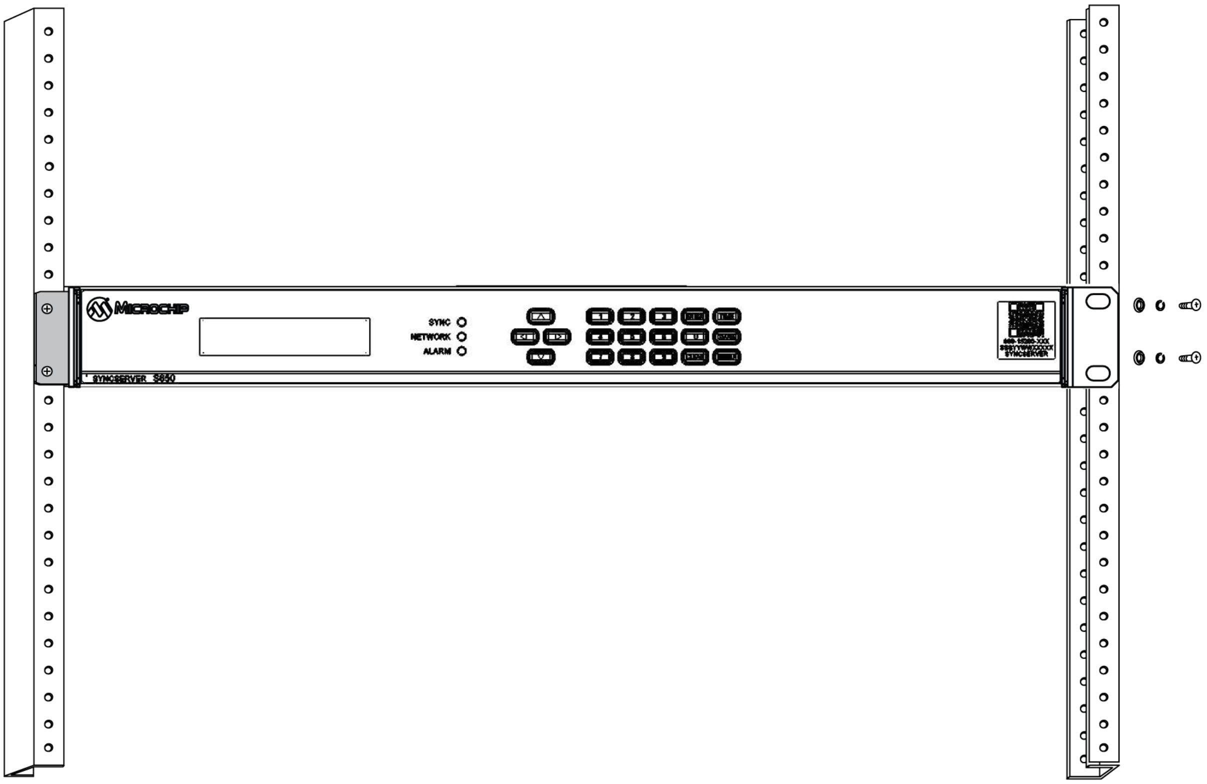


Figure 2-3. Rack Mounting the SyncServer S6x0



2.4 Making Ground and Power Connections

Depending on the specific model, SyncServer S6x0 has either one or two 120/240 VAC connectors, which are located on the left side of the rear panel, as shown in Figure 2-4 and Figure 2-5.

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 Figure 2-6. This screw is located on the left side of the rear panel for all SyncServer S6x0 models, as shown in Figure 2-4 and Figure 2-5.

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

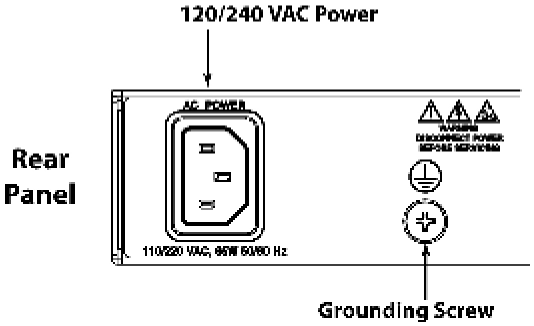

120/240 VAC Power
Rear Panel
AC POWER
WARNING DISCONNECT POWER BEFORE SERVICING
110/220 VAC, 65W 50/60 Hz
Grounding Screw

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

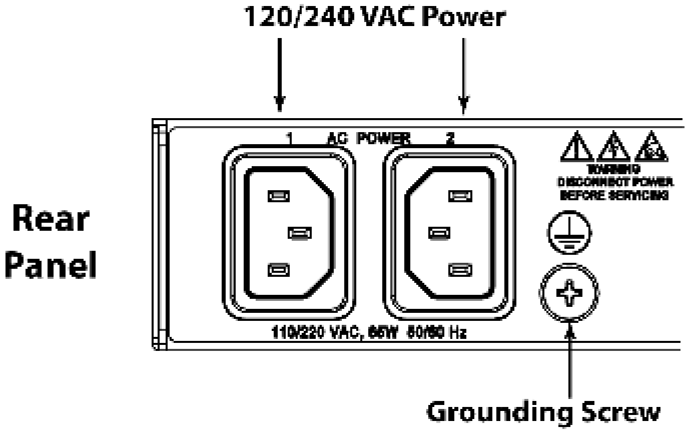
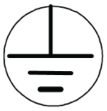

120/240 VAC Power
Rear Panel
1 AC POWER 2
WARNING DISCONNECT POWER BEFORE SERVICING
110/220 VAC, 65W 50/60 Hz
Grounding Screw

Figure 2-6. Universal Ground Symbol



After installing 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 SyncServer S6x0 grounding lug to the earth Ground on the rack. The following steps show the rack grounding method.

Note: Out of many 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 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 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. Following is the suggested method:
    1. Crimp the appropriate customer-supplied UL listed Ring lug to the other end of the 1 mm²/16 AWG green/yellow-striped wire.
    2. Remove the paint and sand the area around the screw hole to ensure the proper conductivity.
    3. Coat the connection with an electrically conductive antioxidant compound, such as Kopr-shield spray.
    4. 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 power connections for the AC version of SyncServer S6x0. An Over-Current Protection Device must be placed in front of the shelf power.

1. Insert the female end of the AC power cord into the AC power connector on SyncServer S6x0. The power receptacles support IEC cable with V-locks. The V-lock 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.

Figure 2-7. SyncServer S6x0 Single AC Power Connector

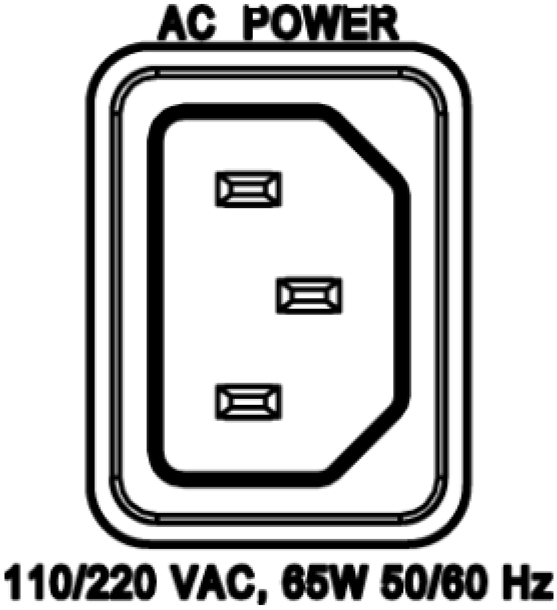
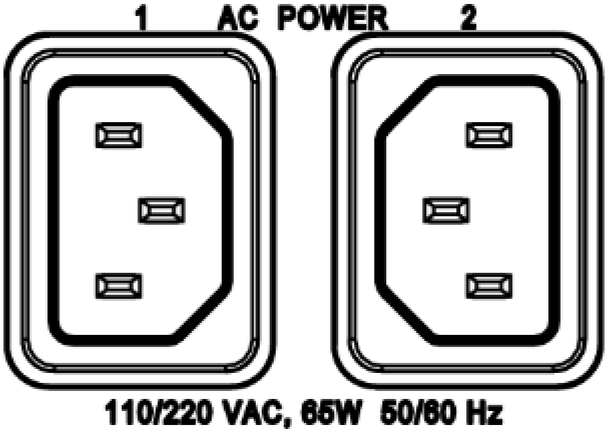


Figure 2-8. SyncServer S6x0 Dual AC Power Connector



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

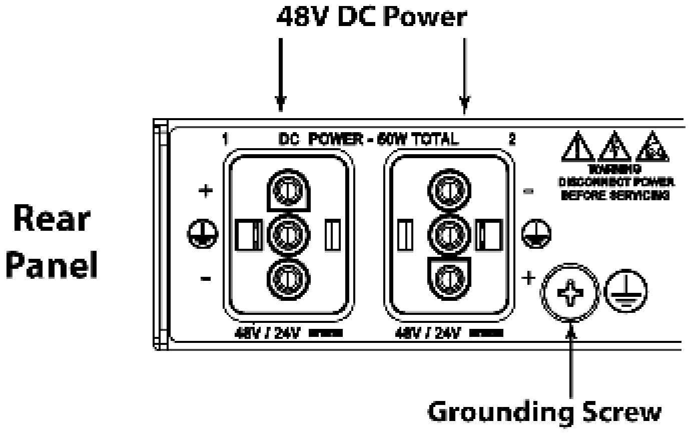
2.4.3 DC Power Connection

Use the following procedure to make power connections for the DC version of SyncServer S6x0. An Over-Current Protection device must be placed in front of the shelf power. 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. 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 must be crimped to the wires.
2. Connect the other end of the DC cable to nominal 24 V_{DC} or 48 V_{DC}.
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 must 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 SyncServer S6x0 are located on the rear panel.

2.5.1 Communications Connections

The communication connections allow user control of SyncServer S6x0. The EIA-232 serial port and Ethernet port 1 (LAN1) are located on the rear panel, as shown in Figure 1-9.

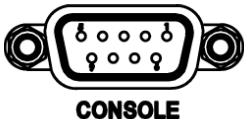
2.5.1.1 Ethernet Port 1

Ethernet port 1 is a standard 100/1000Base-T shielded RJ45 receptacle on the rear panel of the unit. It provides connectivity to a Web interface and to an Ethernet LAN (as well as for NTP input/output). To connect SyncServer S6x0 to an Ethernet network, use an Ethernet RJ45 cable. See Table 2-2 for connector pinouts.

2.5.1.2 Serial (Console) Port

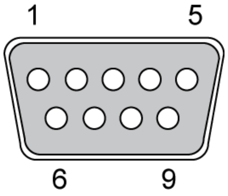
The serial port connection is made through a DB-9 female connector on the rear panel of the unit. This port, which supports a baud rate of 115.2K (115200-8-1-N-1), allows you to connect to a terminal or computer using a terminal emulation software package for remote monitoring and control. This port 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



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

Figure 2-11. Serial Port Male Mating Connector Pins



The following table lists 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

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

2.5.2.1 GNSS Connection

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

Notes:

- The GNSS cable must only be connected while the unit is properly earth grounded.
- To avoid possible damage to equipment, you must provide external lightning protection when installing the GNSS antenna to prevent transients.

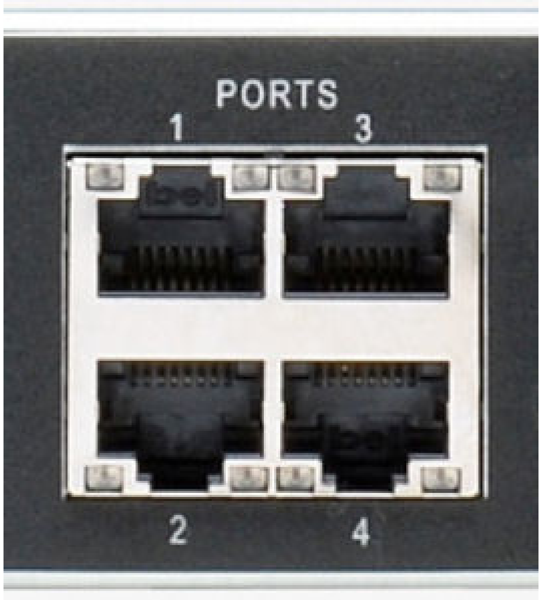
2.5.2.2 Ethernet Connections

The Ethernet ports are standard 100/1000Base-T shielded RJ45 receptacles, which are used for NTP inputs. To connect SyncServer S6x0 to an Ethernet network, use an Ethernet RJ45 cable. The following table lists the connector pinouts.

Table 2-2. System Management Ethernet Connector Pin Assignments

RJ45 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. The following table lists the recommended and supported SFP+ transceivers.

Figure 2-13. 10 GbE Connections

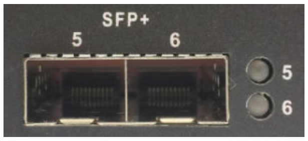


Table 2-3. Recommended and Supported SFP+ (10 GbE) Transceivers

Vendor	Mode	Item Code or P/N
ALU	multi-mode	10GBASE-SR, PN: 3HE04824AA

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

Vendor	Mode	Item Code or P/N
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
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 Figure 1-26. 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 1 PPS or IRIG B AM-In, 10 MHz-In, IRIG AM and IRIG DCLS-Out, 1 PPS-Out and 10 MHz-Out.

The Flex Port technology option enables the six output BNCs (J3–J8) to output any supported signal (time codes, sine waves, programmable rates, and so on.) on all configurable in real time through the secure web interface. Similarly, the two 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 Figure 1-27 to view the signal types for the standard configuration and the configuration with the FlexPort option (Figure 2-14).

See Figure 1-28 for the signal types supported with the Telecom I/O module option (Figure 2-15).

See Table 1-2 for signal types supported with the HaveQuick/PTTI module option (Figure 2-16).

See Figure 2-17 for the fiber optic transmitter module options.

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

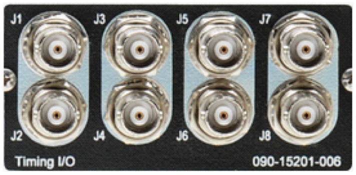


Figure 2-15. Timing I/O with Telecom I/O Connections (090-15201-011)

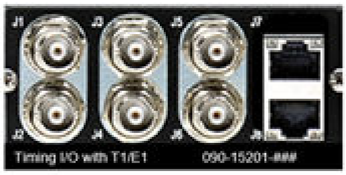


Figure 2-16. Timing I/O with HaveQuick/PTTI Connections (090-15201-012)

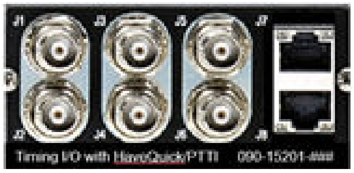
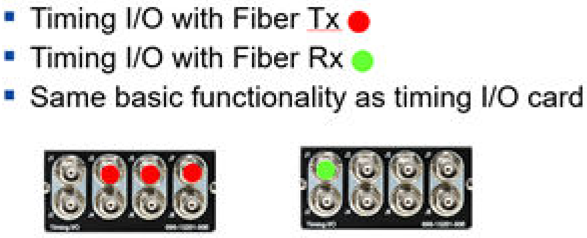


Figure 2-17. Timing I/O with Fiber Optic Transmitter Connections (090-15201-013 and -014)

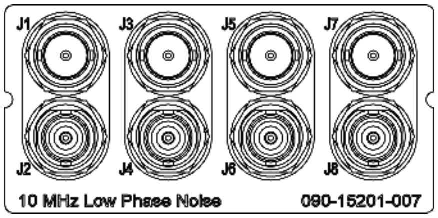


- Timing I/O with Fiber Tx 🔴
- Timing I/O with Fiber Rx 🟢
- Same basic functionality as timing I/O card

2.5.5 LPN Module Connections

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

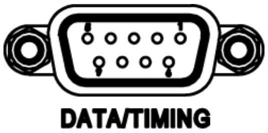
Figure 2-18. LPN BNC Connections



2.5.6 Serial Timing Connection

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.

Figure 2-19. Data/Timing Connection



The following table lists pin-outs for the DB-9 connector.

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

Signal	Pin
TXD	2
RXD	3
Ground	5

See Table 9-26 for TOD format details.

2.5.6.1 1 PPS Output Connection

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

Figure 2-20. 1 PPS Output Connection

2.6 Connecting the GNSS Antenna

The antenna connections for 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 lesser time, provided the antenna has an adequate view of the sky.

Notes:

- The GNSS cables must only be connected while the unit is properly earth grounded.
- The SyncServer S650i does not include a GNSS antenna connector.

Figure 2-21. GNSS Input Connection

Proper cable, grounding techniques, and lightning arrestors must 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 an obstruction blocking part of the sky. Mount the antenna high above roads or parking lots.

Note: For best 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.

⚠ CAUTION

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

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

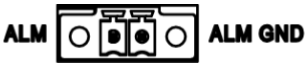
2.7 Connecting Alarm Relay

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 Checklist

Following is the list of checks and procedures to verify if the installation of SyncServer S6x0 is complete.

- Ensure that SyncServer S6x0 chassis is securely attached to mounting rack.
- Verify that all power and ground wires are installed correctly and securely.
- Verify that all communications cables are properly installed.
- Verify that all input and output cables are properly installed.

2.9 Applying Power to SyncServer S6x0

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 SyncServer S6x0 powers up and begins normal operation, all LEDs turn ON. After the self-test is complete and the firmware is operational, the LED states might change to indicate the appropriate state or status. The following table lists the SyncServer S6x0 LEDs.

Table 2-5. LED Descriptions

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

SyncServer 6x0 does not contain a battery-backed real-time clock. Therefore, it always boots up with a default value for the system time. This time is 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 is used for the first log entries when booting up the unit. The time changes to local time during the boot-up process if a time zone has been configured.

3. Keypad/Display Interface

This section describes the Keypad/Display interface of the SyncServer device.

3.1 Overview

The Keypad/Display interface displays the time, system status, and performs 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 SyncServer starts, the display shows “Booting SyncServer please wait...”. Thereafter, 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: During numeric entry, the left/right arrows change where the next number is entered from the keypad. For status displays, the left/right arrows can scroll horizontally when `<previous:next>` is displayed.
- Up/Down Arrow Buttons: In status, scrolls a screen vertically, displays the previous/next screen.
- Number Buttons: Enters a number, or selects a numbered menu item.
  The following 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 describe these three buttons in 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), then the time display shows **GPS** as the time scale.

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

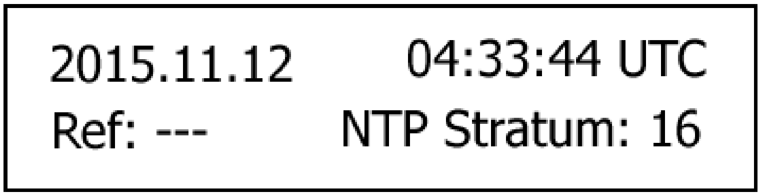
3.3 STATUS Button

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

- 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



```
2015.11.12      04:33:44 UTC
Ref: ---     NTP Stratum: 16
```

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

3.3.1 Network Time Protocol Status Screen

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

Hardware Clock Input Reference is a Stratum 0 source. Stratum 2–15 means that SyncServer is locked to another Network Time Protocol (NTP) time source. Stratum 16 means that 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 might 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. SyncServer replies to clients that send NTP requests. It also sends NTP requests when the NTP daemon is not synchronized (that is, Sync LED is RED) and when it is configured to synchronize to an NTP association (that is, a server type association).

3.3.2 Alarm Status Screen

This is the 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

These are multiple screens—four for each network port. Two screens each for IPv4 and IPv6 are available. 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

- 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
  - Maximum Carrier-to-Noise ratio (C/No): The highest C/No of all satellites (value given for each satellite type)
- NSS Solution
  - Status: OK Service 3D
  - Mode: Auto or Manual

3.3.6 SyncServer Status Screen

This screen displays the hardware and software identification, and the 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

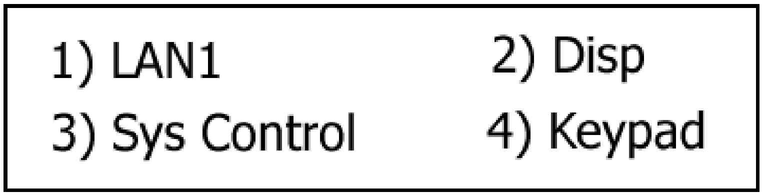
This screen displays the configuration of every slot A/B input and output connections.

- 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

The following figure shows a MENU button that presents a numbered menu of functions.

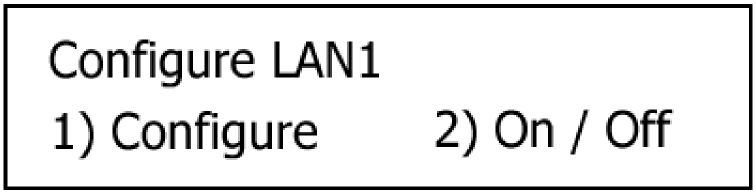
Figure 3-2. Menu of Functions



3.4.1 LAN1

Select LAN1 option to open the Display menu screen.

Figure 3-3. Configure LAN1 Screen

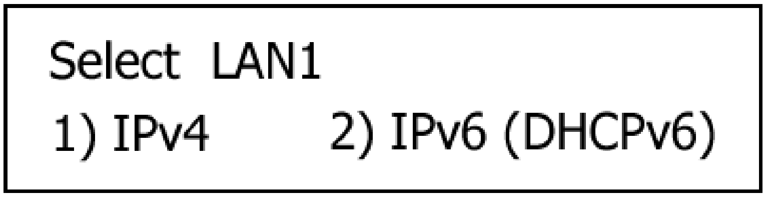


1. **Configure**: Selects IPv4 or IPv6 address mode for LAN1 port. IPv6 automatically configures LAN1 with a dynamic IPv6 address.

If Configure is selected, the Select LAN1 screen appears, as shown in the following figure:

2. **On/Off**: On enables the LAN1 network port. Off disables the LAN1 network port for all traffic types.

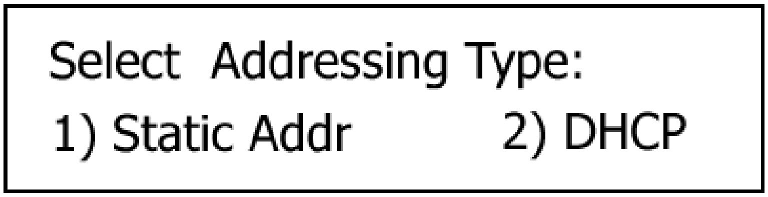
Figure 3-4. Select LAN1 IP Mode Screen



Select LAN1
1) IPv4 2) IPv6 (DHCPv6)

3. **IPv4**: Select IPv4 address mode for LAN1 port.
   If IPv4 is selected, the Select Addressing Type screen appears, as shown in the following figure:
4. **IPv6**: Select IPv6 address mode for LAN1 port.
   If IPv6 (DHCPv6) is selected, the SyncServer automatically configures LAN1 with a dynamic IPv6 address.

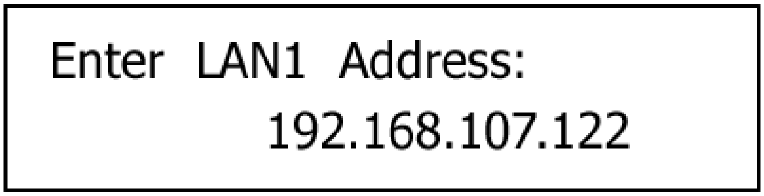
Figure 3-5. Select IPv4 Addressing Type Screen



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 the following figure. After the address is entered, press the ENTER button to enter the Subnet mask (then ENTER) followed by the Gateway address. Once the gateway address has been entered, the LAN 1 port is 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



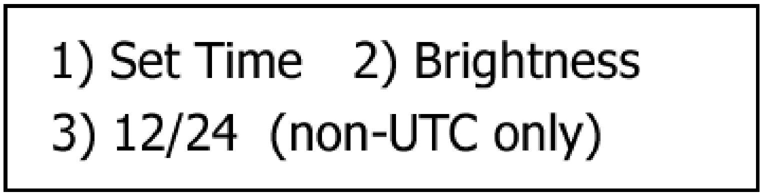
Enter LAN1 Address:
192.168.107.122

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

3.4.2 Display

Select Display to open the Display menu screen.

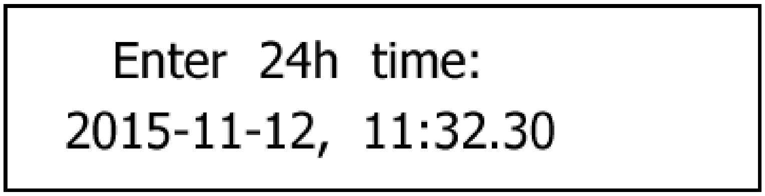
Figure 3-7. Display Menu Screen



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, as shown in the following figure.

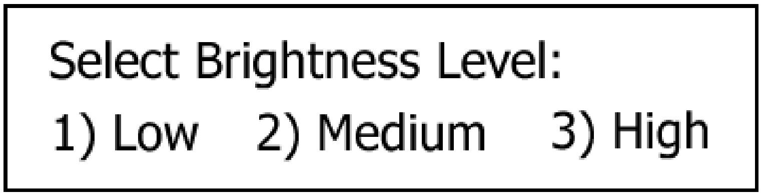
Figure 3-8. Set Time Screen



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

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

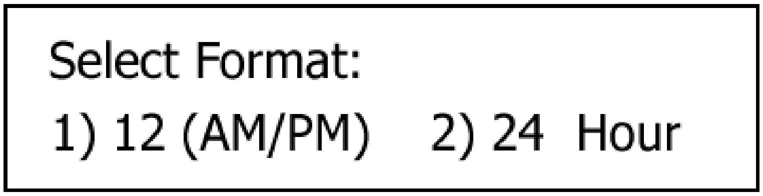
Figure 3-9. Set Brightness Screen



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.
Note: The 12/24 and 24 hour appear only if a local time zone has been specified through the Web interface.

Figure 3-10. Select Time Format Screen



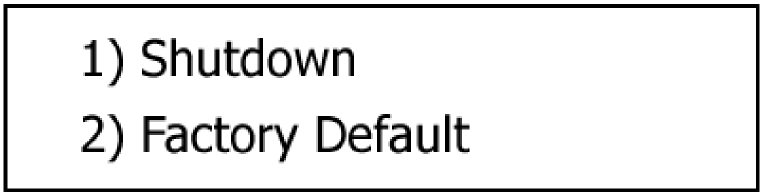
Select Format:
1) 12 (AM/PM) 2) 24 Hour

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

3.4.3 Sys Control

Select Sys Control to open the Shutdown/Factory default screen.

Figure 3-11. Shutdown/Factory Default Screen

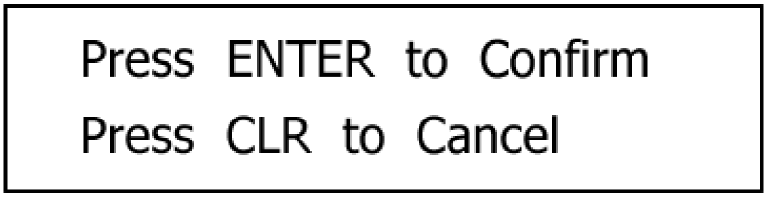


1) Shutdown
2) Factory Default

See section 9.3. Factory Defaults for default settings.

1. **Shutdown**: Halts the SyncServer. The following figure shows the message that appears in the display.
2. **Factory Default**

Figure 3-12. Confirmation Screen

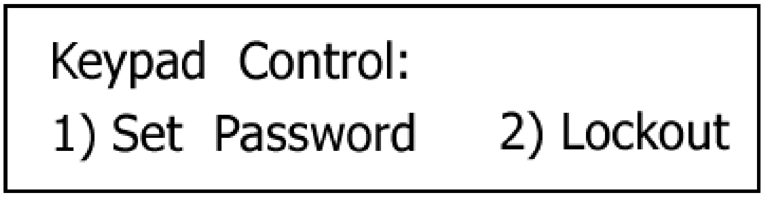


Press ENTER to Confirm
Press CLR to Cancel

3.4.4 Keypad

Select Keypad to open the Keypad Control screen.

Figure 3-13. Keypad Control Display Screen



Keypad Control:

1) Set Password 2) Lockout

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. When asked for confirmation, the factory default password for the keypad is 95134.

4. CLI Commands

This section 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 the list 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 replace the current configuration with the factory default configuration. On SyncServer, user is prompted with **Y** to confirm the step.

Command Syntax:

```
set configuration factory
```

Returning the configuration to factory defaults also includes the following:

- Loss of configured user logins
- Loss of configured network settings (addresses, firewall, and so on.)

Installed licenses remain installed. SyncServer S6x0 reboots as part of this process.

The behavior with this command is identical to using the Web GUI 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 at which SyncServer S6x0 receives a request from the user. The following table lists the general behavior. This function is configurable through the CLI 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 connection responds to ctrl-C and SHIFT-T inputs only.
`ctrl - C`	Disables the connection for time on request operation.
`SHIFT-T`	Enabling time on request triggers a time response on the connection. **Note**: The “T” does not appear (it is not echoed back by SyncServer S6x0).

Enter the `F9<CR>` command to prepare SyncServer S6x0 for the user's request. At the desired moment, send the request to SyncServer S6x0 by entering an upper case “T”. SyncServer S6x0 saves the current ToD, accurate to within 1 microsecond, to a buffer, and then outputs it to the CLI. SyncServer S6x0 continues to provide the ToD 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 ToD 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 the following
  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
```

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

Use function F50 to display the current GPS position, and 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><C
R><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. SyncServer S6x0 returns a response in the following format:

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

The alphanumeric characters 1–9 and A–J represent specific positions, as shown in the preceding response string. The following table lists 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 (for example, GPS, IRIG, and so on). 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 might 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.
<SOURCE>	Clock Source	"A" = Clock to Timing I/O Slot A (J1A) "B" = Clock to Timing I/O Slot B (J1B), "J" = Clock to PTP "P" = Clock to GNSS "R" = Clock to External Input Frequency Reference (J2A/B) "T" = Clock to NTP "F"= None	Same as Web GUI "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 1 PPS.
<SP>			ASCII space character, one or more

...........continued			
Syntax	**Alarm**	**Indicators**	**Description**
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	LPN Oscillator PLL	"–" = Locked "L" = Unlocked	The LPN oscillator indicator might report "Unlocked" during initial lock and holdover recovery. While reporting "Unlocked", LPN module's output signals are not locked to the system clock.
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:** Disabling of GNSS also generates "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. • The disabling of AJ1 also generates "I". • If this input is configured for PPS/10MPPS, then this alarm will react based on the condition of the input • This only applies to slot A.
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 (1/5/10 MHz). This is equivalent to Green indication for slot A–J2 in Web GUI **Dashboard > Timing > Holdover**References row. **Notes:** • Disabling of slot A–J2 also generates "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 must 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.

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

Syntax	Alarm	Indicators	Description
`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 Web GUI **Dashboard > Timing > Holdover**form.
`D`	Timeout		Always “–”
`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:** Disabling of BJ1 will also generate “I”. If this input is configured for PPS/10 MPPS, then 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 (1/5/10 MHz). This is equivalent to Green indication for Slot B–J2 in WebGUI **Dashboard > Timing > Holdover**References row. **Note:** Disabling of Slot B– J2 also generates “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 through 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) is 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 the history
- Anything entered, even if it is not valid syntax (item 2), is 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: This version is also displayed with the `show system` command.
- Backup image (2) is available and 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 logout

Use this command to log off the unit and terminate the session.

```
logout
```

4.1.13 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 >
```

4.1.14 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
```

4.1.15 reboot system

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

4.1.16 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 (that is, user entries) for the configured duration. If the connection is remote SSH, then the connection terminates upon timeout. If the session is direct to the CONSOLE serial port, then auto-logout occurs upon timeout.

Command Syntax:

```
set-session-timeout
```

The system prompts for the timeout value.

Example:

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

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

The system prompts for the timeout value.

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

Enter the following, then press Enter.

```
3600
```

Response:

```
3600 sec timeout set succcessfuly
```

4.1.17 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
```

4.1.18 show system

Use this command to display basic facts about SyncServer S6x0.

Command Syntax:

```
show system
```

Example

```
SyncServer> show system
```

Response

```

Host Name        : SyncServer
Serial Num       : RKT-15309034
Model Num        : SyncServer S650
Build            : 4.1.3
Uname            : Linux SyncServer 4.1.22-ltsi #1 SMP Mon Apr 12 21:05:20 PDT
                   2021 armv7l
Uptime           : 111 day(s) 3 hour(s) 15 minute(s) 44 second(s)
Load Avg         : 0.33 0.33 0.27
Free Mem         : 78.09%
CPU Model        : ARMv7 Processor rev 0 (v7l)
CPU Identifier   : Altera SOCFPGA
Total Mem        : 1005 MB
Oscillator Type  : Rubidium
Update Available : Up to date
```

5. Web Interface

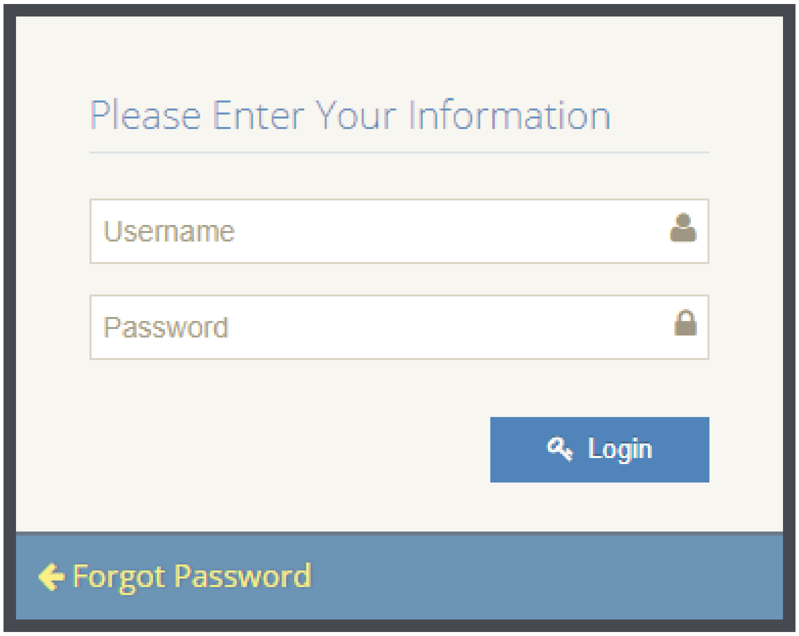
This section describes the Web interface for SyncServer S6x0.

See 6.1.1. Communicating Through LAN1 Ethernet Port for details on how to access the Web interface.

Notes:

- For security reasons, SyncServer S6x0 only supports HTTPS. However, the user gets warnings from most web browsers that a self-signed certificate is being used (not from a recognized certificate authority). You must accept the warnings and proceed to the login page. The internal self-signed certificate can be renewed and updated on the `Security > HTTPS` page. You can also request and install an HTTPS certificate.
- The default user name is **admin** and the default password is: Microsemi. To avoid unauthorized access, you must change the default password. When logging in for the first time, or after a factory default, the system forces you to change the password.

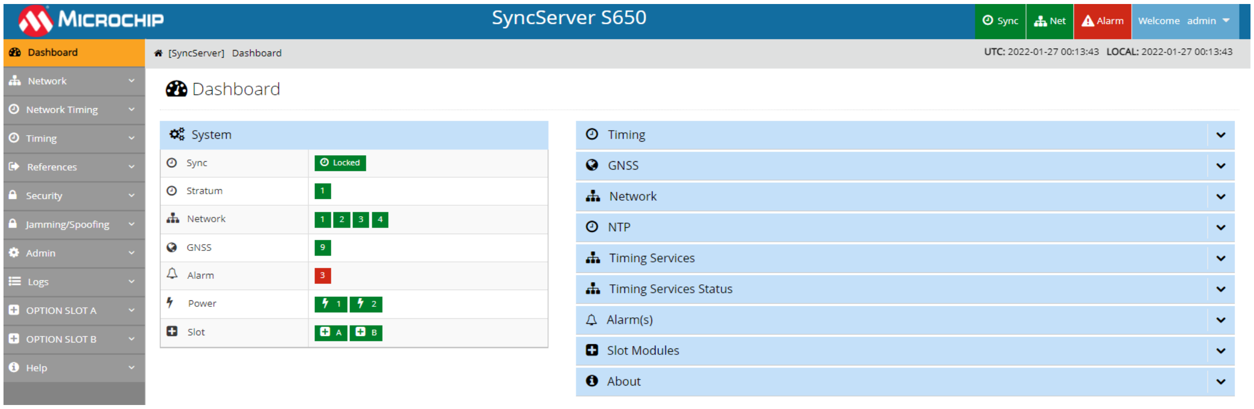
Figure 5-1. Login



For security reasons, SyncServer S6x0 locks out a user for an hour if an invalid password is entered three times. The lockout is 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 must change the default password. When logging in for the first time, or after a factory default, the system forces you to change the password.

Figure 5-2. Dashboard Screen



UTC: 2022-01-27 00:13:43 LOCAL: 2022-01-27 00:13:43

System	
Sync	Locked
Stratum	1
Network	1 2 3 4
GNSS	9
Alarm	3
Power	1 2
Slot	A B

Notes:

- 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.
- If the browser is displaying a busy indicator, then wait until the previous action is complete before starting another action. Depending on the browser used, the web page's responsiveness varies due to the use of the encryption cipher suite used in S6x0. Microchip recommends using the Google Chrome browser. Under heavy network traffic load, the web responsiveness degrades.
- When system is under full rated load, opening more than one web session is not recommended, as it has a large performance impact.

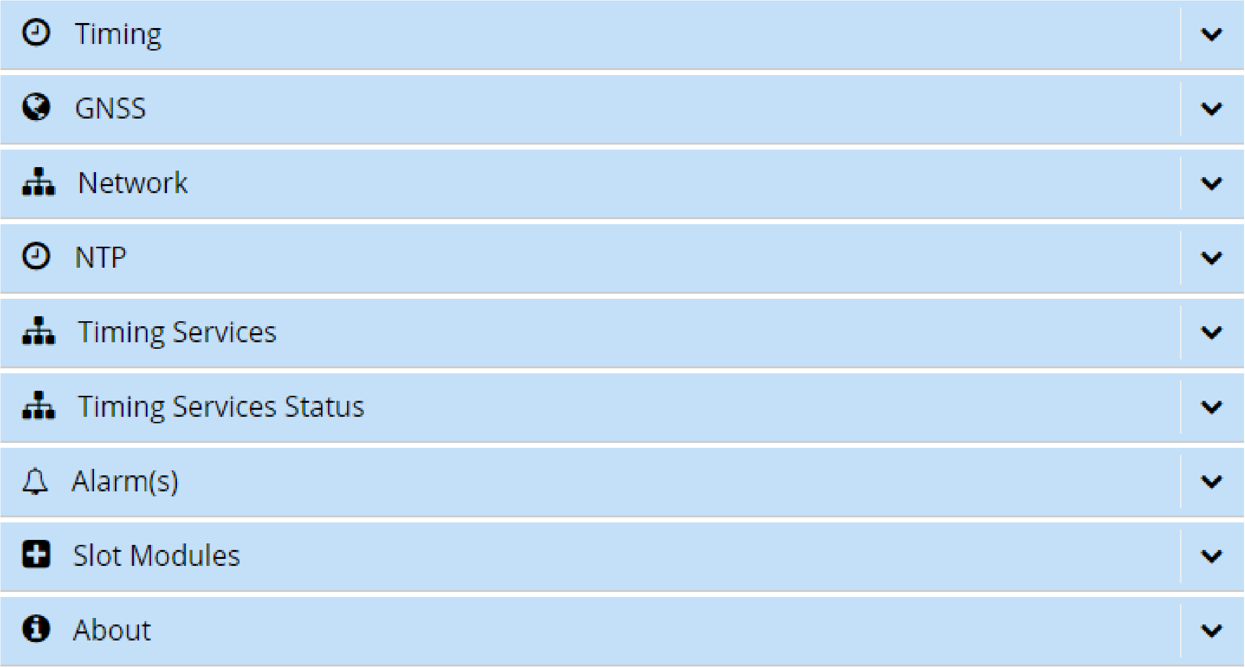
5.1 Status/Information Windows

The following figure shows the Status/Information windows in the dashboard, that display 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.

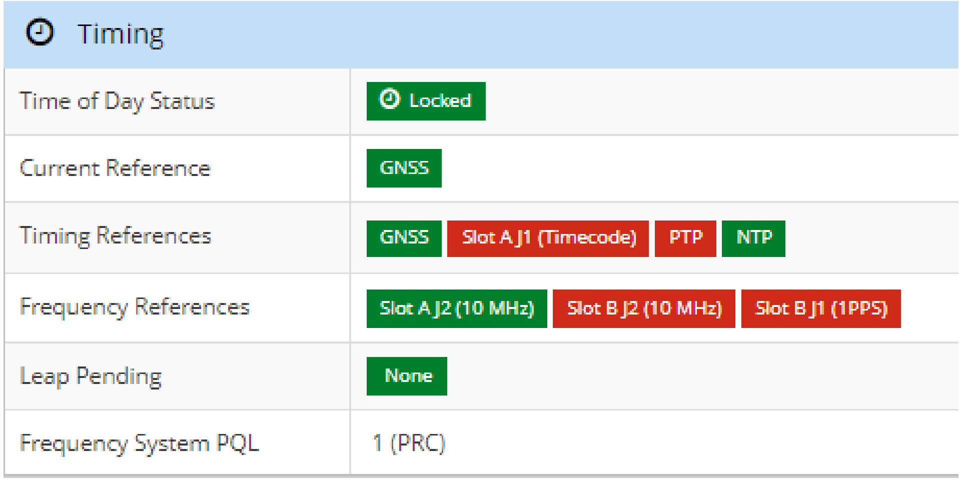
Figure 5-3. Status/Information Windows



5.1.1 Timing Status and Information

The following figure shows the Timing window in the dashboard that displays status details and information about system timing, including current reference, lock status, and status of input references. For details, see Table 5-1.

Figure 5-4. Timing Window



Timing

Time of Day Status	Locked
Current Reference	GNSS
Timing References	GNSS 🟥 Slot A J1 (Timecode) 🟥 PTP NTP
Frequency References	Slot A J2 (10 MHz) 🟥 Slot B J2 (10 MHz) 🟥 Slot B J1 (1PPS)
Leap Pending	None
Frequency System PQL	1 (PRC)

Note: SyncServer 6x0 does not contain a battery-backed real-time clock. Therefore, it always boots up with a default value for the system time. This time is 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 is used for the first log entries when booting up the unit. The time changes 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: Only if internal oscillator.
Timing References	This row shows all enabled time references.	Green: If a time reference is ready to be used. Red: If it is not ready.
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.	Green Holdover source: If is ready to be used. Red Holdover source: If it is not ready.
Leap Pending	This row indicates if a Leap second is pending.	Green: If there is no warning of a Leap second pending. Red: If there is a warning of a Leap second pending.
Frequency System PQL	This row indicates the value of the system PQL which is a frequency quality level for the system. It is based on the current reference or the internal oscillator, if in holdover.	There is no color for this row.

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 includes 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 might be different for a brief time.

If there are no valid timing references, but there is a valid frequency reference, then there must be text shown, as 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 displays 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 frequency and time).
Freerun	SyncServer does not have a time reference and never has had one since powerup.	—
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, by definition, has 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 must 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 does 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 in holdover using an external frequency reference OR we are in holdover using 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 do 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.	—

Note:

1. The main purpose of holdover is to allow tS6xx 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 that 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 S6xx. Once the S6xx reacquires GNSS and relocks, the NTP Reference Time Stamp is again 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 must never return to stratum 16. Instead, it uses the reference time stamp behavior.

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 frequency 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 is identically indicated in the Current Reference row 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 appears 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 is the current source. If there is no qualified Frequency Reference (nothing green in that row), then only SyncServer internal reference remains, and it appears in the Current Reference row. In this case, the entry is one of the following, depending on the specific SyncServer product oscillator type: • Internal Rb • Internal OCXO • Standard

5.1.2 GNSS Status and Information

The GNSS window in the dashboard, as shown in the following figure, 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?" might be temporarily displayed if the system is not fully tracking the satellite.

Figure 5-5. GNSS Window

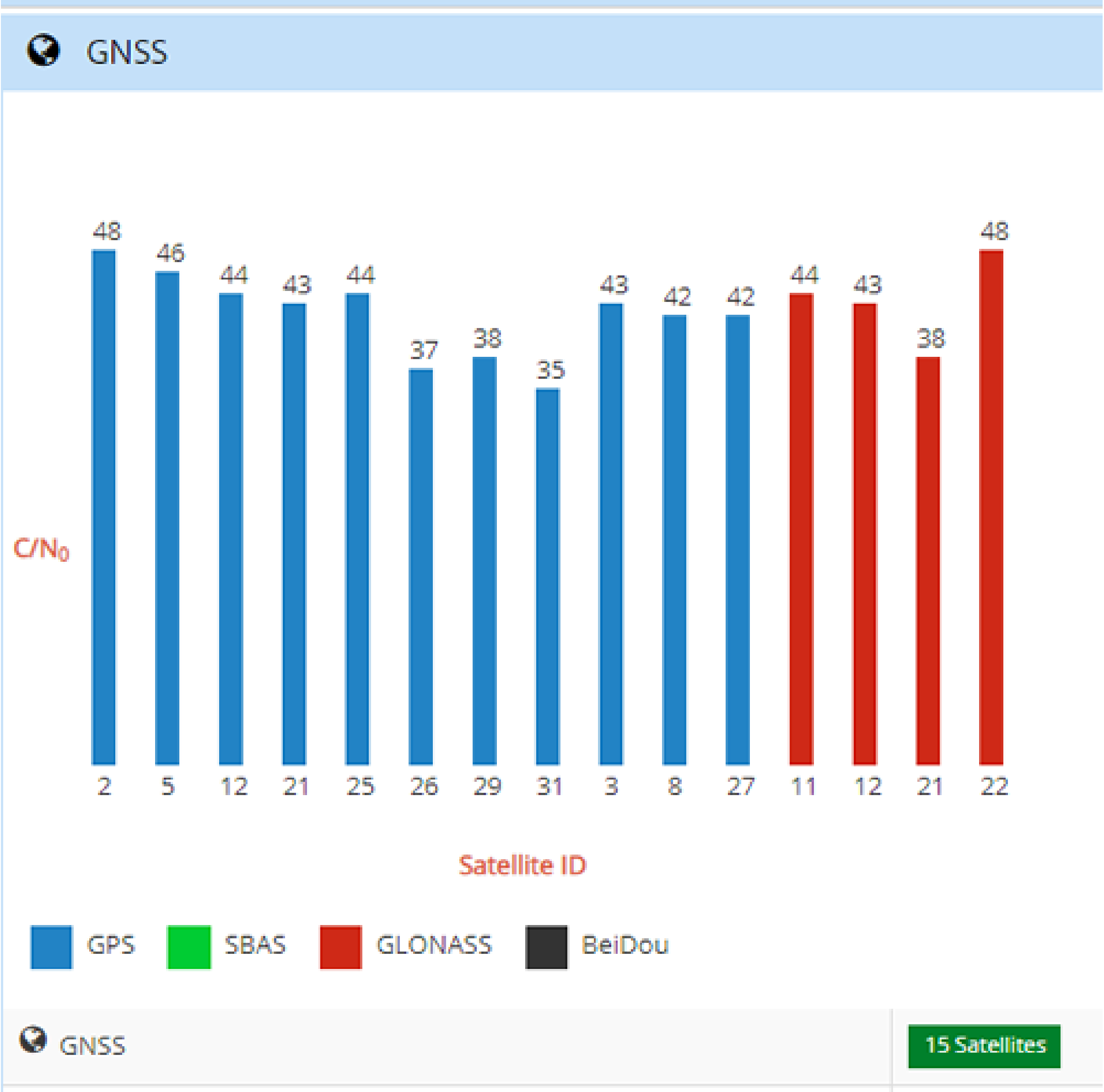


Table 5-4. GNSS Window—Descriptions

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	—

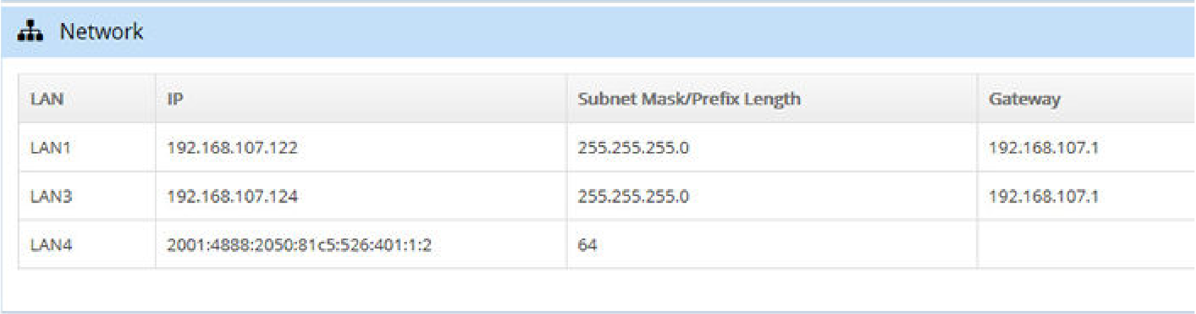
...........continued

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.

5.1.3 Network Status and Information

The Network window in the dashboard displays status details and information about the network ports in use.

Figure 5-6. Network Window



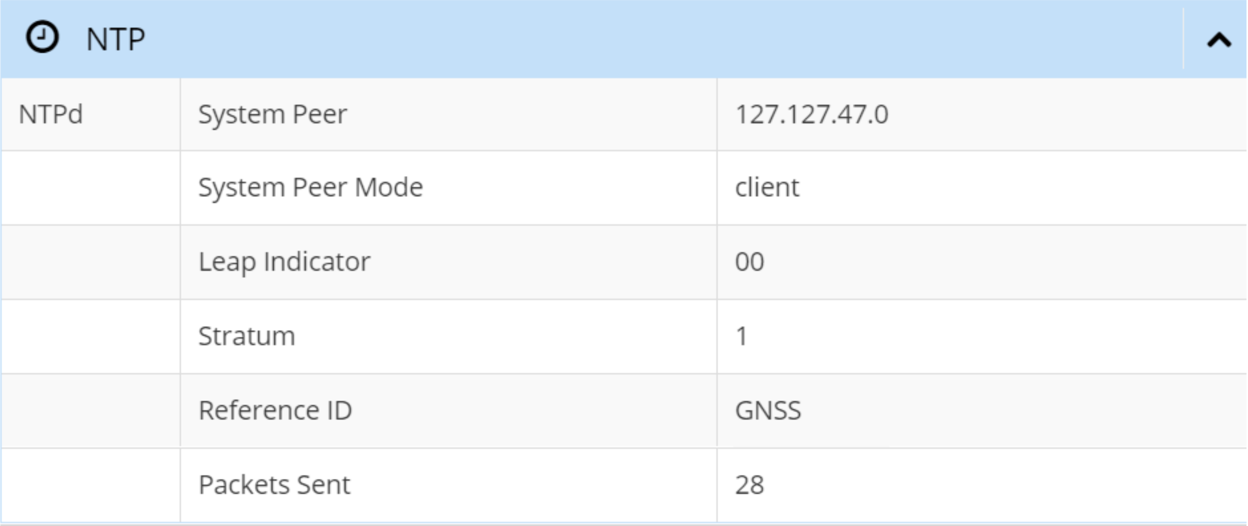
Network

LAN	IP	Subnet Mask/Prefix Length	Gateway
LAN1	192.168.107.122	255.255.255.0	192.168.107.1
LAN3	192.168.107.124	255.255.255.0	192.168.107.1
LAN4	2001:4888:2050:81c5:526:401:1:2	64	

5.1.4 NTP Status and Information

The NTP window in the dashboard displays status details and information about the NTP configuration.

Figure 5-7. NTP Window



NTP

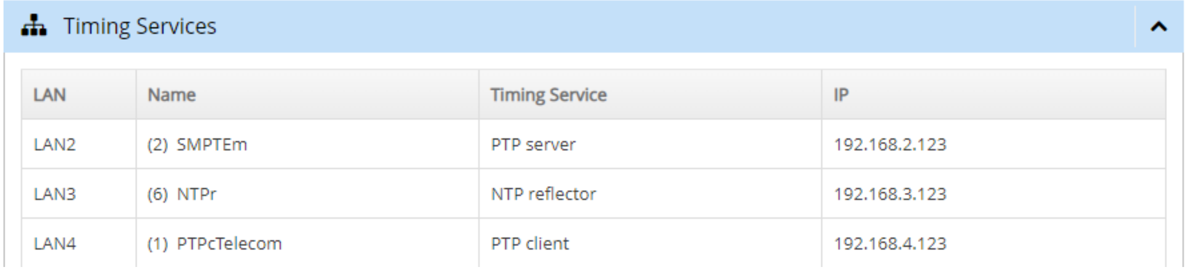
NTPd	System Peer	127.127.47.0
	System Peer Mode	client
	Leap Indicator	00
	Stratum	1
	Reference ID	GNSS
	Packets Sent	28

Note: The dashboard provides 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) is only 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.

5.1.5 Timing Services Information

The following figure shows the Timing Services window in the dashboard. It displays status details and information about the timing service on each port.

Figure 5-8. Timing Services Window



Timing Services

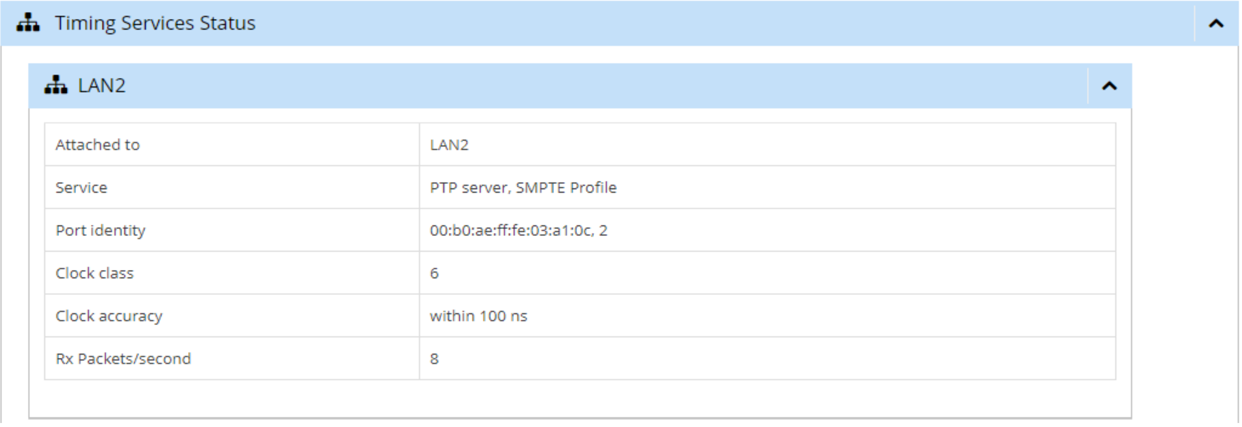
LAN	Name	Timing Service	IP
LAN2	(2) SMPTEm	PTP server	192.168.2.123
LAN3	(6) NTPr	NTP reflector	192.168.3.123
LAN4	(1) PTPcTelecom	PTP client	192.168.4.123

5.1.6 Timing Services Status

The Timing Services Status window in the dashboard 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 Server is found in the window `Network Timing > NTPr/PTP` status, in the Port State row.

Figure 5-9. Timing Services Status Window



Timing Services Status

LAN2

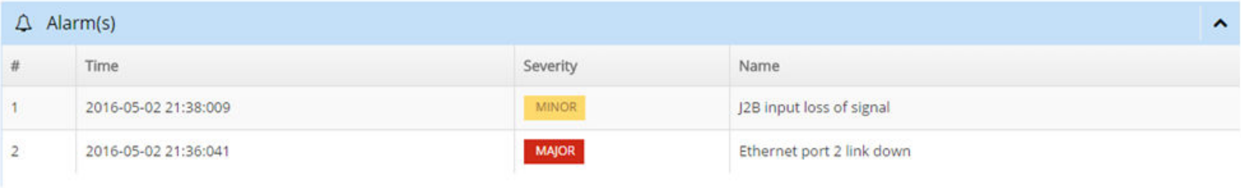
Attached to	LAN2
Service	PTP server, SMPTE Profile
Port identity	00:b0:ae:ff:fe:03:a1:0c, 2
Clock class	6
Clock accuracy	within 100 ns
Rx Packets/second	8

5.1.7 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



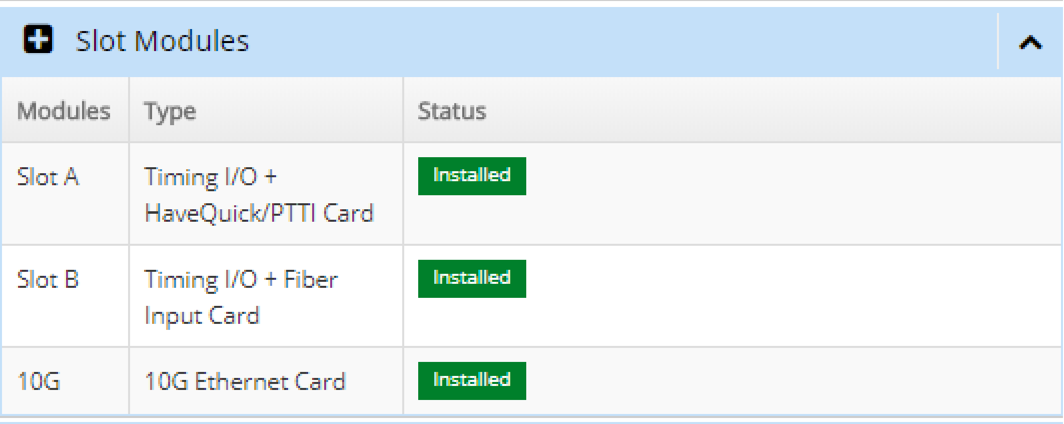
Alarm(s)

#	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

5.1.8 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



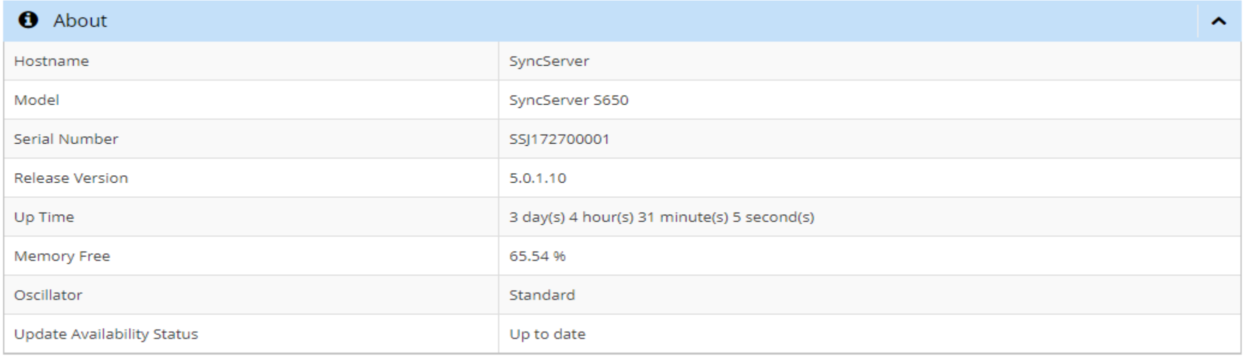
Slot Modules

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

5.1.9 "About" Device Information

The following figure shows the About window in the dashboard, that displays system information about the unit.

Figure 5-12. About Window



About

Hostname	SyncServer
Model	SyncServer S650
Serial Number	SSJ172700001
Release Version	5.0.1.10
Up Time	3 day(s) 4 hour(s) 31 minute(s) 5 second(s)
Memory Free	65.54 %
Oscillator	Standard
Update Availability Status	Up to date

Notes:

- The update available feature only functions if LAN1 has been configured with an IPv4 address and a DNS server is configured. The DNS server can be either automatically configured through DHCP or manually, when using a static IP address. The update available feature can be disabled on the `Admin->General` page.
- You can check for the latest version number of SyncServer S600 and S650 softwares at the following URLs: http://update.microsemi.com/SyncServer_S600

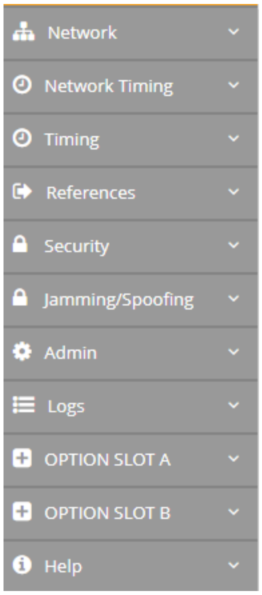
  http://update.microsemi.com/SyncServer_S650

  The number of the most current version of the software appears. You can compare this to the version number installed in 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, contact the Technical Support team.

5.2 Navigation Windows

The navigation portion of the Web interface is used to access the various pages to configure many aspects of SyncServer S6x0 and to view the status information. The navigation menu expands and contracts depending on the current selection.

Figure 5-13. Navigation Portion of Dashboard



5.2.1 Network Configuration Windows

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

5.2.1.1 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:

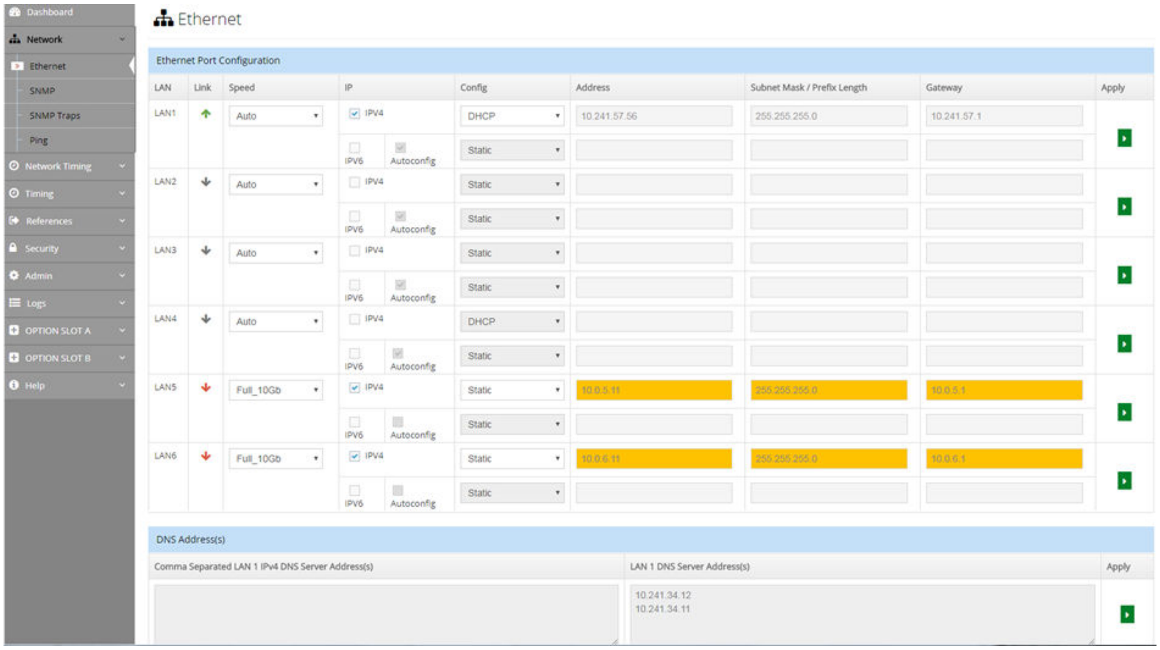
- Speed
  - Auto | Full 100 | Full 1000
- IP format
  - IPv4 | IPv6
- Config
  - Static | Dynamic
  - IPv6 Auto Config
- IP address
- Subnet mask for IPv4, prefix length for IPv6
- Gateway address

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

See 12. Port Details for information on Ethernet port isolation, management port rules, and timing port rules.

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

Figure 5-14. Network—Ethernet Configuration Window



Ethernet

Ethernet Port Configuration

LAN	Link	Speed	IP		Config	Address	Subnet Mask / Prefix Length	Gateway	Apply
LAN1	↑	Auto	☑ IPV4		DHCP	10.241.57.56	255.255.255.0	10.241.57.1	▶
			□ IPV6	☑ Autoconfig	Static				
LAN2	↓	Auto	□ IPV4		Static				▶
			□ IPV6	☑ Autoconfig	Static				
LAN3	↓	Auto	□ IPV4		Static				▶
			□ IPV6	☑ Autoconfig	Static				
LAN4	↓	Auto	□ IPV4		DHCP				▶
			□ IPV6	☑ Autoconfig	Static				
LAN5	↓	Full_10Gb	☑ IPV4		Static	10.0.5.11	255.255.255.0	10.0.5.1	▶
			□ IPV6	□ Autoconfig	Static				
LAN6	↓	Full_10Gb	☑ IPV4		Static	10.0.6.11	255.255.255.0	10.0.6.1	▶
			□ IPV6	□ Autoconfig	Static				

DNS Address(s)

Comma Separated LAN 1 IPv4 DNS Server Address(s)	LAN 1 DNS Server Address(s)	Apply
	10.241.34.12 10.241.34.11	▶

5.2.1.2 Network—SNMP Configuration

Use this window to add, edit, or delete v2 communities, and to add or delete SNMP users.

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.

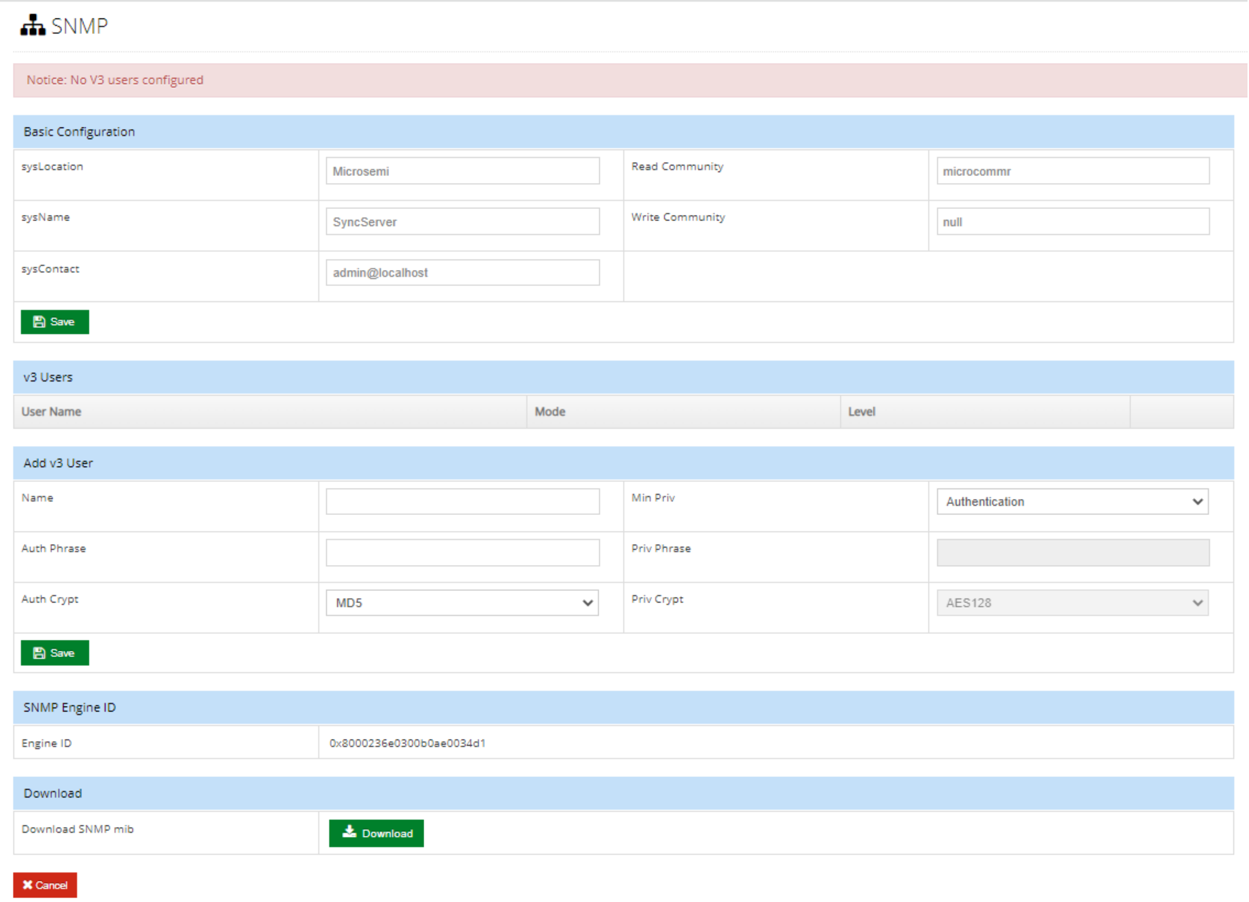
Note: SNMPv2 can be disabled by configuring blank read and write community names.

- Add v3 User—up to 10 users can be added.
  - Name, 1–32 characters.
  - Authentication phrase, 1–49 characters.
  - Authentication encryption: MD5, SHA1, SHA224, SHA256, SHA384, or SHA512.
  - Privacy phrase, 8–99 characters.
  - Privacy selection: “Authentication” or “Authentication & Privacy”.
  - Privacy encryption: AES128, AES192, AES192C, AES256, or AES256C.
- SNMP user names, community names, and privacy/authentication phrases can contain all ASCII characters except (<), (&), (>), (“), and ('). However, community names might contain (&).

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

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

Figure 5-15. Network—SNMP Window



SNMP

Notice: No V3 users configured

Basic Configuration

sysLocation	Microsemi	Read Community	microcommr
sysName	SyncServer	Write Community	null
sysContact	admin@localhost		

v3 Users

User Name	Mode	Level	

Add v3 User

Name		Min Priv	Authentication
Auth Phrase		Priv Phrase	
Auth Crypt	MD5	Priv Crypt	AES128

SNMP Engine ID

Engine ID	0x8000236e0300b0ae0034d1

Download

Download SNMP mib	Download

5.2.1.3 Network—SNMP Trap Configuration

Use this window to 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.

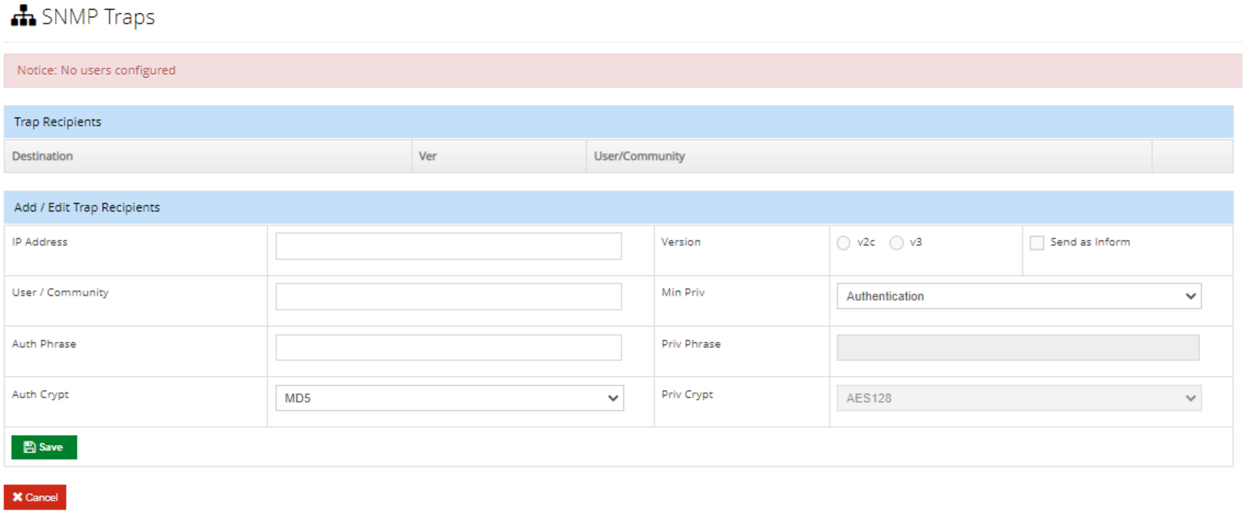
- Authentication Phrase (v3 only), 1–32 characters.
- Privacy Selection: “Authentication” or “Authentication & Privacy”.
- Privacy Phrase (v3 only), 1–32 characters.
- Authentication Encryption: MD5, SHA1, SHA224, SHA256, SHA384, or SHA512 (v3 only).
- Privacy encryption: AES128, AES192, AES192C, AES256, or AES256 (v3 only).
- Checkbox enable to send SNMP inform instead of SNMP trap.

The following figure shows the SNMP traps window.

Notes:

- Some SNMP browsers and trap managers require that an SNMPv3 user must be created with the same username and authentication as used for the trap configuration, so that the SNMPv3 discovery process completes properly.
- 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).
- Up to 10 SNMP trap recipients can be configured.
- Changing an SNMP configuration parameter (such as community or SNMPv3 user), causes SNMP to restart and the MIB2 `sysuptime` to restart counting upward.

Figure 5-16. Network—SNMP Traps



SNMP Traps

Notice: No users configured

Trap Recipients

Destination	Ver	User/Community	

Add / Edit Trap Recipients

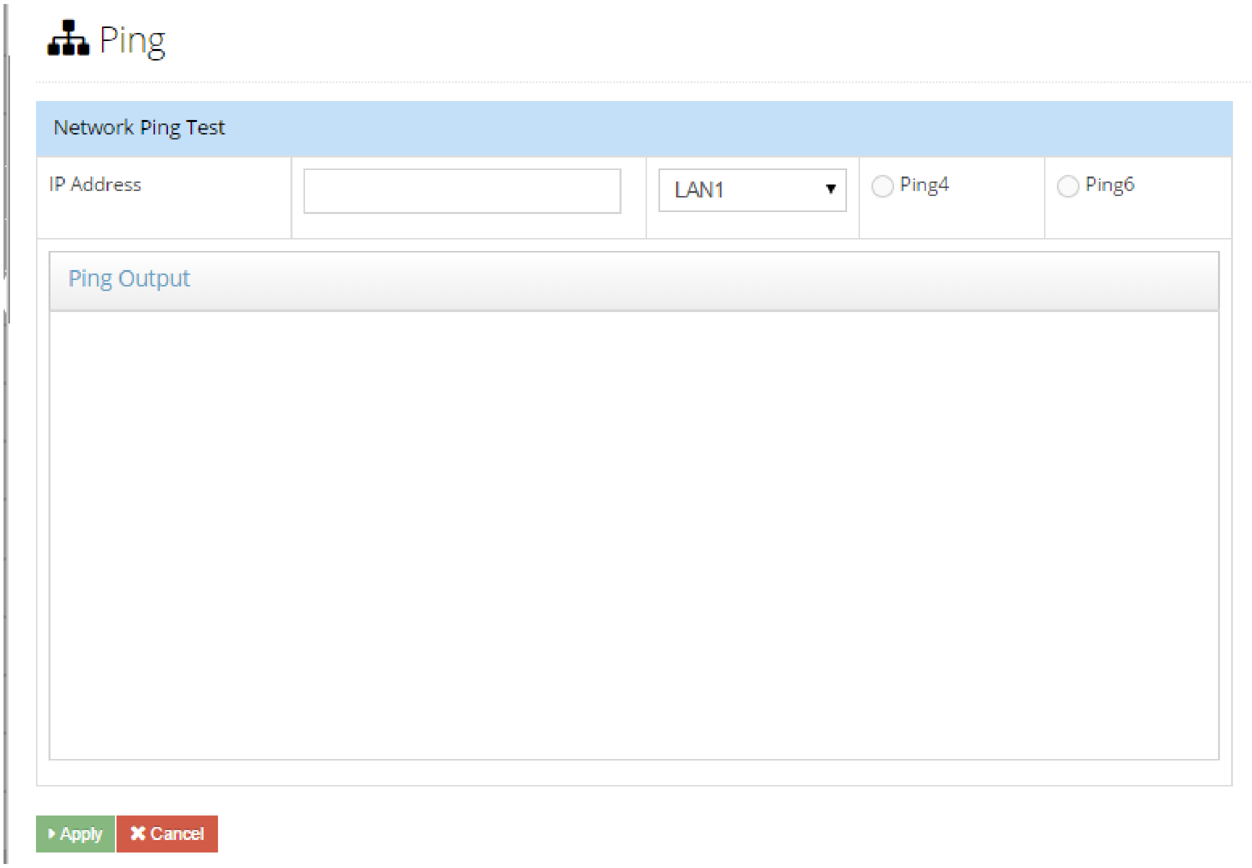
IP Address		Version	○ v2c ○ v3	□ Send as Inform
User / Community		Min Priv	Authentication	
Auth Phrase		Priv Phrase		
Auth Crypt	MD5	Priv Crypt	AES128	

5.2.1.4 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 is displayed in the window when completed. An IPv4 or IPv6 address must be entered in the IP address field.

Ping might not operate as expected when IPv6 auto-config is enabled. An IPv6 source address can be used that does not route correctly to the destination address.

Figure 5-17. Network—Ping Window



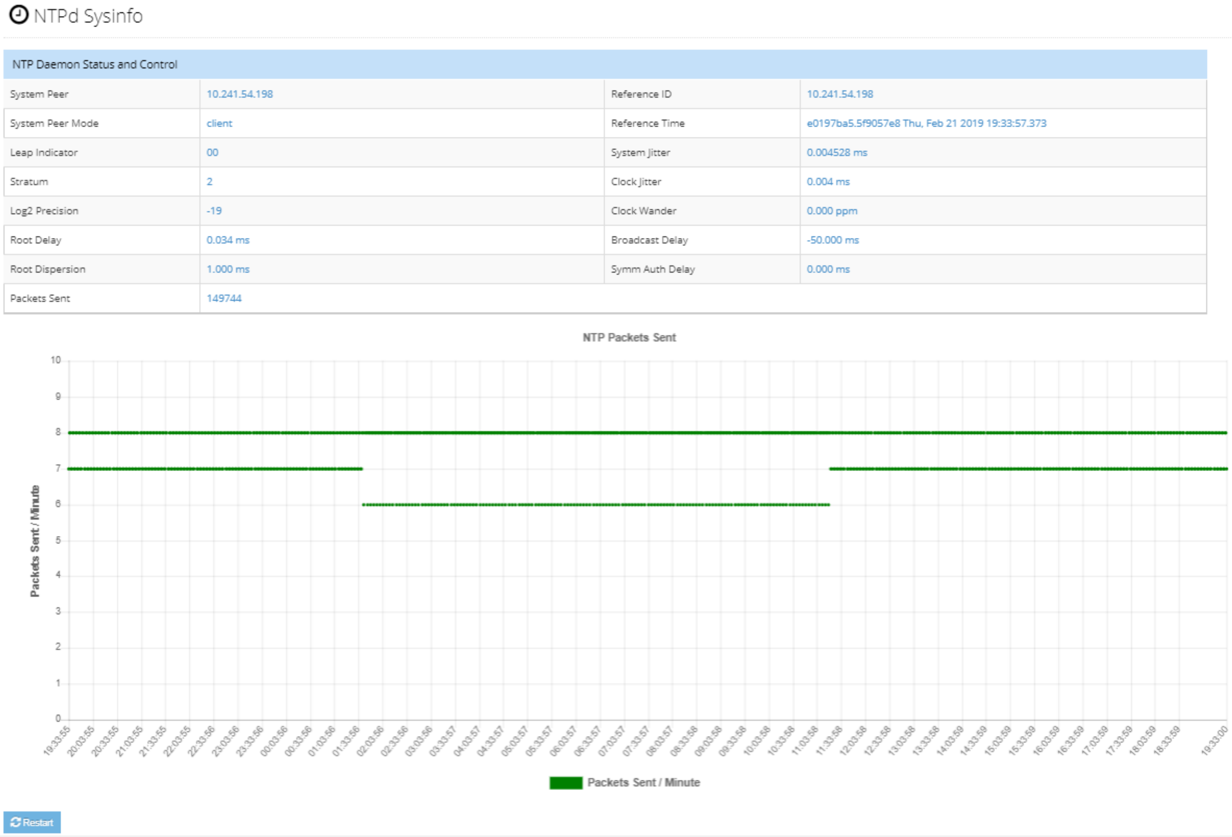
5.2.2 Network Timing Windows

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

5.2.2.1 NTP SysInfo Window

Use this window to view NTP Daemon Status and Control.

Figure 5-18. NTP SysInfo Window



NTPd Sysinfo

NTP Daemon Status and Control			
System Peer	10.241.54.198	Reference ID	10.241.54.198
System Peer Mode	client	Reference Time	e0197ba5.5f9057e8 Thu, Feb 21 2019 19:33:57.373
Leap Indicator	00	System Jitter	0.004528 ms
Stratum	2	Clock Jitter	0.004 ms
Log2 Precision	-19	Clock Wander	0.000 ppm
Root Delay	0.034 ms	Broadcast Delay	-50.000 ms
Root Dispersion	1.000 ms	Symm Auth Delay	0.000 ms
Packets Sent	149744		

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 restarts NTPd. This also clears the statistics and the graph.

The following table lists the descriptions of NTP Daemon Status and Control parameters.

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 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 always persists until at least one message is 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 (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 must 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 used 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, as the association with its state variables is created only when an NTP message arrives. Also, 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 can be used 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: • Warning: 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) 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 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 (SyncServer) is present, but that it has yet to validate its time from its time sources. Once 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 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, 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 not synchronized, 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 is 0, as 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 can 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 starts with a value of INIT (might be displayed as 73.78.73.84, the ASCII decimal values). Once a peer has been selected, the clock might be stepped, in which case the reference ID field changes to STEP (or 83.84.69.80). Once the PLL is locked, the stratum is updated and the reference ID identifies the selected peer. In the case of a SyncServer operating at stratum 1, the reference ID displays the source for the local timing reference (such as GNSS). In the case where the selected peer is another NTP server, the reference ID displays the IP address of the server or a hash unique to the association between SyncServer and the remote server.
Reference Time	The time when 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 (for example, GNSS and 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 SyncServer.

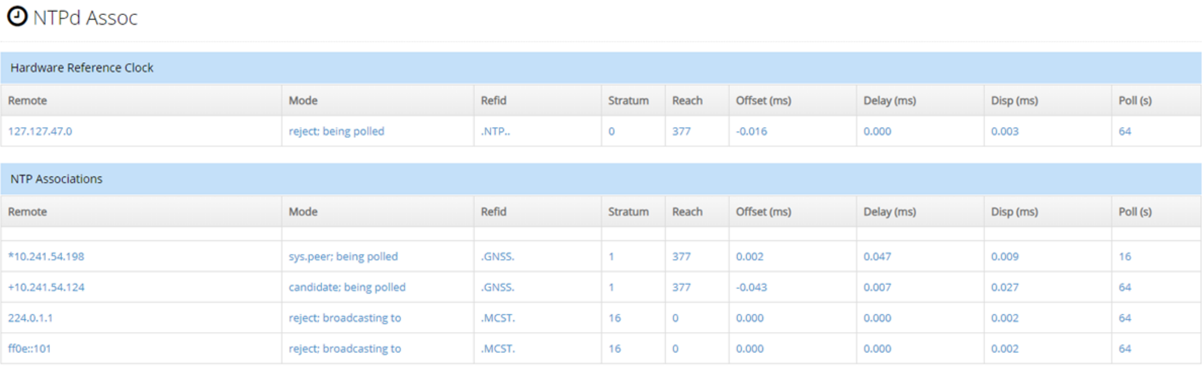
Note: If the system is using NTP as the reference and the NTP server is performing a leap smear, then all non-NTP outputs of the system are degraded, especially outputs that are present on the optional I/O modules.

5.2.2.2 NTP Associations

Use this window to view NTP associations.

The following table lists the descriptions of NTPd associations parameters.

Figure 5-19. NTPd Associations Window



NTPd Assoc

Hardware Reference Clock

Remote	Mode	Refid	Stratum	Reach	Offset (ms)	Delay (ms)	Disp (ms)	Poll (s)
127.127.47.0	reject: being polled	.NTP..	0	377	-0.016	0.000	0.003	64

NTP Associations

Remote	Mode	Refid	Stratum	Reach	Offset (ms)	Delay (ms)	Disp (ms)	Poll (s)
*10.241.54.198	sys.peer: being polled	.GNSS.	1	377	0.002	0.047	0.009	16
+10.241.54.124	candidate: being polled	.GNSS.	1	377	-0.043	0.007	0.027	64
224.0.1.1	reject: broadcasting to	.MCST.	16	0	0.000	0.000	0.002	64
ff0e::101	reject: broadcasting to	.MCST.	16	0	0.000	0.000	0.002	64

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 case of a remote NTP connection, this is 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 the system variables. However, the actual system synchronization is derived from a Pulse-Per-Second (PPS) signal, either indirectly through the PPS reference clock driver or directly through the Kernel interface.
Mode	This displays the `ntpq` tally code and the NTP association mode. Tally codes include `reject`, `falsetick`, `excess`, `outlyer`, `candidate`, `selected`, `sys.peer`, and `pps.peer`. More details for ntpq can be found on the Internet. NTP association modes include unspecified (`unspec`), symmetric active (`symmetric active`), symmetric passive (`symmetric passive`), client (`being polled`), server (`replying`), broadcast (`broadcasting to`), and broadcast client (`sending broadcasting`). For more details, see www.eecis.udel.edu/~mills/ntp/html/assoc.html.
Ref ID	This four-byte field is 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 starts with a value of INIT (might 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 changes to STEP (or 83.84.69.80). Once the PLL is locked, the stratum is updated and the reference ID identifies the selected peer. In the case of a SyncServer operating at stratum 1, the reference ID displays the source for the local timing reference (for example, GNSS, IRIG, and FREE). When the selected peer is another NTP server, the reference ID displays the IP address of the server or a hash unique to the association between SyncServer and the remote server.

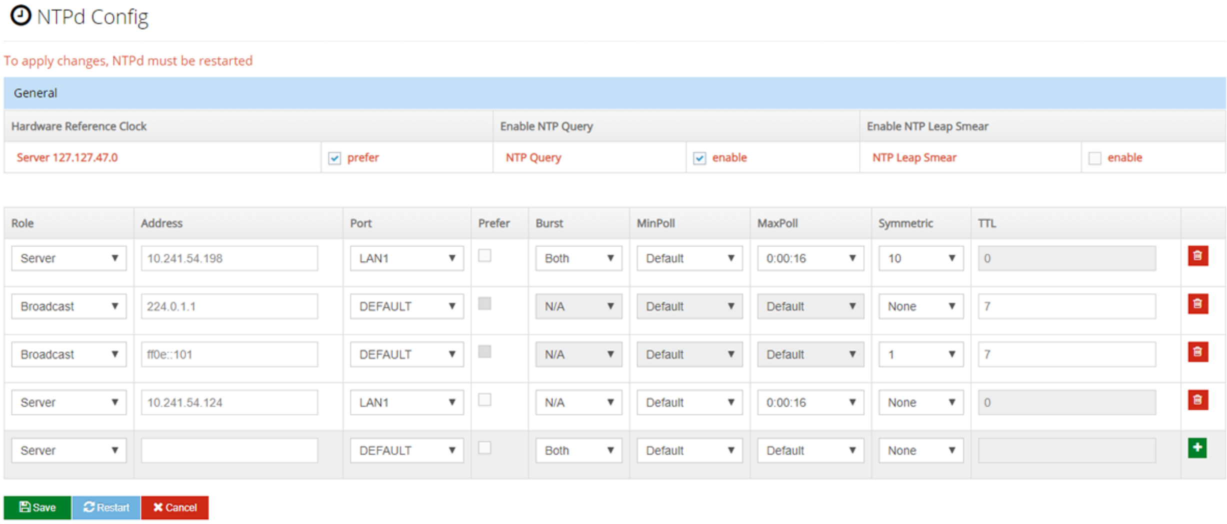
...........continued

Parameter	Description
Stratum	The stratum level of the remote clock is 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 SyncServer is one (Stratum 1).
Reach	This is an 8-bit shift register that keeps track of the last eight 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, and 377. If the value is not one of those just shown, then there might 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 SyncServer is a broadcast or multicast server.
Offset (ms)	The time offset between 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 milliseconds 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 SyncServer relative to the peer. They provide not only precision measurements of offset and delay, but also definitive maximum error bounds, so that 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.

5.2.2.3 NTP Configuration Window

This window is used to configure NTP parameters, including the Role (Server, Peer, or Broadcast), Address, and Port. Table 5-7 lists the descriptions of NTP configuration parameters.

Figure 5-20. NTP Configuration Window



NTPd Config

To apply changes, NTPd must be restarted

General

Hardware Reference Clock		Enable NTP Query		Enable NTP Leap Smear	
Server 127.127.47.0	☑ prefer	NTP Query	☑ enable	NTP Leap Smear	□ enable

Role	Address	Port	Prefer	Burst	MinPoll	MaxPoll	Symmetric	TTL	
Server	10.241.54.198	LAN1	□	Both	Default	0:00:16	10	0	
Broadcast	224.0.1.1	DEFAULT	□	N/A	Default	Default	None	7	
Broadcast	ff0e::101	DEFAULT	□	N/A	Default	Default	1	7	
Server	10.241.54.124	LAN1	□	N/A	Default	0:00:16	None	0	
Server		DEFAULT	□	Both	Default	Default	None		+

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

NTP Query Parameter: If the NTP Query checkbox is enabled, then SyncServer responds 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 SyncServer implements a UTC leap second smear function at any forthcoming UTC leap second event. The unit smears 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 server NTP clock and only affects the NTP responses for NTPd and NTP Reflector operations. It does not affect any other ToD functions, such as IRIG outputs, and so on. 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, 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 peers can synchronize to the node that has the best remaining reference.
	Broadcast: Creates a broadcast server association. When configured with a broadcast address (for example, 192.168.61.255), the association broadcasts NTP messages from the Network interface with the matching IP address (for example, 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”)
Prefer	The NTP daemon synchronizes with an association marked prefer over an equivalent association that is not. The internal hardware reference clock prefer setting can be cleared 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 of the operating scenarios, the local hardware reference clock (which often than tracks GNSS) is the only reference being used. With the Prefer being selected, and no statistically better reference available, the time server achieves 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 goes through a standard validation procedure for a reference clock. This procedure takes several minutes and must 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.

..........continued

Parameter	Description
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 must 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 (16s).
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 (1,024s), but can be increased to an upper limit of 17 (36.4h).
Symmetric	This option specifies an optional MD5 or SHA symmetric key ID. The MD5 key must be 20 characters. The SHA/SHA512 key must be 40 hex characters.
TTL	This field is used to specify the TTL in the IP header for broadcast packets. This controls 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, and 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 be either 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].

5.2.2.4 NTPd Most Recently Used (MRU) List Window

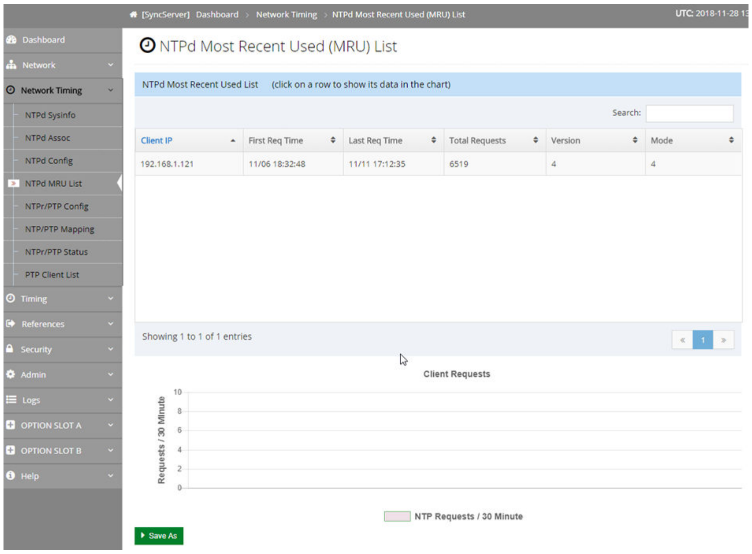
Use this window to display a list of the most recently used clients.

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 displays data for up to the last 24 hours.

Figure 5-21. NTP MRU List Window



NTPd Most Recent Used (MRU) List

NTPd Most Recent Used List (click on a row to show its data in the chart)

Client IP	First Req Time	Last Req Time	Total Requests	Version	Mode
192.168.1.121	11/06 18:32:48	11/11 17:12:35	6519	4	4

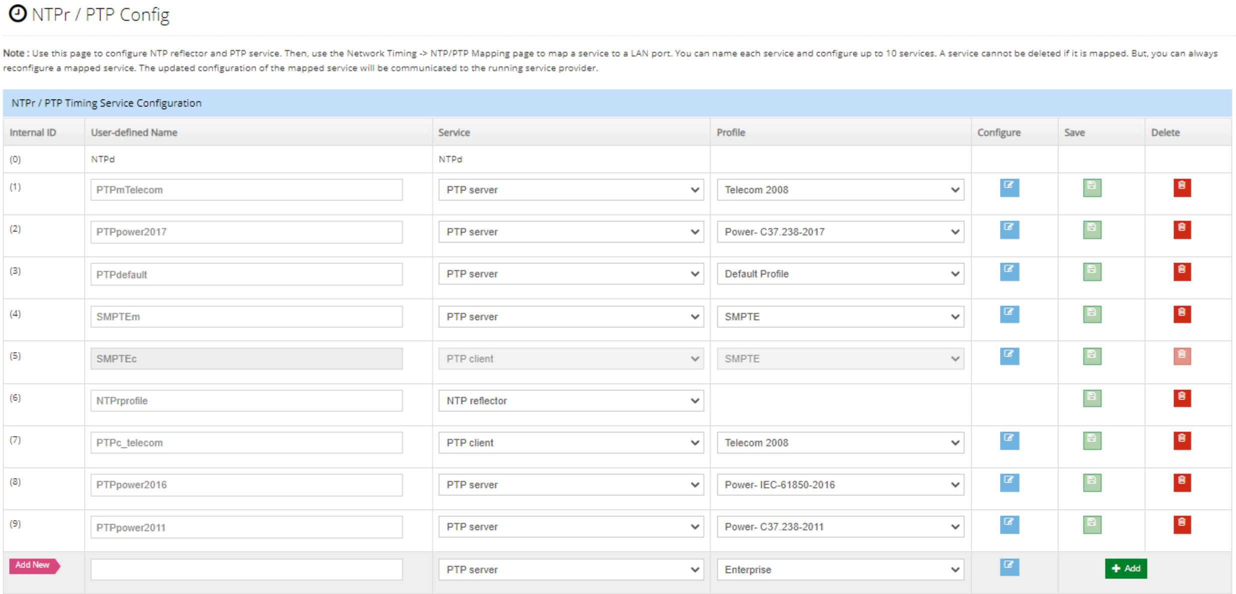
Showing 1 to 1 of 1 entries

5.2.2.5 NTP/PTP Services Configuration Window

Use this window to configure NTP reflector and PTP services.

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



NTPr / PTP Config

Note : Use this page to configure NTP reflector and PTP service. Then, use the Network Timing -> NTP/PTP Mapping page to map a service to a LAN port. You can name each service and configure up to 10 services. A service cannot be deleted if it is mapped. But, you can always reconfigure a mapped service. The updated configuration of the mapped service will be communicated to the running service provider.

NTPr / PTP Timing Service Configuration

Internal ID	User-defined Name	Service	Profile	Configure	Save	Delete
(0)	NTPd	NTPd				
(1)	PTPmTelecom	PTP server	Telecom 2008	✎	💾	🗑
(2)	PTPpower2017	PTP server	Power- C37.238-2017	✎	💾	🗑
(3)	PTPdefault	PTP server	Default Profile	✎	💾	🗑
(4)	SMPTEm	PTP server	SMPTE	✎	💾	🗑
(5)	SMPTEc	PTP client	SMPTE	✎	💾	🗑
(6)	NTPrprofile	NTP reflector			💾	🗑
(7)	PTPc_telecom	PTP client	Telecom 2008	✎	💾	🗑
(8)	PTPpower2016	PTP server	Power- IEC-61850-2016	✎	💾	🗑
(9)	PTPpower2011	PTP server	Power- C37.238-2011	✎	💾	🗑
Add New		PTP server	Enterprise	✎	+ Add	

Table 5-8. NTP/PTP Services Configuration Parameters

Parameter/Column	Description
Internal ID	S6x0 automatically assigns this number as a unique identifier to reference this specific timing service when it appears on other forms. The assigned values are 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. Though not preferred, 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 server. **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. Therefore, the best way to work with these three columns (Service, Profile, and 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 server (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 be 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	Saves the timing service configured on this row. This also saves the settings (if any) that are associated with Configure for this same row.
Delete	Removes the specific timing service configuration associated with this row. If the row being deleted is currently mapped for use on a physical port, then this action is not allowed. To remove, you must unmap it first on the Network Timing NTP/PTP Mapping form.

IEEE® 1588 2.1 must only be configured for the PTP server 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 only supports 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 does not respond to IPv4 NTP packets if the reflector is enabled for IPv6. The unit does 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 and 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 1 GbE 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 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 following table lists the primary trade-offs.

Figure 5-23. NTP Packet Reflector

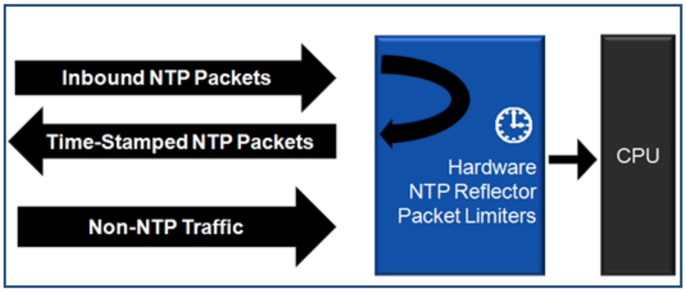


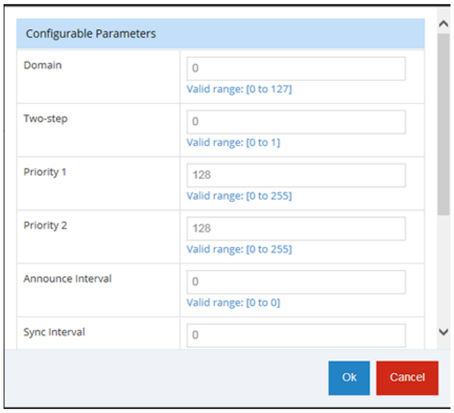
Table 5-9. NTP Reflector vs. NTP Daemon Performance Trade-Offs

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

Important: 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 do 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 notifies 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 is disabled for up to 15 seconds. During this time, the traffic is forwarded to the CPU. If the traffic rate exceeds the all-packets threshold, then the traffic is dropped and an alarm is generated.

Figure 5-24. PTP Configuration Parameters



Configurable Parameters

Domain	0 Valid range: [0 to 127]
Two-step	0 Valid range: [0 to 1]
Priority 1	128 Valid range: [0 to 255]
Priority 2	128 Valid range: [0 to 255]
Announce Interval	0 Valid range: [0 to 0]
Sync Interval	0

For a list of PTP parameters, including default value and range, see Table 9-43 to Table 9-64.

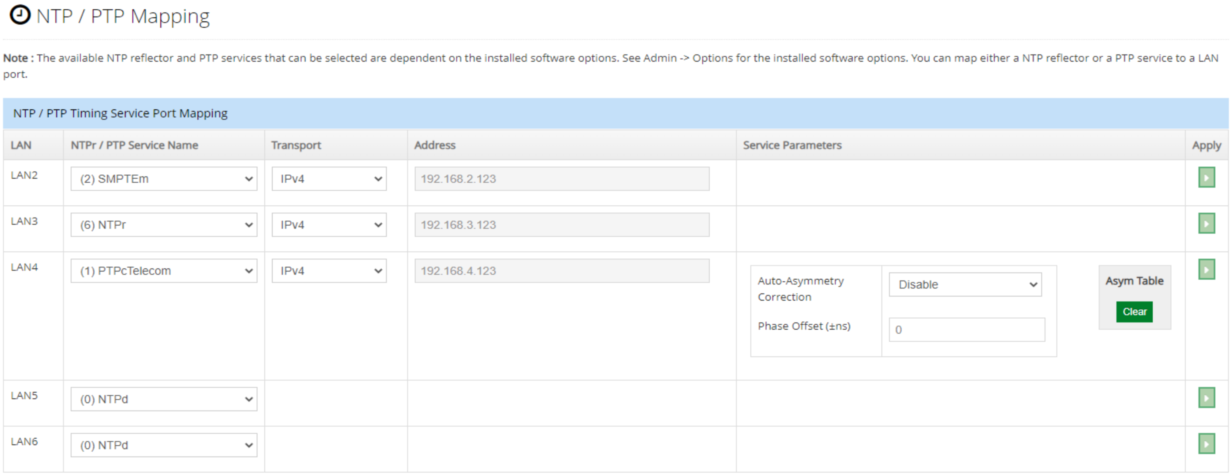
5.2.2.6 NTP/PTP Mapping Window

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

The NTP Reflector and PTP capability are 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 server and the PTP client in the SyncServer. If asymmetry correction is enabled without GPS, then the PTP client only adjusts the system frequency and does not adjust the system time. Calibration takes one to two hours.

Figure 5-25. NTP/PTP Mapping Window



NTP / PTP Mapping

Note : The available NTP reflector and PTP services that can be selected are dependent on the installed software options. See Admin -> Options for the installed software options. You can map either a NTP reflector or a PTP service to a LAN port.

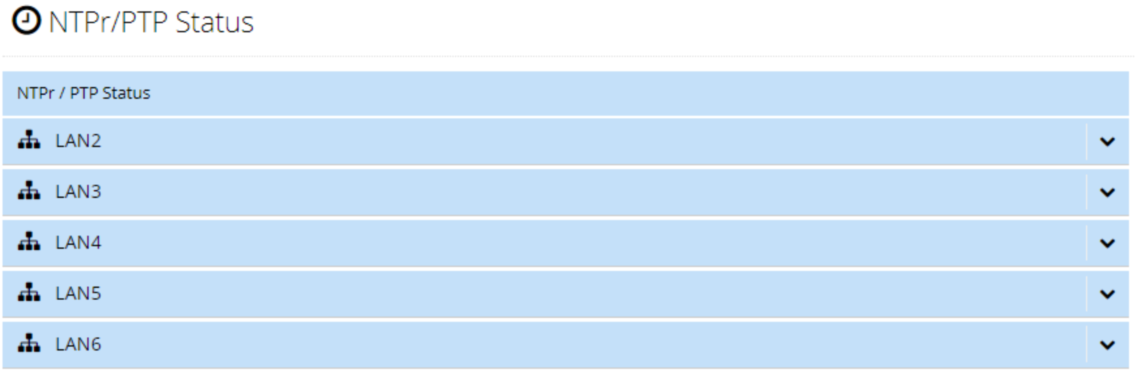
NTP / PTP Timing Service Port Mapping

LAN	NTPr / PTP Service Name	Transport	Address	Service Parameters	Apply
LAN2	(2) SMPTEm	IPv4	192.168.2.123		▶
LAN3	(6) NTPr	IPv4	192.168.3.123		▶
LAN4	(1) PTPcTelecom	IPv4	192.168.4.123	Auto-Asymmetry Correction: Disable Phase Offset (±ns): 0 Asym Table: Clear	▶
LAN5	(0) NTPd				▶
LAN6	(0) NTPd				▶

5.2.2.7 NTPr/PTP Status Window

This window displays the status of ports with NTP reflector or PTP service.

Figure 5-26. NTPr/PTP Status Window

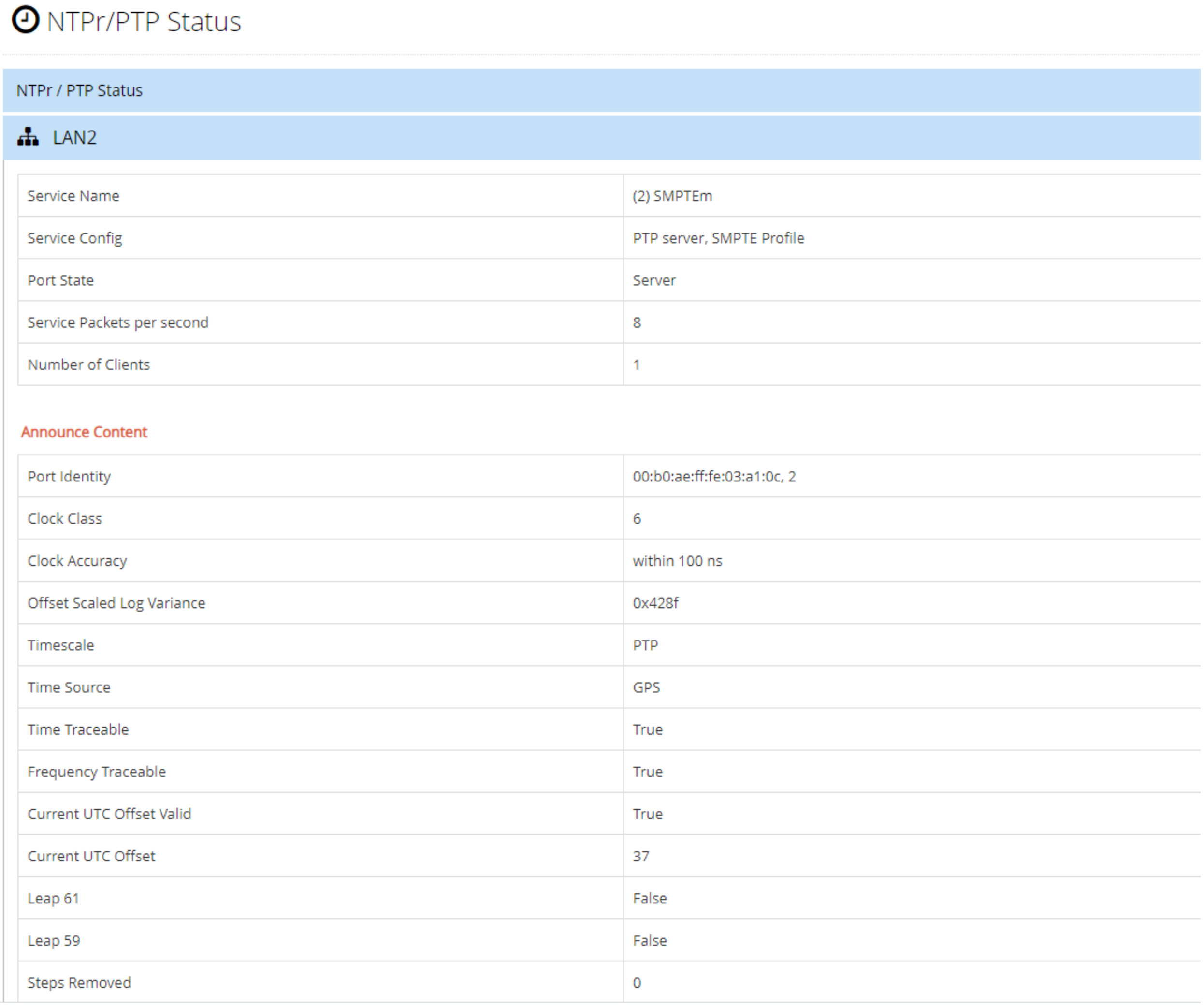


NTPr/PTP Status

NTPr / PTP Status

- LAN2
- LAN3
- LAN4
- LAN5
- LAN6

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



NTPr/PTP Status

NTPr / PTP Status

LAN2

Service Name	(2) SMPTEm
Service Config	PTP server, SMPTE Profile
Port State	Server
Service Packets per second	8
Number of Clients	1

Announce Content

Port Identity	00:b0:ae:ff:fe:03:a1:0c, 2
Clock Class	6
Clock Accuracy	within 100 ns
Offset Scaled Log Variance	0x428f
Timescale	PTP
Time Source	GPS
Time Traceable	True
Frequency Traceable	True
Current UTC Offset Valid	True
Current UTC Offset	37
Leap 61	False
Leap 59	False
Steps Removed	0

5.2.2.7.1 FPP Metrics for PTP Client Status

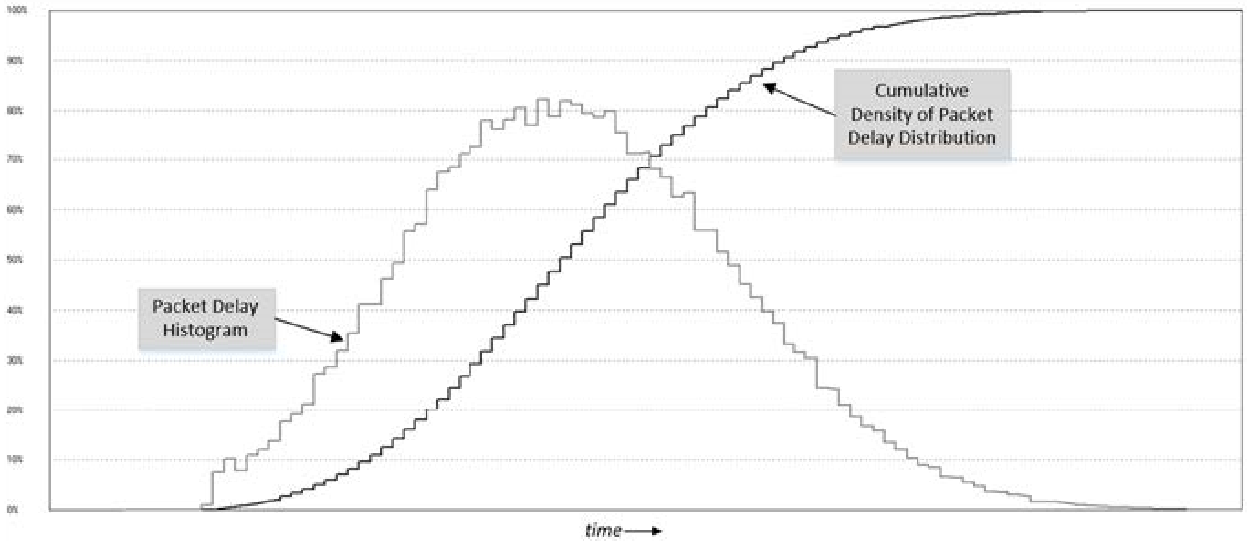
Several metrics are displayed for a port operating as a PTP client.

Forward Event packets provide the rate at which sync packets are received. Reverse Event packets provides the rate at which delay response packets are received.

The cluster width for Foor Packet Percentage 1 (FPP1) and FPP2 are set with the other PTP client configuration parameters on the NTPr/PTP Config page.

FPP is a standard measure defined in ITU G.8261.1-2012. The overall concept: As the variation of packet-delay increases (for example, a population of packet transit times from device A to device B), the potential to derive a given level of sync from that flow decreases. The following figure shows the first steps toward obtaining an FPP measure in a simple manner.

Figure 5-28. Overlay Of Probability Distribution Of Packet-Delay And CDF Of Same Distribution

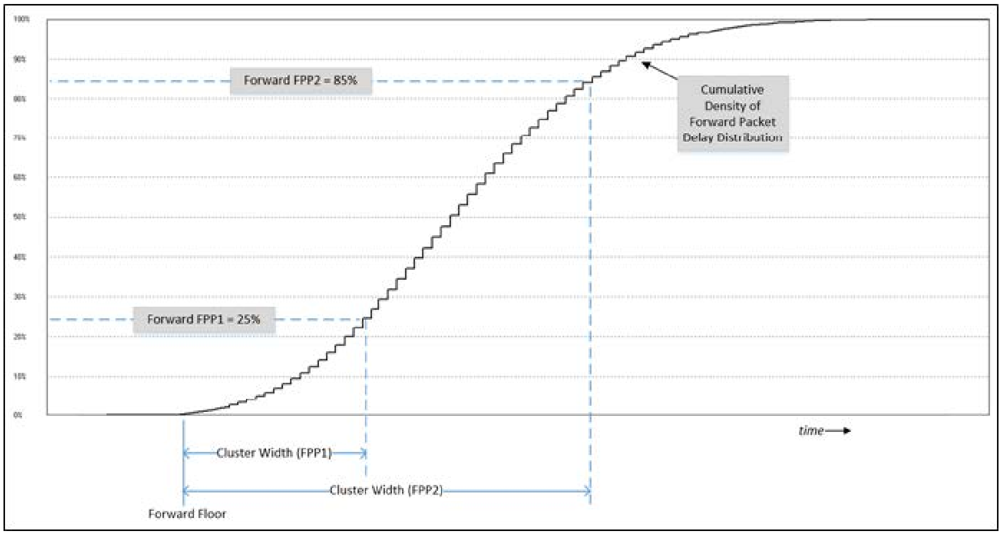


The Packet Delay Histogram graph represents a population of packet transit times taken over some duration. X-axis is the packet transit time (longer transit to the right) and y-axis is the number of packets that exhibited that transit time. The plot is essentially a Probability Density Function (PDF) of the transit times of the packets. From the PDF, a Cumulative Density Function (CDF) can be derived by integrating and normalizing. The result is also shown in the preceding figure. The y-axis labels on the plot are appropriate for any CDF, ranging from 0% to 100% (sometimes, a CDF is shown to range from 0–1). This plot shows, at any place on the x-axis, the percentage of the packet-delay population that had a shorter (or equal) transit time vs. this x-axis value.

Working from the CDF, the following figure shows how the FPP-related metric configurations relate to the FPP result. For this example, the distribution is associated with the forward-flow direction. By convention, this is based on the T1 to T2 (PTP master to PTP client) flow. T1 is the timestamp of a Sync packet originating in the PTP master, T2 is the timestamp of that same packet upon arrival at the PTP monitored input on SyncServer.

The impact of the Cluster Width controls on the FPP metric is evident in the following figure. These values define the time-interval into the CDF (from the "floor") at which the FPP% must be determined. For the example shown, the Forward FPP1% is approximately 25% and FPP2% is approximately 85%. For FPP1 for this observation, 25% of the forward timestamp pairs occurred within the FPP1 defined cluster width of the forward floor.

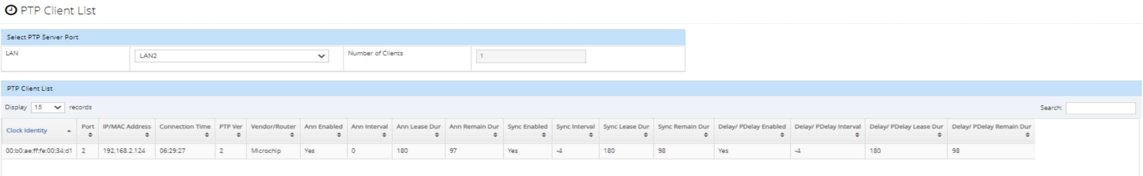
Figure 5-29. Obtaining FPP From Cumulative Density Function



5.2.2.8 PTP Client List Window

This window displays the list of PTP clients and client details. The PTP client list is useful for initial PTP network setup, to assure that expected PTP clients are connected to expected SyncServer LAN port(s), and to check that the PTP client settings from one location. The PTP client list is not available for the Enterprise profile in the Multicast mode.

Figure 5-30. PTP Client List Window



PTP Client List

Select PTP Server Port

LAN: LAN2 | Number of Clients: 1

PTP Client List

Display 15 records | Search:

Clock Identity	Port	IP/MAC Address	Connection Time	PTP Ver	Vendor/Router	Ann Enabled	Ann Interval	Ann Lease Dur	Ann Remain Dur	Sync Enabled	Sync Interval	Sync Lease Dur	Sync Remain Dur	Delay/ PDelay Enabled	Delay/ PDelay Interval	Delay/ PDelay Lease Dur	Delay/ PDelay Remain Dur
00:b0:ae:ff:fe:00:34:d1	2	192.168.2.124	06:29:27	2	Microchip	Yes	0	180	97	Yes	-4	180	98	Yes	-4	180	98

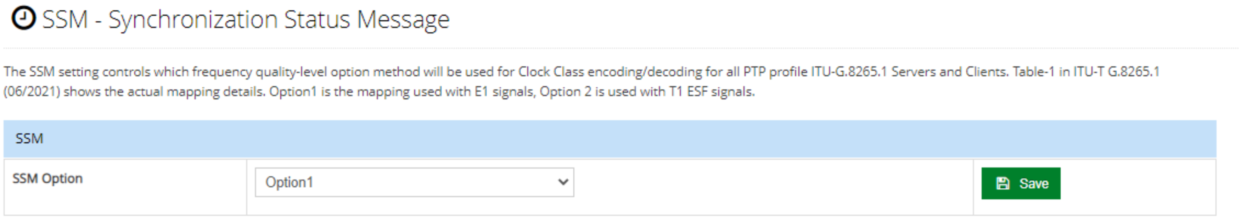
Client details displayed include the following:

- 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

5.2.2.9 SSM Window

This window allows configuration of the frequency quality-level option that is used for Clock Class encoding/decoding for all PTP profile ITU-G.8265.1 Servers and Clients. Table 1 in ITU-T G.8265.1 lists the actual mapping details. Option1 is the mapping used with E1 signals and Option 2 is used with T1 ESF signals.

Figure 5-31. SSM Window



SSM - Synchronization Status Message

The SSM setting controls which frequency quality-level option method will be used for Clock Class encoding/decoding for all PTP profile ITU-G.8265.1 Servers and Clients. Table-1 in ITU-T G.8265.1 (06/2021) shows the actual mapping details. Option1 is the mapping used with E1 signals, Option 2 is used with T1 ESF signals.

SSM

SSM Option: Option1

5.2.3 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: SyncServer 6x0 does not contain a battery-backed real-time clock. Therefore, it always boots up with a default value for the system time. This time is 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 is used for the first log entries when booting up the unit. The time changes to local time during the boot-up process if a time zone has been configured.

The system monitors all inputs and determines if there is a valid signal on each input. The system only uses one reference at a time. The highest priority valid input is used. This is specified on the Timing->Input Control page. Each reference has a different priority—the slot A and slot B references 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.

5.2.3.1 Timing—Input Control Window

This window enables external time and frequency references, and manually sets the time when no external time reference is 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.

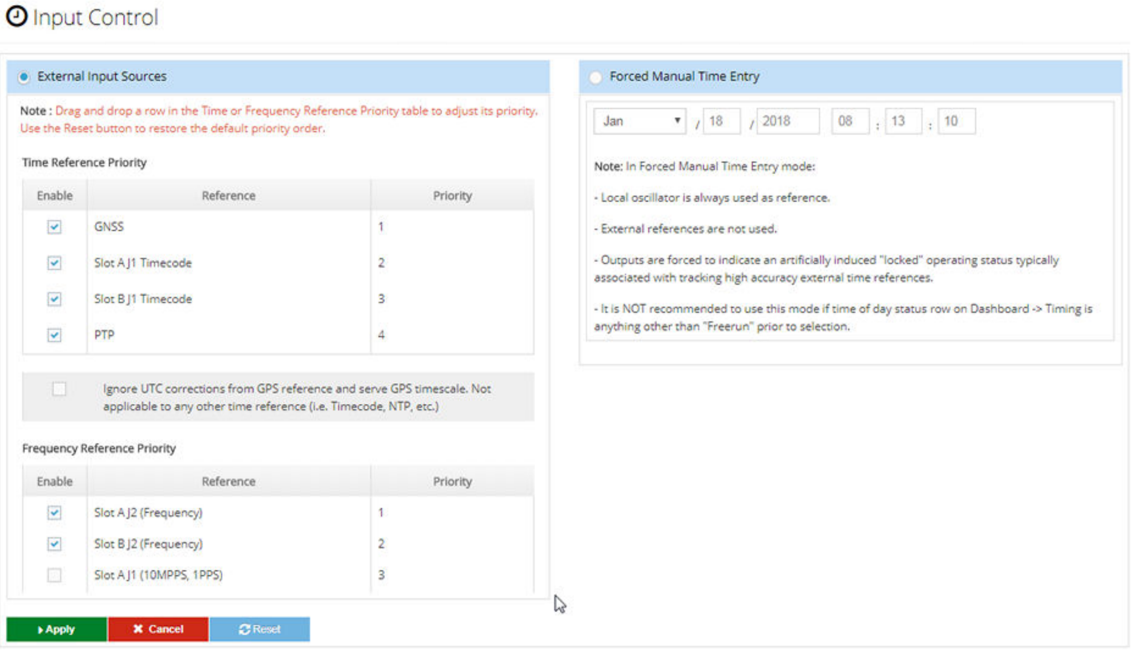
Use this window to manually set the IRIG input year, UTC offset from TAI, and Leap Second Notification. See 6.5. Provisioning Inputs with Manual Entry Controls for details.

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

Note: If “Forced Manual Time Entry” is selected on the Input Control form (while ToD status = Freerun), or if time is set from front-panel, then the unit might 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 SyncServer S6x0 is rebooted when leaving manual Time mode.

Figure 5-32. Timing-Input Control Window—Upper Portion



Input Control

● External Input Sources

Note : Drag and drop a row in the Time or Frequency Reference Priority table to adjust its priority. Use the Reset button to restore the default priority order.

Time Reference Priority

Enable	Reference	Priority
☑	GNSS	1
☑	Slot A J1 Timecode	2
☑	Slot B J1 Timecode	3
☑	PTP	4

□ Ignore UTC corrections from GPS reference and serve GPS timescale. Not applicable to any other time reference (i.e. Timecode, NTP, etc.)

Frequency Reference Priority

Enable	Reference	Priority
☑	Slot A J2 (Frequency)	1
☑	Slot B J2 (Frequency)	2
□	Slot A J1 (10MPPS, 1PPS)	3

○ Forced Manual Time Entry

Jan / 18 / 2018 08 : 13 : 10

Note: In Forced Manual Time Entry mode:

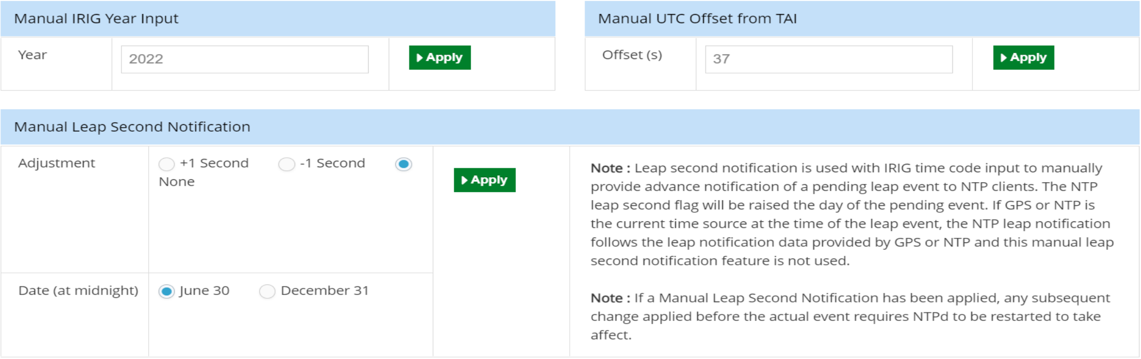
- Local oscillator is always used as reference.

- External references are not used.

- Outputs are forced to indicate an artificially induced "locked" operating status typically associated with tracking high accuracy external time references.

- It is NOT recommended to use this mode if time of day status row on Dashboard -> Timing is anything other than "Freerun" prior to selection.

Figure 5-33. Timing-Input Control Window—Lower Portion



Manual IRIG Year Input

Year: 2022

Manual UTC Offset from TAI

Offset (s): 37

Manual Leap Second Notification

Adjustment: ○ +1 Second ○ -1 Second ● None

Date (at midnight): ● June 30 ○ December 31

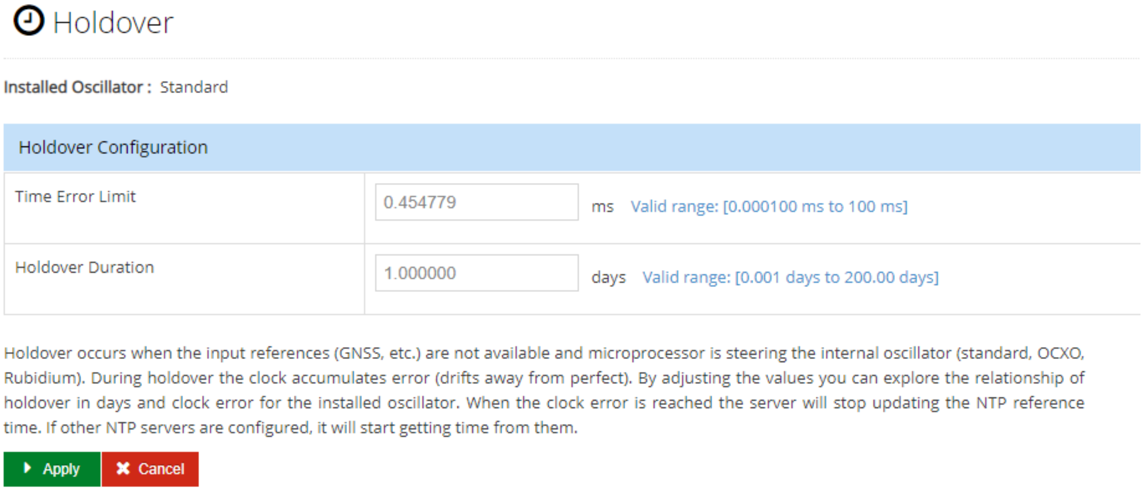
Note : Leap second notification is used with IRIG time code input to manually provide advance notification of a pending leap event to NTP clients. The NTP leap second flag will be raised the day of the pending event. If GPS or NTP is the current time source at the time of the leap event, the NTP leap notification follows the leap notification data provided by GPS or NTP and this manual leap second notification feature is not used.

Note : If a Manual Leap Second Notification has been applied, any subsequent change applied before the actual event requires NTPd to be restarted to take affect.

5.2.3.2 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, the unit attempts to lock to external NTP servers.

Figure 5-34. Timing—Holdover Window



Holdover

Installed Oscillator : Standard

Holdover Configuration

Time Error Limit	0.454779 ms Valid range: [0.000100 ms to 100 ms]
Holdover Duration	1.000000 days Valid range: [0.001 days to 200.00 days]

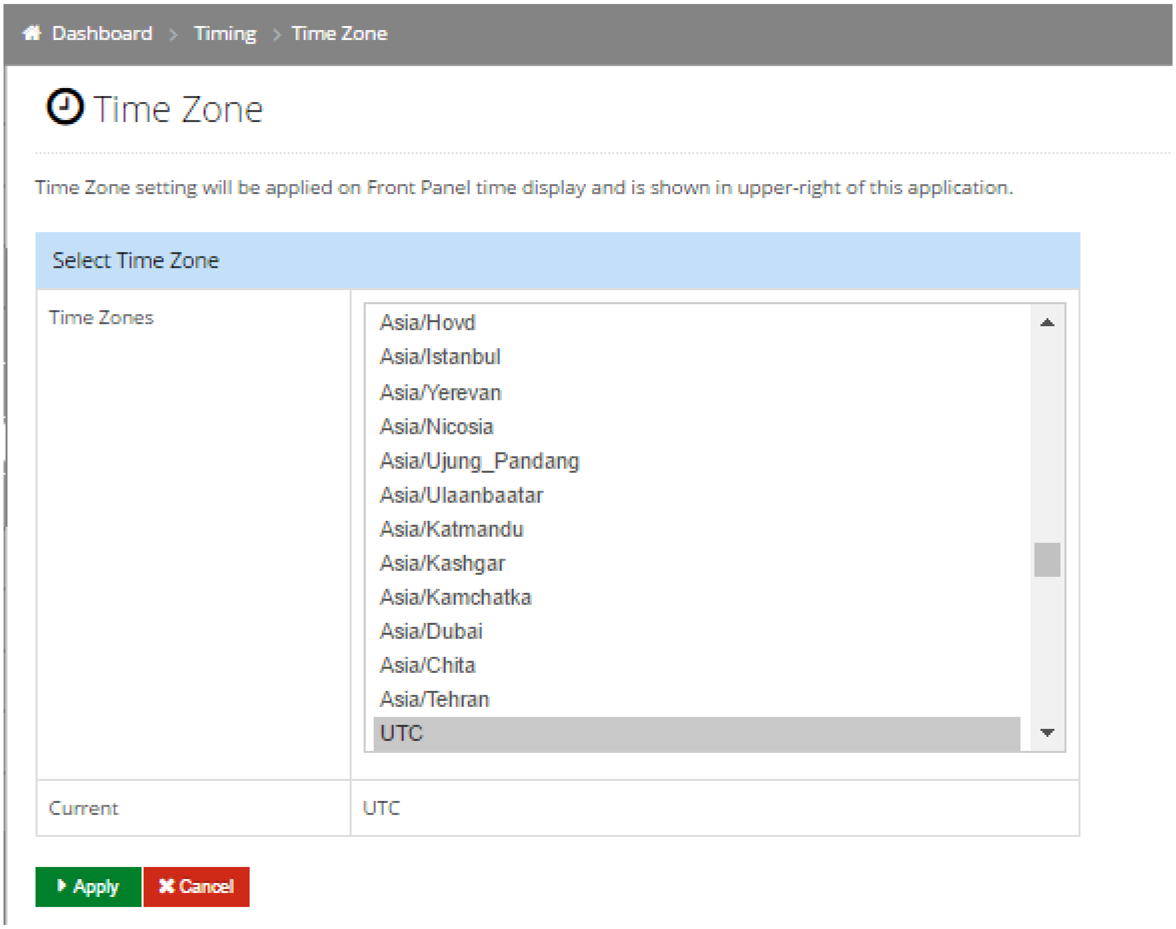
Holdover occurs when the input references (GNSS, etc.) are not available and microprocessor is steering the internal oscillator (standard, OCXO, Rubidium). During holdover the clock accumulates error (drifts away from perfect). By adjusting the values you can explore the relationship of holdover in days 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 start getting time from them.

Holdover occurs when the input references (GNSS, and so on) are not available and microprocessor is steering the internal oscillator (standard, OCXO, and 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 stops updating the NTP reference time. If other NTP servers are configured, then it starts getting time from other NTP servers. The value obtained with this estimator is a conservative estimate of the performance of the unit. Actual performance might vary and is typically better than the estimate.

5.2.3.3 Timing—Time Zone Configuration Window

This window selects the desired time zone for SyncServer S6x0. The time zone is only for the front panel display. NTP time continues to be served in UTC.

Figure 5-35. Timing—Time Zone Window



Time Zone

Time Zone setting will be applied on Front Panel time display and is shown in upper-right of this application.

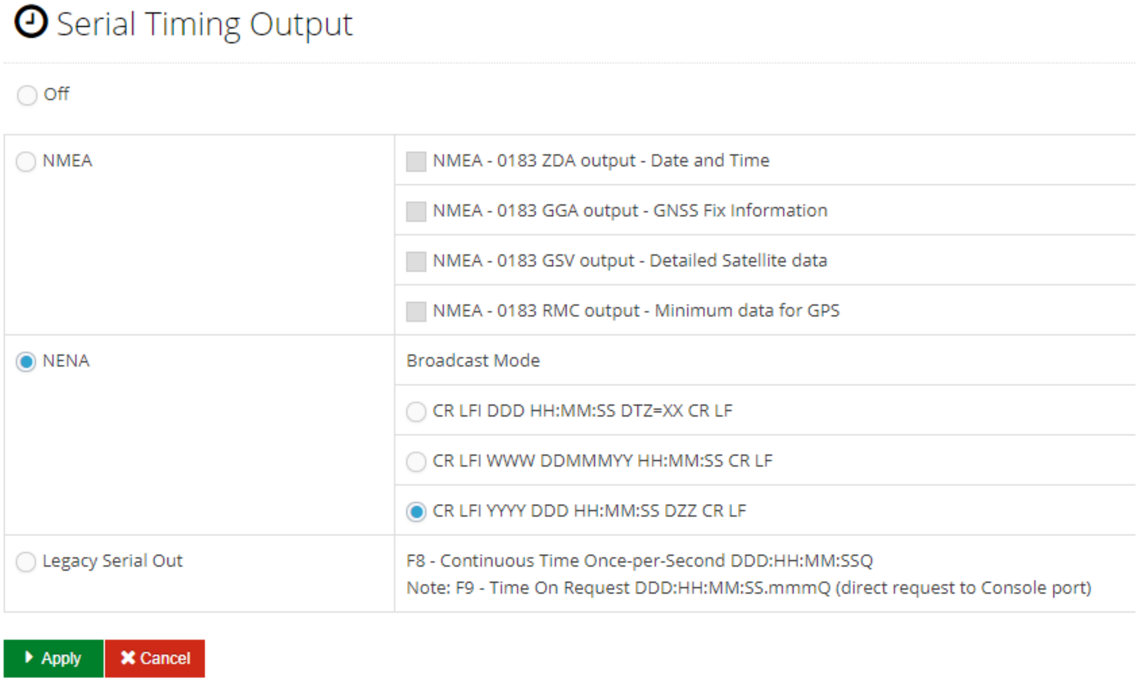
Select Time Zone

Time Zones	Asia/Hovd Asia/Istanbul Asia/Yerevan Asia/Nicosia Asia/Ujung_Pandang Asia/Ulaanbaatar Asia/Katmandu Asia/Kashgar Asia/Kamchatka Asia/Dubai Asia/Chita Asia/Tehran UTC
Current	UTC

5.2.3.4 Timing—Serial Output Configuration Window

This window selects the format for the serial timing output for SyncServer S6x0.

Figure 5-36. Timing—Serial Output Window



Serial Timing Output

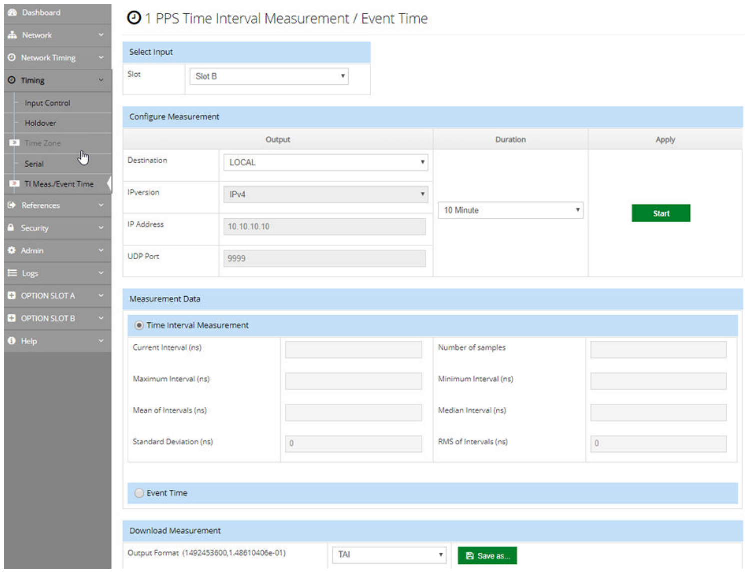
○ Off

○ NMEA	□ NMEA - 0183 ZDA output - Date and Time
	□ NMEA - 0183 GGA output - GNSS Fix Information
	□ NMEA - 0183 GSV output - Detailed Satellite data
	□ NMEA - 0183 RMC output - Minimum data for GPS
● NENA	Broadcast Mode
	○ CR LFI DDD HH:MM:SS DTZ=XX CR LF
	○ CR LFI WWW DDMMMYY HH:MM:SS CR LF
	● CR LFI YYYY DDD HH:MM:SS DZZ CR LF
○ Legacy Serial Out	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)

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

This window sets up 1 PPS time interval measurements and event time. See section 6.9. Making Time-Interval or Event Timestamp Measurements for details on using this feature.

Figure 5-38. 1 PPS Time Interval Measurement/Event Time Window



1 PPS Time Interval Measurement / Event Time

Select Input

Slot: Slot B

Configure Measurement

Output		Duration	Apply
Destination	LOCAL	10 Minute	Start
IPversion	IPv4		
IP Address	10.10.10.10		
UDP Port	9999		

Measurement Data

● Time Interval Measurement

Current Interval (ns)		Number of samples	
Maximum Interval (ns)		Minimum Interval (ns)	
Mean of Intervals (ns)		Median Interval (ns)	
Standard Deviation (ns)	0	RMS of Intervals (ns)	0

○ Event Time

Download Measurement

Output Format (1492453600,1.48610406e-01): TAI

5.2.3.5.1 Requirements

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

5.2.3.5.2 Capabilities

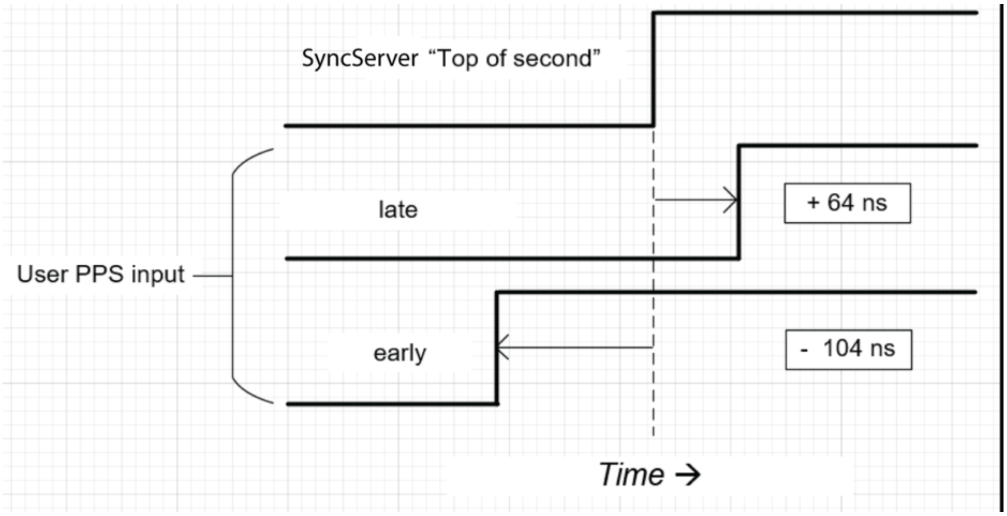
- Make measurements on a 1 PPS signal connected to J1 port of either module A or module B. Measures the rising edge of the signal compared to SyncServer system time.

- 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 at sourceforge.net/. 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 …`

    Notes:
    - The 1 PPS input must be disabled on the `Timing->Input control` page. The measurement is not useful if SyncServer is using 1 PPS as the reference.
    - Measurements are not useful if the SyncServer system clock is not set or is changing. Therefore, it is not recommended to use the measurement feature when SyncServer is in Warmup, Free-run, or Locking Clock states.
    - If the user 1 PPS input is later than the internal 1 PPS, then the measurement is positive. If the user 1 PPS is early, then the measurement result is negative, as shown in the following figure.
    - Input LOS alarms can be generated if the input is slower than 1 PPS. Microchip recommends disabling the LOS alarm actions on the `Admin->Alarms` page under this condition.

Figure 5-39. Time-Interval Measurement (Conceptual)



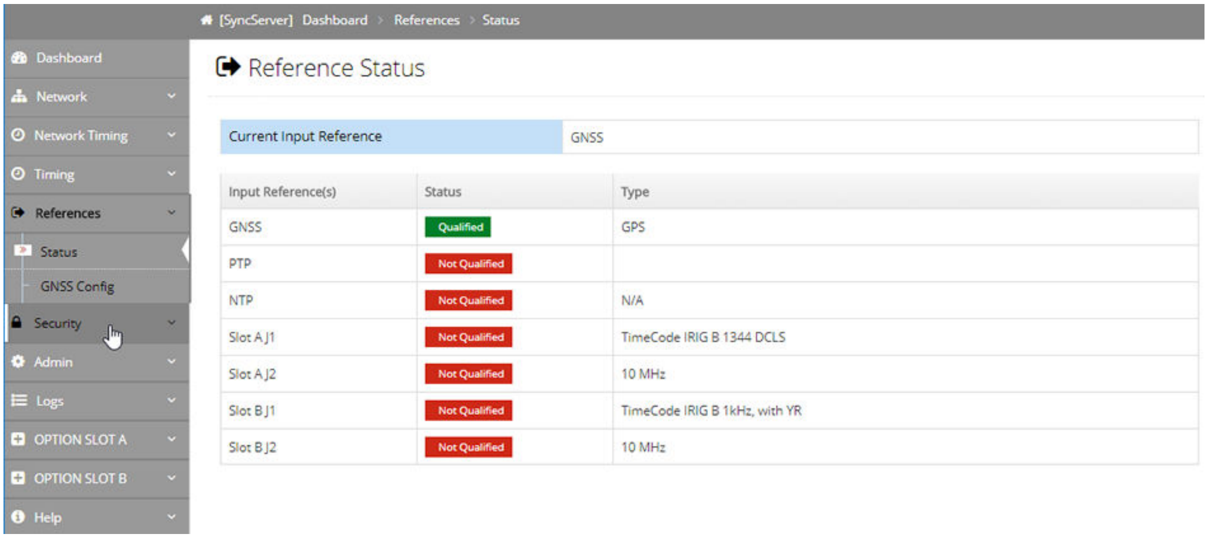
5.2.4 References Configuration Window

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

5.2.4.1 References—Reference Status Window

Use this window to view status information for system references.

Figure 5-40. References—Status Window



Reference Status

Current Input Reference	GNSS

Input Reference(s)	Status	Type
GNSS	Qualified	GPS
PTP	Not Qualified	
NTP	Not Qualified	N/A
Slot A J1	Not Qualified	TimeCode IRIG B 1344 DCLS
Slot A J2	Not Qualified	10 MHz
Slot B J1	Not Qualified	TimeCode IRIG B 1kHz, with YR
Slot B J2	Not Qualified	10 MHz

5.2.4.2 References—Reference GNSS Window

This window configures GNSS position and operating mode.

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 might take an extended period before the change is fully incorporated.

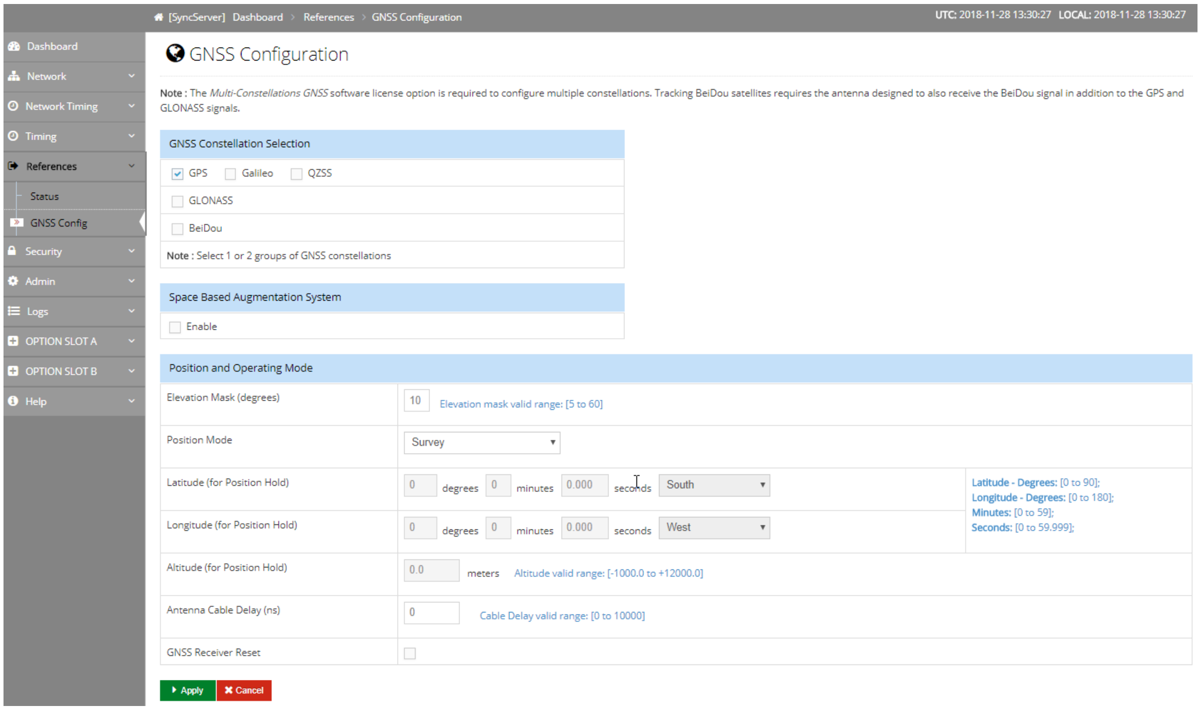
If the GNSS multi-constellation license is installed, then GPS, GLONASS, Galileo, QZSS, and BeiDou can be selected. Only one or two of the constellations groups can be selected. GPS, Galileo, and QZSS are considered part of one constellation group, and all can be selected together as one of the two available 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 that SyncServer S6x0 automatically surveys the position and then transitions 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 SyncServer S6x0. The position needs to be accurately determined to avoid creating timing errors.
- Dynamic means that SyncServer S6x0 continuously determines 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/s. For Seaborne, vertical velocity is assumed to be zero, and maximum horizontal velocity is 25 m/s. For Airborne, maximum horizontal velocity is 500 m/s and maximum vertical velocity is 100 m/s. For unpressurized airborne applications, the maximum operational altitude for the product is 25,000 ft (7620 m).

Figure 5-41. References—GNSS Window



GNSS Configuration

Note : The *Multi-Constellations GNSS* software license option is required to configure multiple constellations. Tracking BeiDou satellites requires the antenna designed to also receive the BeiDou signal in addition to the GPS and GLONASS signals.

GNSS Constellation Selection

☑ GPS ☐ Galileo ☐ QZSS

☐ GLONASS

☐ BeiDou

Note : Select 1 or 2 groups of GNSS constellations

Space Based Augmentation System

☐ Enable

Position and Operating Mode		
Elevation Mask (degrees)	10 Elevation mask valid range: [5 to 60]	
Position Mode	Survey ▾	

Latitude (for Position Hold)	0 degrees 0 minutes 0.000 seconds South ▾	**Latitude - Degrees:** [0 to 90];
		Longitude - Degrees: [0 to 180];
		Minutes: [0 to 59];
		Seconds: [0 to 59.999];

Longitude (for Position Hold)	0 degrees 0 minutes 0.000 seconds West ▾	
Altitude (for Position Hold)	0.0 meters Altitude valid range: [-1000.0 to +12000.0]	
Antenna Cable Delay (ns)	0 Cable Delay valid range: [0 to 10000]	
GNSS Receiver Reset	☐	

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 does 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.

5.2.5 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.

5.2.5.1 Security—Users Window

Use this window to add or delete users, and for Password Maintenance, as shown in Figure 5-42. All users and administrators have the same privileges.

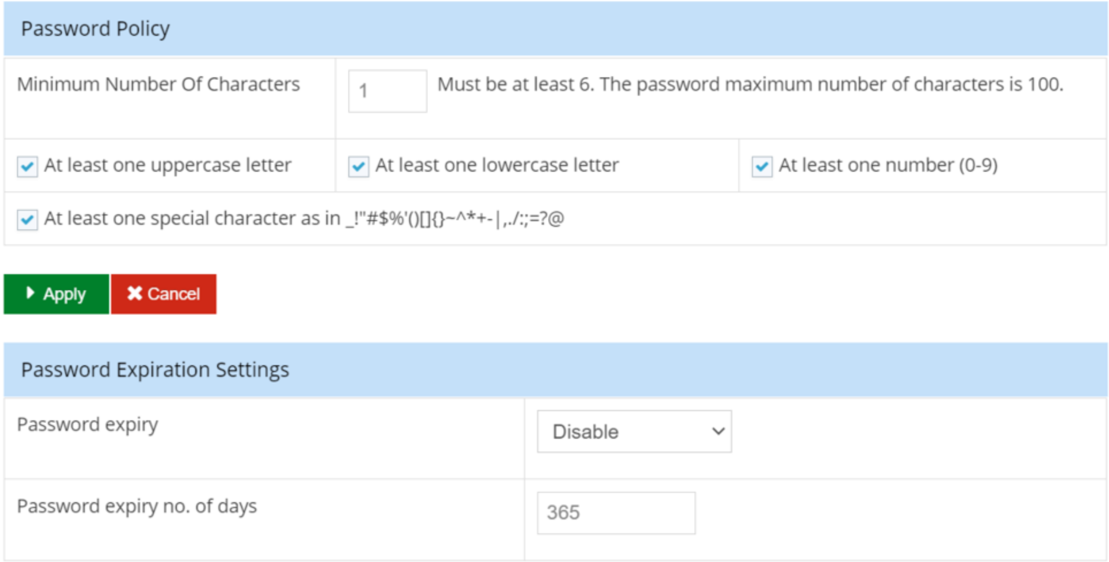
The top section allows configuration of the password policy. The minimum length and the types of characters (uppercase, lowercase, number, and special) that must be in the password can be configured.

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. User names must start with an alpha character.
  - abcdefghijklmnopqrstuvwxyz
  - 0123456789
  - _
- The following characters are not allowed for the password:
  (', “, <, >, &,), and $.
- The following characters are allowed for the password:
  - 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 5-42. Users Configuration Window—Upper Portion



Password Policy

Minimum Number Of Characters: 1 — Must be at least 6. The password maximum number of characters is 100.

☑ At least one uppercase letter ☑ At least one lowercase letter ☑ At least one number (0-9)

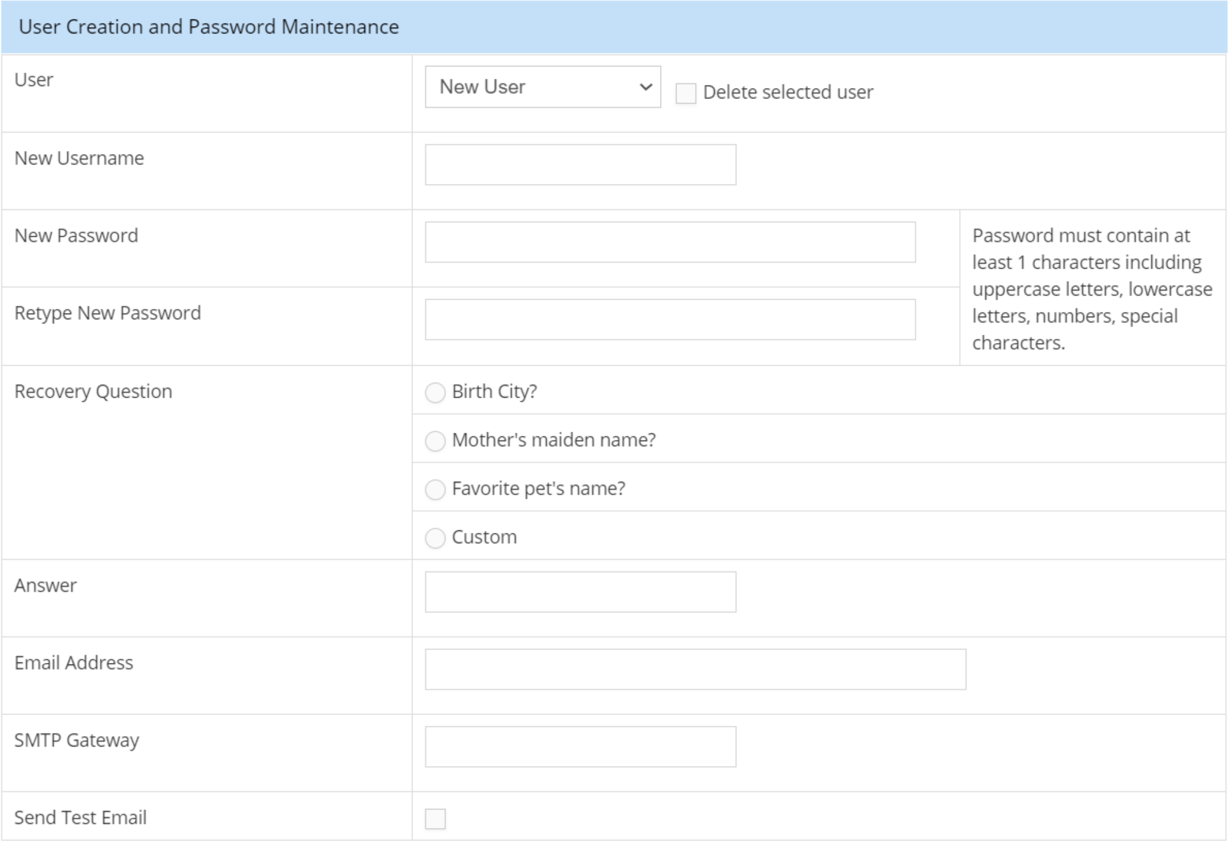
☑ At least one special character as in _!"#$%'()[]{}~^*+-|,./:;=?@

Password Expiration Settings

Password expiry: Disable

Password expiry no. of days: 365

Figure 5-43. Users Configuration Window—Lower Portion



User Creation and Password Maintenance

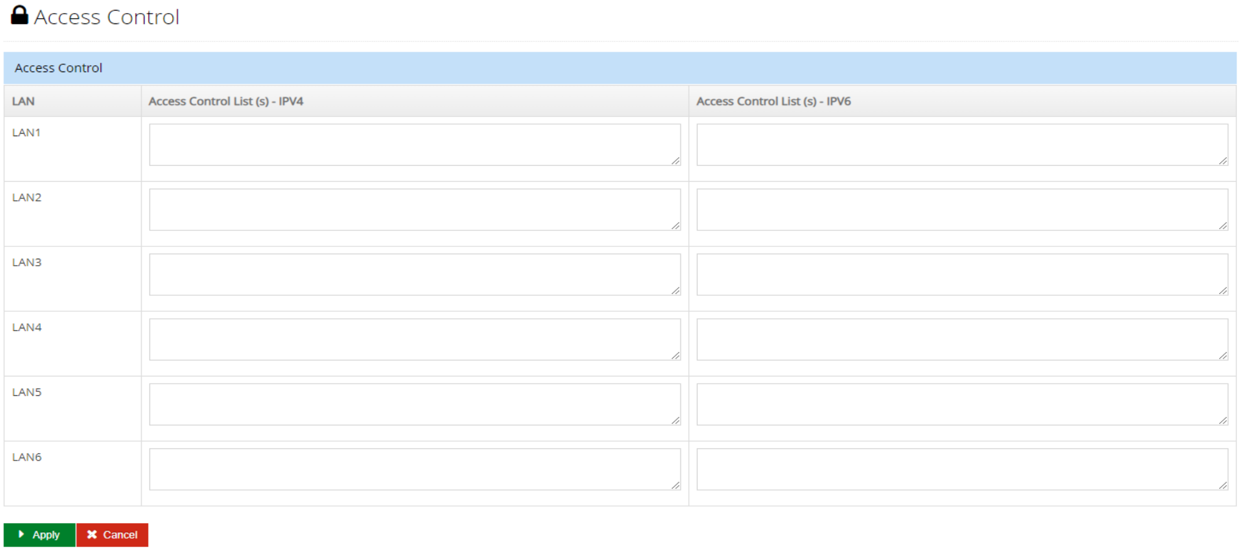
User	New User ▾ □ Delete selected user	
New Username		
New Password		Password must contain at least 1 characters including uppercase letters, lowercase letters, numbers, special characters.
Retype New Password		
Recovery Question	○ Birth City? ○ Mother's maiden name? ○ Favorite pet's name? ○ Custom	
Answer		
Email Address		
SMTP Gateway		
Send Test Email	□	

5.2.5.2 Security—Access Control Configuration Window

Use this window to configure access control for LAN1–LAN6 (whitelist). If nothing is configured, then the unit accepts data from all devices. If any addresses are configured, only packets from those devices are accepted. Each field supports a maximum of 1000 characters. Enter IP addresses separated by a comma, as shown in the following figure.

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

Figure 5-44. Security—Access Control Configuration Window



Access Control

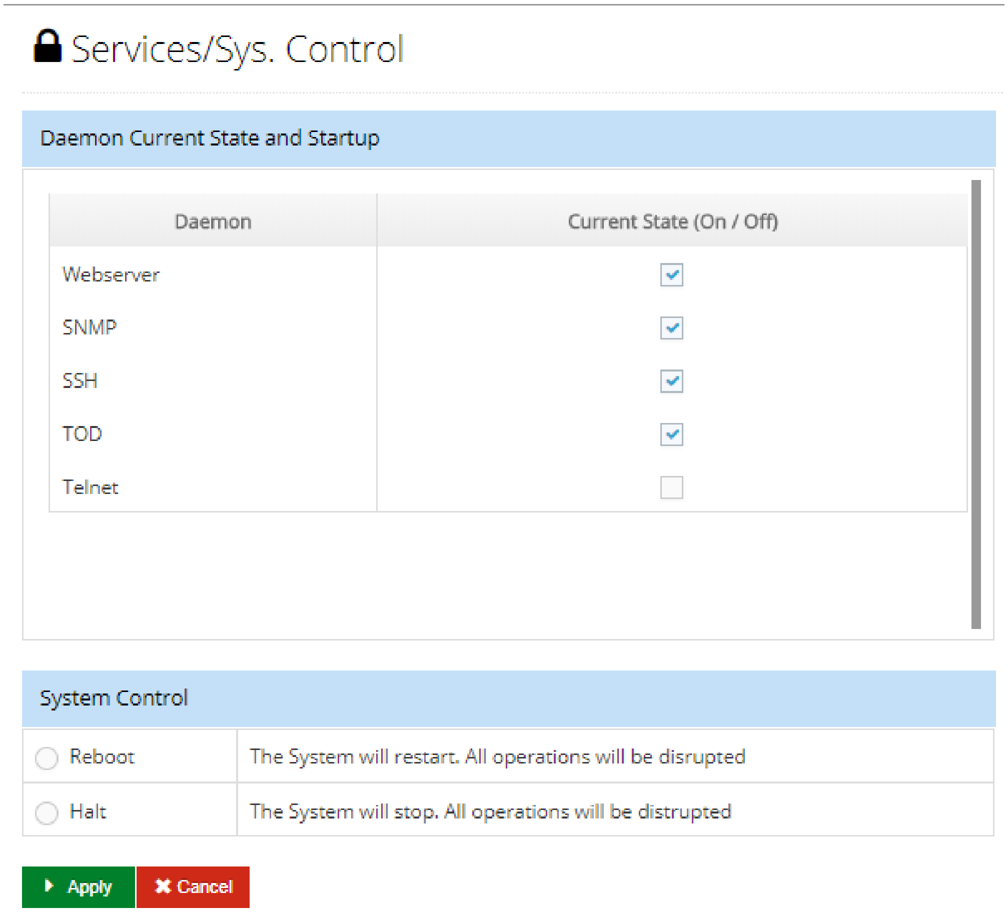
Access Control

LAN	Access Control List (s) - IPV4	Access Control List (s) - IPV6
LAN1		
LAN2		
LAN3		
LAN4		
LAN5		
LAN6		

5.2.5.3 Security—Services and 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.

Figure 5-45. Security—Services and System Control Configuration Window



Services/Sys. Control

Daemon Current State and Startup

Daemon	Current State (On / Off)
Webserver	☑
SNMP	☑
SSH	☑
TOD	☑
Telnet	□

System Control

○ Reboot	The System will restart. All operations will be disrupted
○ Halt	The System will stop. All operations will be distrupted

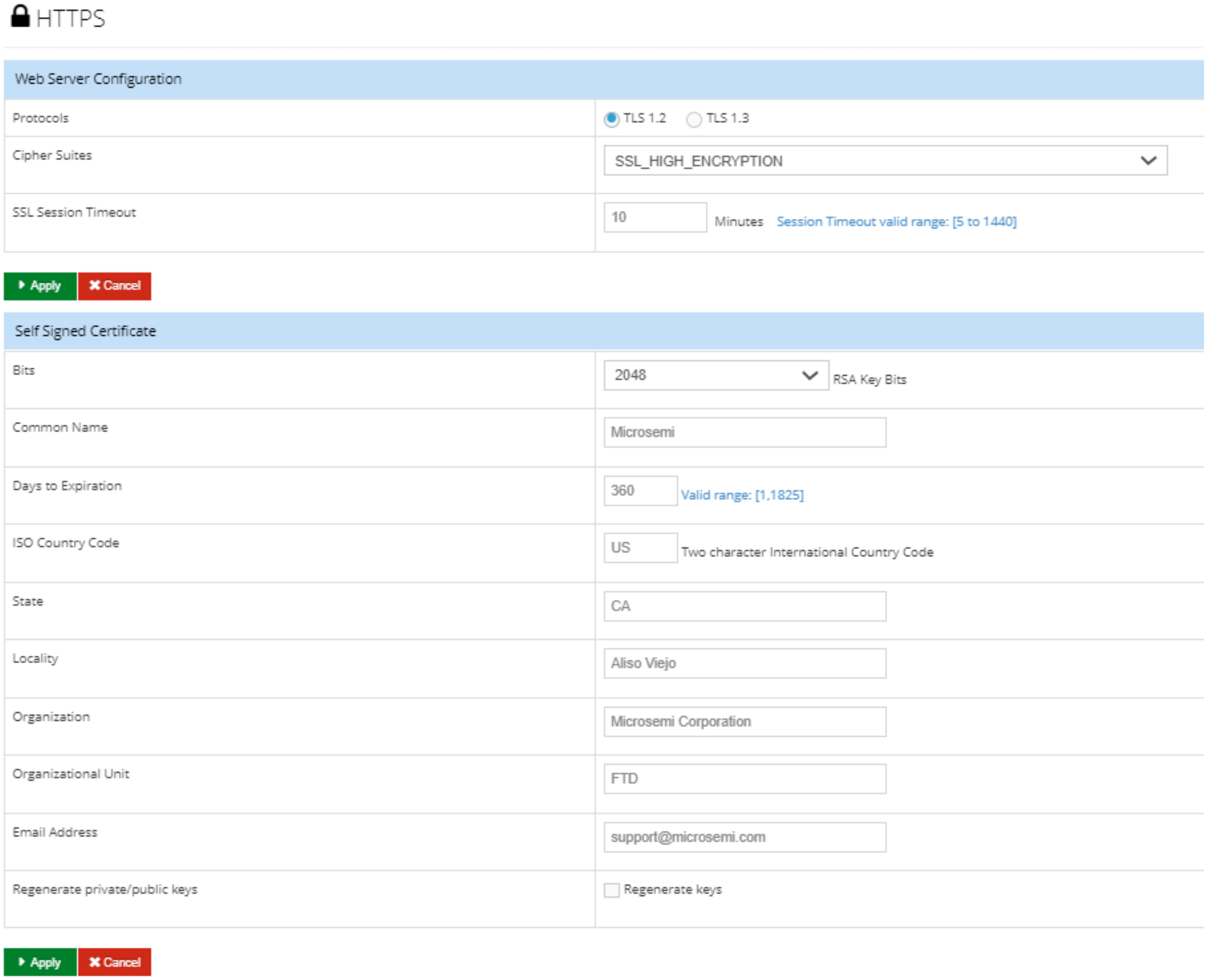
5.2.5.4 Security—HTTPS Configuration Window

This window configures the web server. It can also be used to configure a self-signed certificate. However, this must only be configured on this page if the security license is not installed. If the security license is installed, then use the X.509 SS Cert and X.509 mapping pages. This page updates the "System default certificate".

Number of allowed characters:

- Common name: 1–63 characters
- State: 1–63 characters
- Locality: 1–63 characters
- Organization: 1–63 characters

Figure 5-46. Security—HTTPS Configuration Window



HTTPS

Web Server Configuration

Protocols	● TLS 1.2 ○ TLS 1.3
Cipher Suites	SSL_HIGH_ENCRYPTION
SSL Session Timeout	10 Minutes Session Timeout valid range: [5 to 1440]

Self Signed Certificate

Bits	2048 RSA Key Bits
Common Name	Microsemi
Days to Expiration	360 Valid range: [1,1825]
ISO Country Code	US Two character International Country Code
State	CA
Locality	Aliso Viejo
Organization	Microsemi Corporation
Organizational Unit	FTD
Email Address	support@microsemi.com
Regenerate private/public keys	□ Regenerate keys

Table 5-10. Supported HTTPS Protocols

Model	TLS 1.1	TLS 1.2	TLS 1.3
SyncServer S600	—	x	x
SyncServer S650	—	x	x

Table 5-11. HTTPS Configuration Parameters

Parameter/Column	Description
Protocols	TLS 1.2 or TLS 1.3

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

Parameter/Column	Description
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 removes ciphers that are deemed to be less secure.

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).
Email Address	Email address associated with company

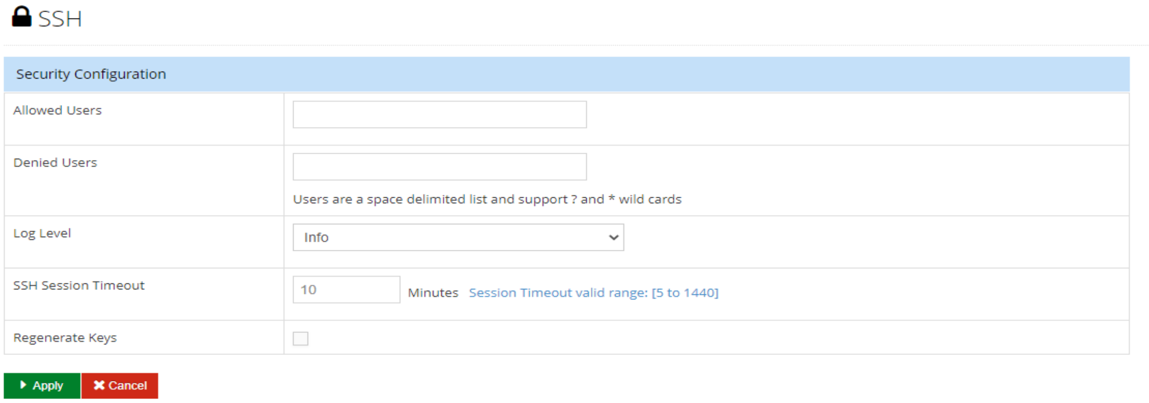
Regenerate keys—check this box to regenerate the public/private keys.

Note: If the security license is installed, Microchip recommends using the X.509 SS Cert and X.509 Mapping pages instead of this page for configuring a self-signed certificate.

5.2.5.5 Security—SSH Configuration Window

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

Figure 5-47. Security—SSH Configuration Window



SSH

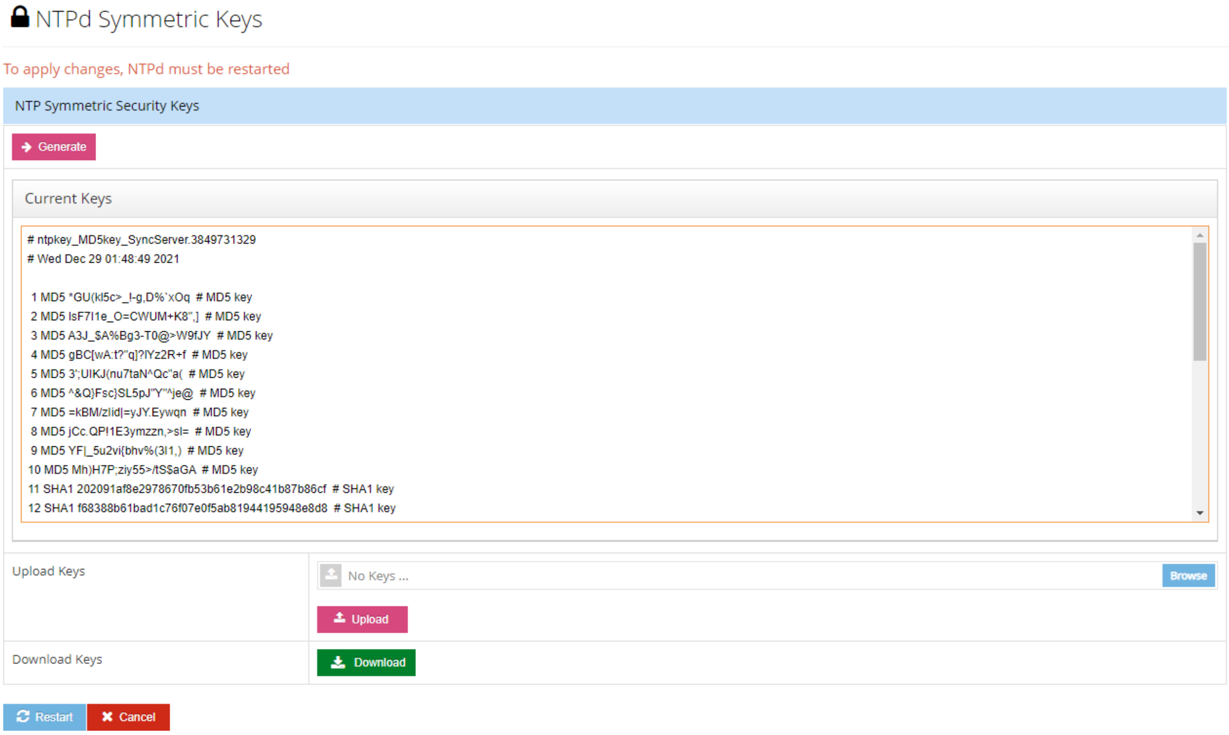
Security Configuration

Allowed Users	
Denied Users	Users are a space delimited list and support ? and * wild cards
Log Level	Info
SSH Session Timeout	10 Minutes Session Timeout valid range: [5 to 1440]
Regenerate Keys	□

5.2.5.6 Security—NTPd Symmetric Keys Configuration Window

Use this window to generate, upload and download NTP Symmetric Security keys. MD5 keys must be 20 characters long. SHA/SHA512 keys must be 40 hex characters.

Figure 5-48. Security—NTPd Symmetric Keys Window



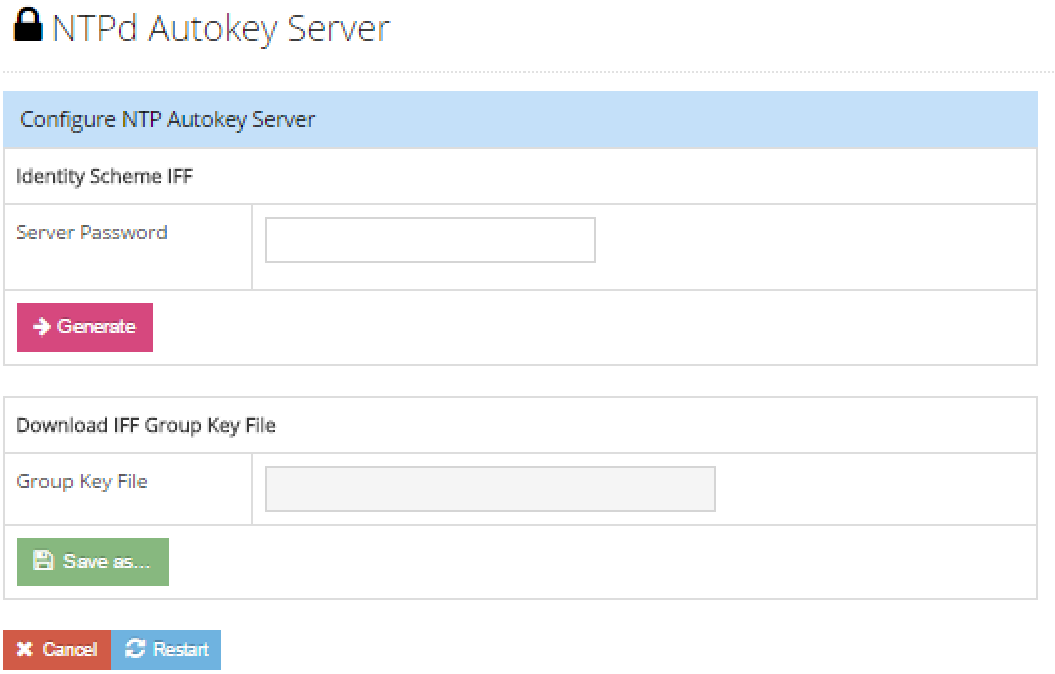
```
# ntpkey_MD5key_SyncServer.3849731329
# Wed Dec 29 01:48:49 2021

 1 MD5 *GU(kl5c>_!-g,D%`xOq  # MD5 key
 2 MD5 IsF7I1e_O=CWUM+K8",]  # MD5 key
 3 MD5 A3J_$A%Bg3-T0@>W9fJY  # MD5 key
 4 MD5 gBC[wA:t?"q]?IYz2R+f  # MD5 key
 5 MD5 3';UIKJ(nu7taN^Qc"a(  # MD5 key
 6 MD5 ^&Q}Fsc}SL5pJ"Y"^je@  # MD5 key
 7 MD5 =kBM/zIid|=yJY.Eywqn  # MD5 key
 8 MD5 jCc.QP!1E3ymzzn,>sl=  # MD5 key
 9 MD5 YF|_5u2vi{bhv%(3I1,)  # MD5 key
10 MD5 Mh)H7P;ziy55>/tS$aGA  # MD5 key
11 SHA1 202091af8e2978670fb53b61e2b98c41b87b86cf  # SHA1 key
12 SHA1 f68388b61bad1c76f07e0f5ab81944195948e8d8  # SHA1 key
```

5.2.5.7 Security—NTPd Autokey Server Configuration Window

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

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

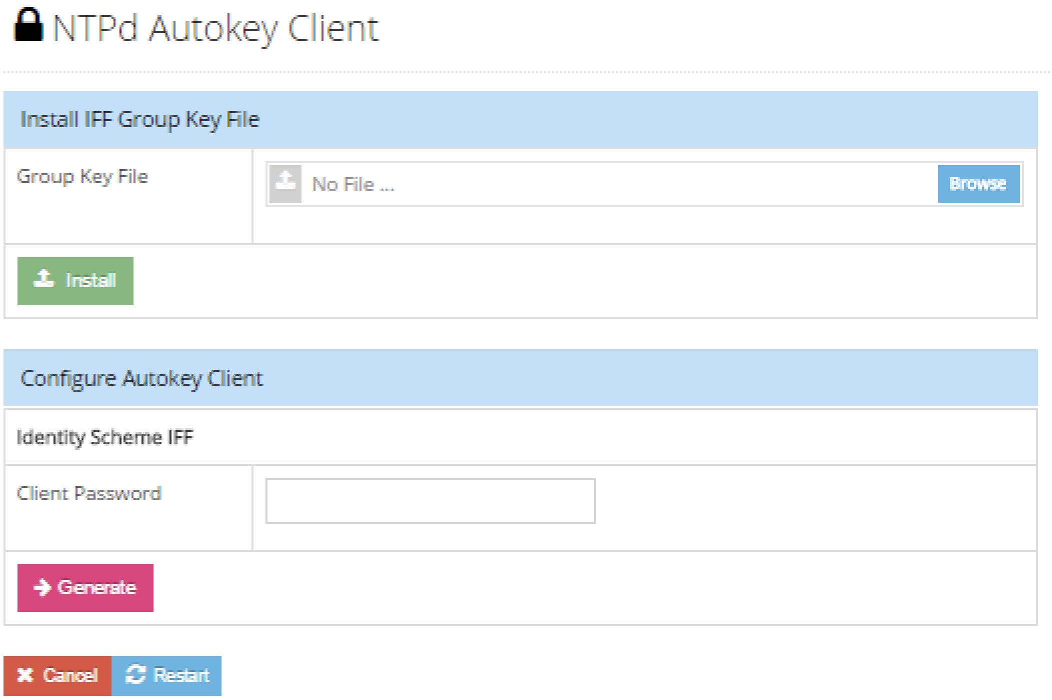
Figure 5-49. Security— NTPd Autokey Server Configuration Window



5.2.5.8 Security—NTPd Autokey Client Configuration Window

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

Figure 5-50. Security—NTPd Autokey Client Configuration Window



NTPd Autokey Client

Install IFF Group Key File

Group Key File: No File ...

Configure Autokey Client

Identity Scheme IFF

Client Password

5.2.5.9 Security—RADIUS Configuration Window

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

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 can login to SyncServer. If the authentication fails, then SyncServer continues its local authentication using the local users list.

Notes:

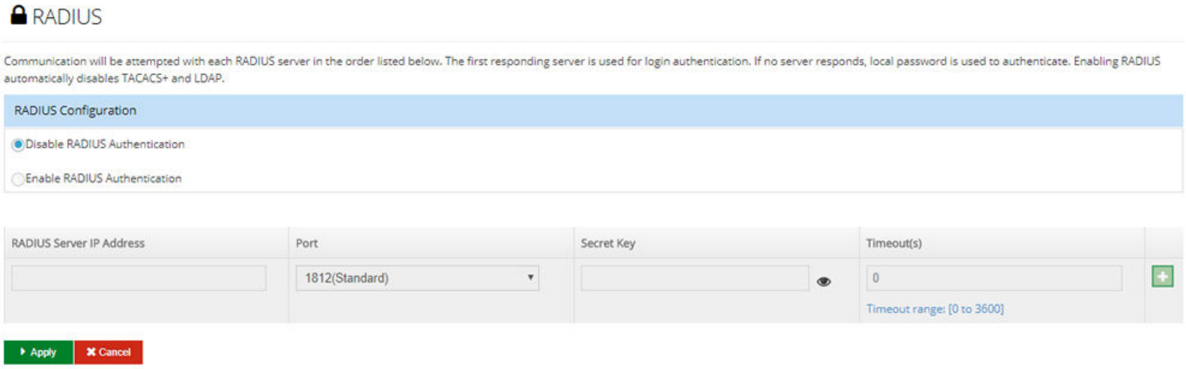
- RADIUS key: 1–16 characters
- Most RADIUS servers do not accept the # and ' characters for the key.

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.

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.

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 5-51. Security—RADIUS Configuration Window



RADIUS

Communication will be attempted with each RADIUS server in the order listed below. The first responding server is used for login authentication. If no server responds, local password is used to authenticate. Enabling RADIUS automatically disables TACACS+ and LDAP.

RADIUS Configuration

● Disable RADIUS Authentication

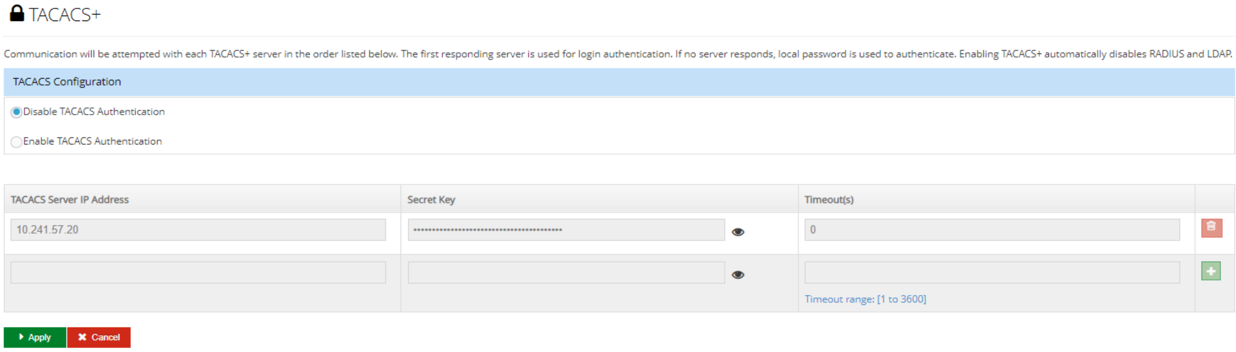
○ Enable RADIUS Authentication

RADIUS Server IP Address	Port	Secret Key	Timeout(s)	
	1812(Standard)		0 Timeout range: [0 to 3600]	+

5.2.5.10 Security—TACACS+ Configuration Window

Use this window to enable and configure TACACS+ authentication. Up to five TACACS+ servers can be configured. After entering the TACACS+ information, click the green **+** icon to add the row. Then, click the **Save** icon to save the information.

Figure 5-52. Security—TACACS+ Configuration Window



TACACS+

Communication will be attempted with each TACACS+ server in the order listed below. The first responding server is used for login authentication. If no server responds, local password is used to authenticate. Enabling TACACS+ automatically disables RADIUS and LDAP.

TACACS Configuration

● Disable TACACS Authentication

○ Enable TACACS Authentication

TACACS Server IP Address	Secret Key	Timeout(s)	
10.241.57.20	••	0	🗑
		Timeout range: [1 to 3600]	+

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. When a server successfully 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. SyncServer local authentication happens at the end.

Notes:

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

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).

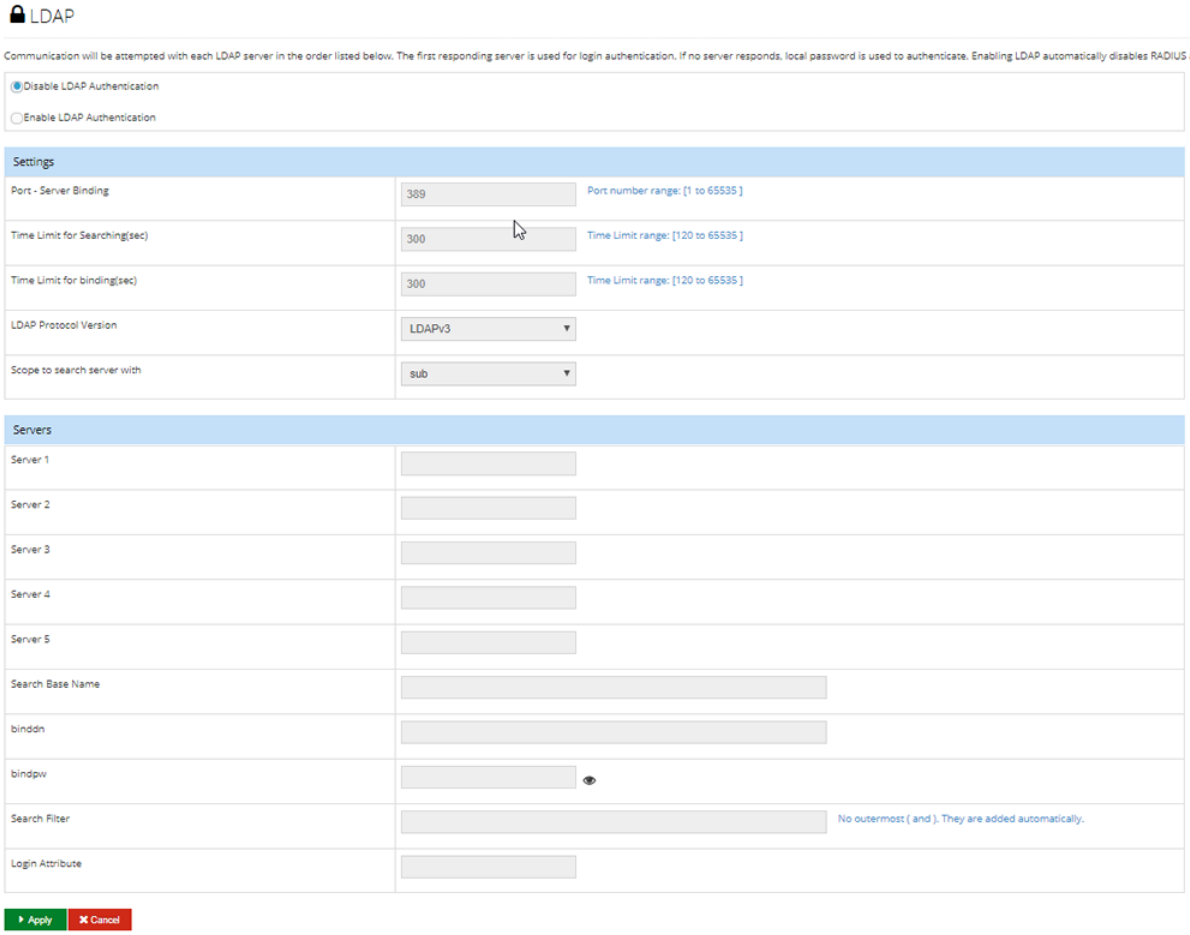
SyncServer S600/S650 has only one level of management access of Authentication/Authorization and that is full control. There is no read-only management access. Therefore,
Authentication = Authorization when there is only one level of management access.

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.

5.2.5.11 Security—LDAP Configuration Window

Use this window to enable LDAP, and configure LDAP settings and servers. Up to five LDAP servers can be configured.

Figure 5-53. Security—LDAP Configuration Window



LDAP

Communication will be attempted with each LDAP server in the order listed below. The first responding server is used for login authentication. If no server responds, local password is used to authenticate. Enabling LDAP automatically disables RADIUS a

● Disable LDAP Authentication

○ Enable LDAP Authentication

Settings		
Port - Server Binding	389	Port number range: [1 to 65535]
Time Limit for Searching(sec)	300	Time Limit range: [120 to 65535]
Time Limit for binding(sec)	300	Time Limit range: [120 to 65535]
LDAP Protocol Version	LDAPv3 ▾	
Scope to search server with	sub ▾	

Servers		
Server 1		
Server 2		
Server 3		
Server 4		
Server 5		
Search Base Name		
binddn		
bindpw		
Search Filter		No outermost (and). They are added automatically.
Login Attribute		

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 authenticates 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 can login to SyncServer. If the authentication fails, then SyncServer continues its local authentication using the local users list.

- 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.

Notes:

- 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).
- 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.
- 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

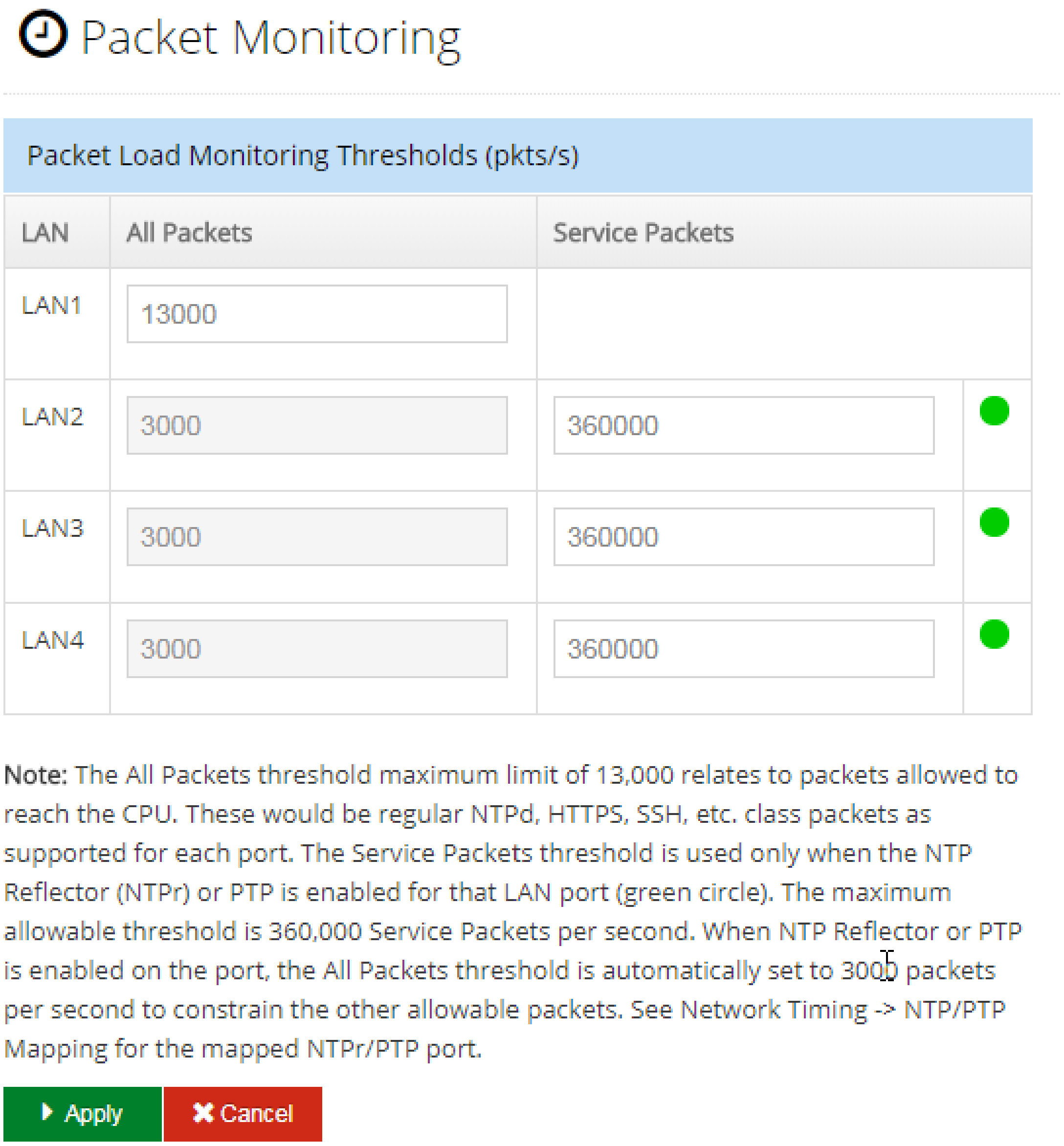
Parameter/Column	Description
Port-Server Binding	IP port for server
Time Limit for Searching	Timeout for searches
Time Limit for binding (sec)	Timeout for binding
LDAP Protocol Version	LDAPv2 or LDAPv3
Scope to search with	• base: Limits search to base object • one: Limits search to immediate children of base object, but not base object • sub: Search base objects and all child objects
Server 1–5	Enter up to five 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.

5.2.5.12 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 also generates the “Excessive traffic on port” alarm if the threshold is exceeded, and identifies the impacted port. Packets that are handled by the NTP reflector or PTP server 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 server. 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 is 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.

If a timing service is enabled on a port it is identified by the green indicator on this form, as shown in the following figure.

Figure 5-54. Security—Packet Monitoring Window



Packet Monitoring

Packet Load Monitoring Thresholds (pkts/s)

LAN	All Packets	Service Packets	
LAN1	13000		
LAN2	3000	360000	●
LAN3	3000	360000	●
LAN4	3000	360000	●

Note: The All Packets threshold maximum limit of 13,000 relates to packets allowed to reach the CPU. These would be regular NTPd, HTTPS, SSH, etc. class packets as supported for each port. The Service Packets threshold is used only when the NTP Reflector (NTPr) or PTP is enabled for that LAN port (green circle). The maximum allowable threshold is 360,000 Service Packets per second. When NTP Reflector or PTP is enabled on the port, the All Packets threshold is automatically set to 3000 packets per second to constrain the other allowable packets. See Network Timing -> NTP/PTP Mapping for the mapped NTPr/PTP port.

5.2.5.13 Security—X.509 Self-Signed Certificates and Certificate Signing Request

Use this window to generate a X.509 self-signed certificate or a Certificate Signing Request (CSR). CSRs are created in the Base-64 encoded PEM format. This format includes the "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE REQUEST-----" lines at the beginning and end of the CSR.

This feature requires the optional security license.

Note: Some certificate authorities require the user to change the public/private keys before requesting a new certificate. To change the keys, check the "Regenerate keys" box on the configuration form.

SyncServer generates a new set of public/private keys for each new CSR or self-signed certificate. If you want to regenerate keys for an existing CSR or self-signed certificate, then click the regenerate keys box on the configuration form and then click the update button.

After downloading the CSR, have your certificate authority create a signed certificate for you to install on the X.509 install page. Then, use the X.509 mapping page to map this certificate to HTTPS or syslog.

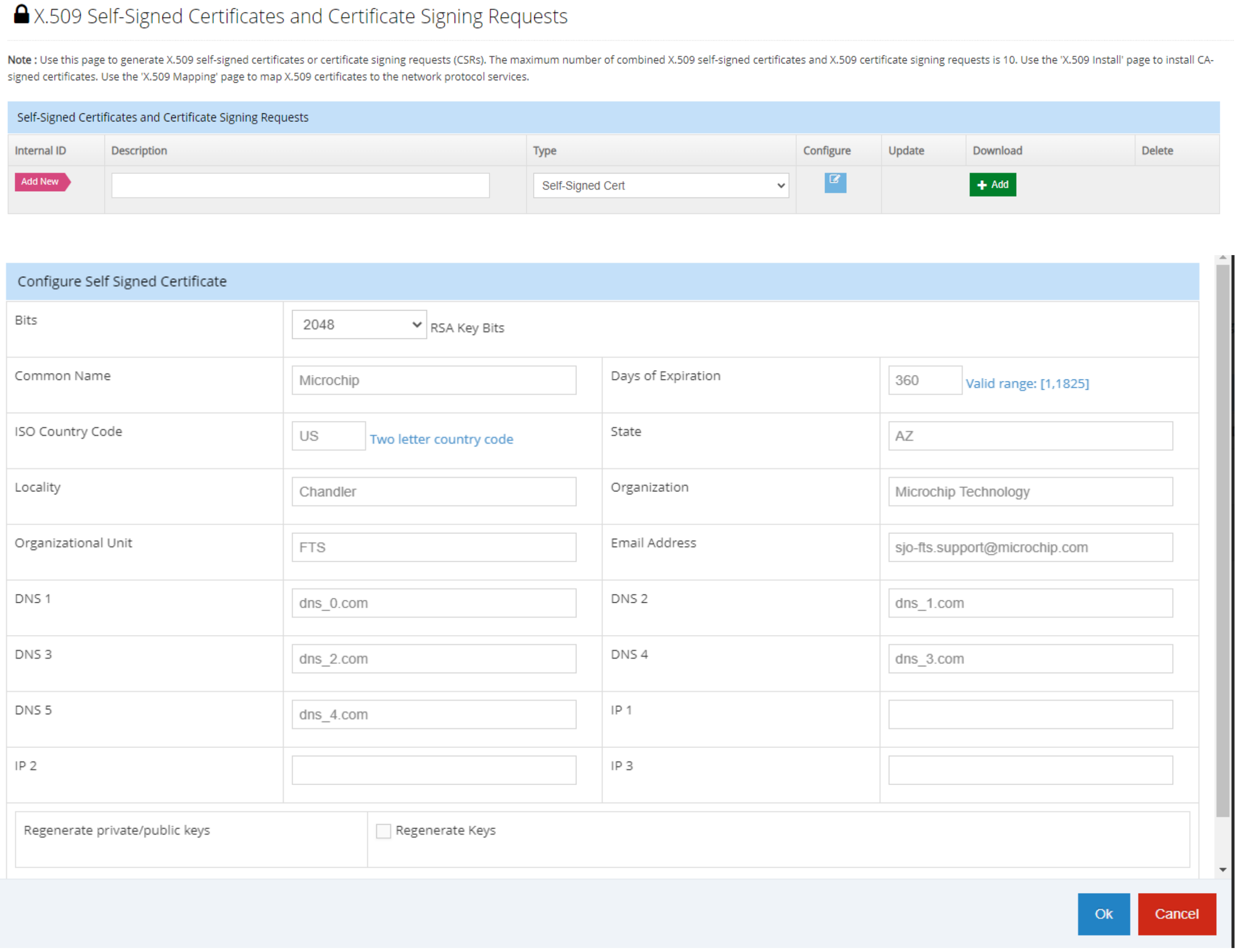
If you have created a new self-signed certificate, then go to the X.509 mapping page to select and use the new certificate.

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

Note: Information must be entered in at least one of the DNS or IP fields for Subject Alternative Name (SAN).

The CSR page accepts the following information from the user on the certificate configuration form:

Figure 5-55. Security—X.509 CSR Window



X.509 Self-Signed Certificates and Certificate Signing Requests

Note : Use this page to generate X.509 self-signed certificates or certificate signing requests (CSRs). The maximum number of combined X.509 self-signed certificates and X.509 certificate signing requests is 10. Use the 'X.509 Install' page to install CA-signed certificates. Use the 'X.509 Mapping' page to map X.509 certificates to the network protocol services.

Self-Signed Certificates and Certificate Signing Requests

Internal ID	Description	Type	Configure	Update	Download	Delete
Add New		Self-Signed Cert			+ Add	

Configure Self Signed Certificate

Bits	2048 RSA Key Bits		
Common Name	Microchip	Days of Expiration	360 Valid range: [1,1825]
ISO Country Code	US Two letter country code	State	AZ
Locality	Chandler	Organization	Microchip Technology
Organizational Unit	FTS	Email Address	sjo-fts.support@microchip.com
DNS 1	dns_0.com	DNS 2	dns_1.com
DNS 3	dns_2.com	DNS 4	dns_3.com
DNS 5	dns_4.com	IP 1	
IP 2		IP 3	
Regenerate private/public keys	□ Regenerate Keys		

Table 5-14. X.509 Configuration Parameters

Parameter/Column	Description
Bits	Number of RSA key bits—2048 or 4096
Common Name	FQDN of Sync Server.
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).

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

Parameter/Column	Description
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.
IP 1	IP for optional Subject Alternative Name (SAN). Leave a blank if not required.
IP 2	IP for optional Subject Alternative Name (SAN). Leave a blank if not required.
IP 3	IP for optional Subject Alternative Name (SAN). Leave a blank if not required.
IP 4	IP for optional Subject Alternative Name (SAN). Leave a blank if not required.
Add	The CSR or self-signed certificate is generated when this button is pressed.
Download	This button allows the user to download the corresponding CSR or self-signed certificateas a file.
Update	This button allows the user to update an existing CSR or self-signed certificate after changing something on the configuration form.

Special characters `, . : ; &` are allowed on the CSR page.

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

5.2.5.14 Security—X.509 Install

This feature requires an optional security license.

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 extensions 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.

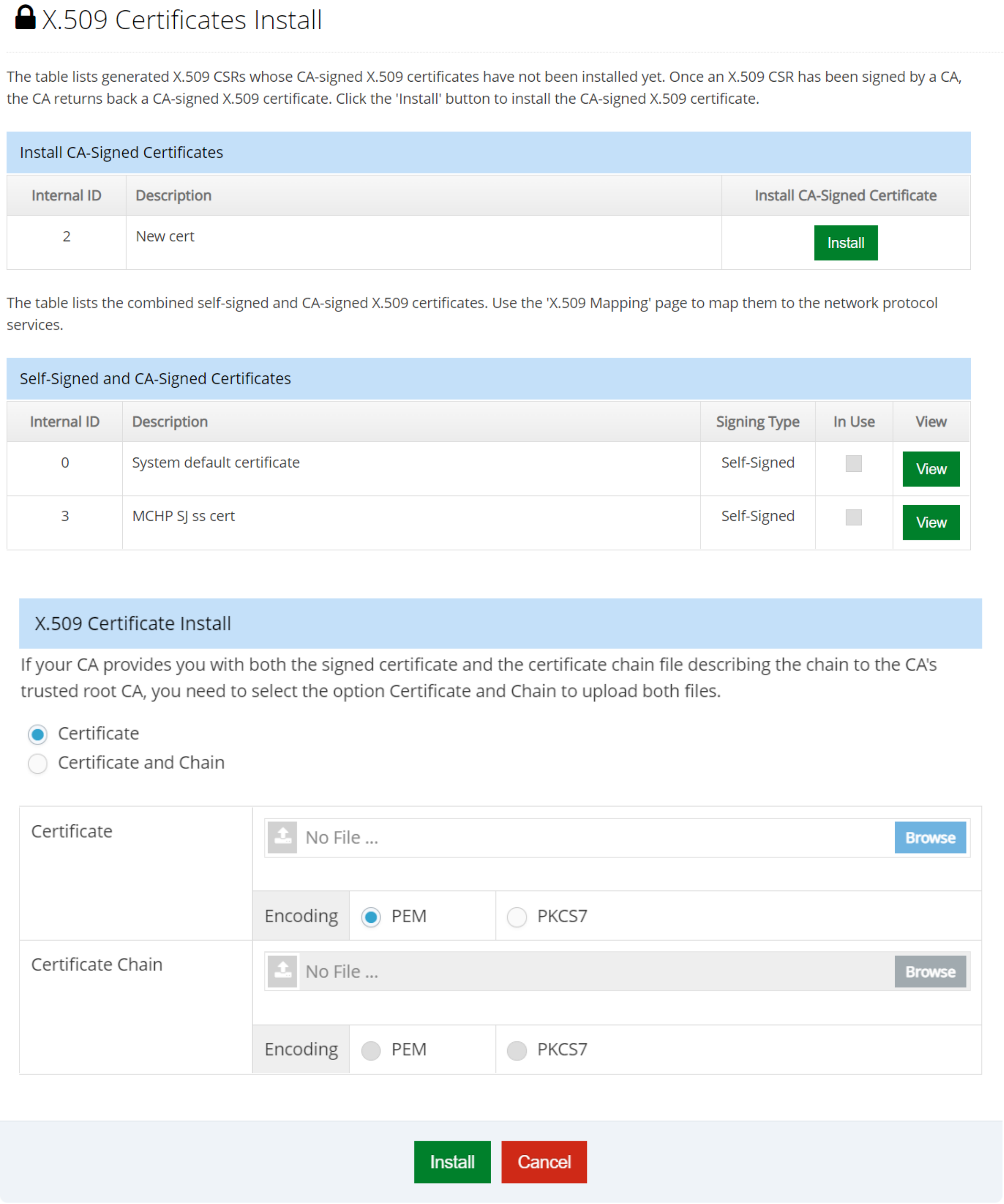
You must select the appropriate CSR for the certificate to install and click the **Instal**l button. A form is brought up to allow the user to upload the signed certificate/chain files and then click the **Install** button on the form to install the certificate on SyncServer.

The “Self-Signed and CA-Signed Certificates” section lists the certificates currently loaded and being used in the system. It also allows the user to view each of the certificates. The root/intermediate CA's certificate(s) are installed in client web browsers that have access to SyncServer. The browser being used must be able to identify the

Certification Authority as a known or trusted CA. This allows the browser to show the connection to SyncServer as being secure (https).

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

Figure 5-56. Security—X.509 Install Window



X.509 Certificates Install

The table lists generated X.509 CSRs whose CA-signed X.509 certificates have not been installed yet. Once an X.509 CSR has been signed by a CA, the CA returns back a CA-signed X.509 certificate. Click the 'Install' button to install the CA-signed X.509 certificate.

Install CA-Signed Certificates

Internal ID	Description	Install CA-Signed Certificate
2	New cert	Install

The table lists the combined self-signed and CA-signed X.509 certificates. Use the 'X.509 Mapping' page to map them to the network protocol services.

Self-Signed and CA-Signed Certificates

Internal ID	Description	Signing Type	In Use	View
0	System default certificate	Self-Signed	□	View
3	MCHP SJ ss cert	Self-Signed	□	View

X.509 Certificate Install

If your CA provides you with both the signed certificate and the certificate chain file describing the chain to the CA's trusted root CA, you need to select the option Certificate and Chain to upload both files.

● Certificate
○ Certificate and Chain

Certificate	No File ... Browse		
	Encoding	● PEM	○ PKCS7
Certificate Chain	No File ... Browse		
	Encoding	○ PEM	○ PKCS7

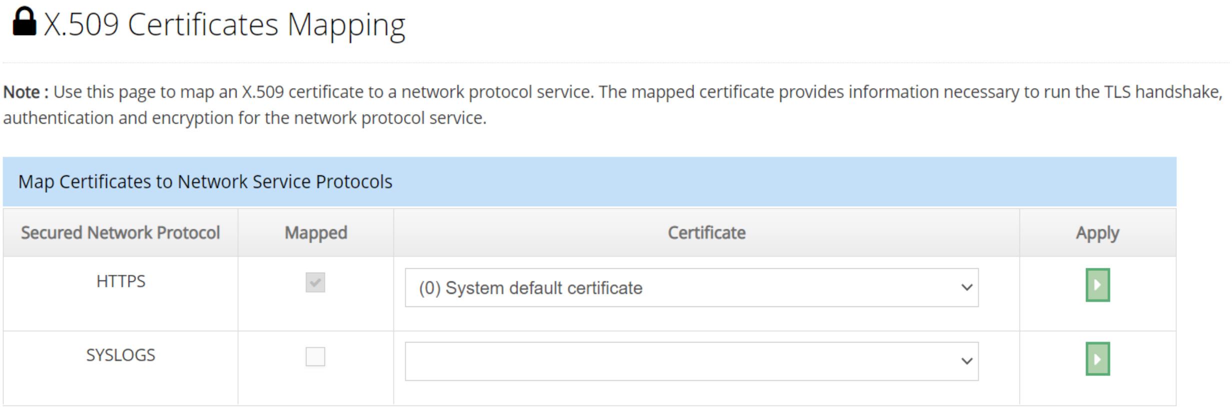
5.2.6 Security—X.509 Certificates Mapping

This page requires the security license.

This page allows you to map certificates that are loaded on the system to selected protocols. These protocols include HTTPS and SYSLOGS. Certificates can be either self-signed or signed.

For a protocol, select the desired certificate from the pull-down and click **Apply** button.

Figure 5-57. 5x-Mapping



X.509 Certificates Mapping

Note : Use this page to map an X.509 certificate to a network protocol service. The mapped certificate provides information necessary to run the TLS handshake, authentication and encryption for the network protocol service.

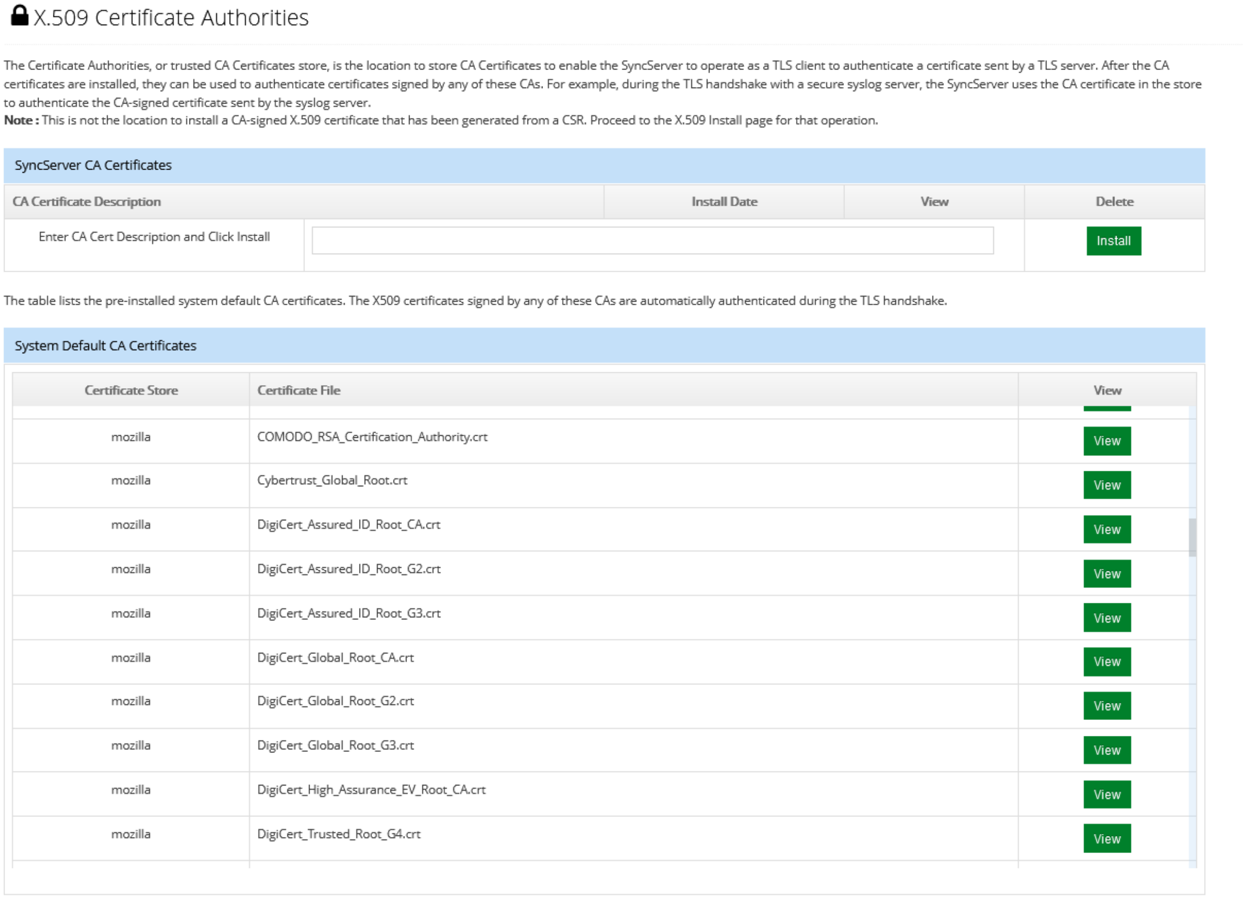
Map Certificates to Network Service Protocols

Secured Network Protocol	Mapped	Certificate	Apply
HTTPS	☑	(0) System default certificate	▶
SYSLOGS	□		▶

5.2.7 Security—X.509 Certificate Authorities

This page requires the security license. It allows the user to load CA certificates and view currently installed certificates. These CA certificates are used to verify CA-signed certificates when SyncServer is the TLS client. For example, a CA certificate is used during the TLS handshake with a secure syslog server.

Figure 5-58. 5X-CA Certificate



X.509 Certificate Authorities

The Certificate Authorities, or trusted CA Certificates store, is the location to store CA Certificates to enable the SyncServer to operate as a TLS client to authenticate a certificate sent by a TLS server. After the CA certificates are installed, they can be used to authenticate certificates signed by any of these CAs. For example, during the TLS handshake with a secure syslog server, the SyncServer uses the CA certificate in the store to authenticate the CA-signed certificate sent by the syslog server.
Note : This is not the location to install a CA-signed X.509 certificate that has been generated from a CSR. Proceed to the X.509 Install page for that operation.

SyncServer CA Certificates

CA Certificate Description	Install Date	View	Delete
Enter CA Cert Description and Click Install			Install

The table lists the pre-installed system default CA certificates. The X509 certificates signed by any of these CAs are automatically authenticated during the TLS handshake.

System Default CA Certificates

Certificate Store	Certificate File	View
mozilla	COMODO_RSA_Certification_Authority.crt	View
mozilla	Cybertrust_Global_Root.crt	View
mozilla	DigiCert_Assured_ID_Root_CA.crt	View
mozilla	DigiCert_Assured_ID_Root_G2.crt	View
mozilla	DigiCert_Assured_ID_Root_G3.crt	View
mozilla	DigiCert_Global_Root_CA.crt	View
mozilla	DigiCert_Global_Root_G2.crt	View
mozilla	DigiCert_Global_Root_G3.crt	View
mozilla	DigiCert_High_Assurance_EV_Root_CA.crt	View
mozilla	DigiCert_Trusted_Root_G4.crt	View

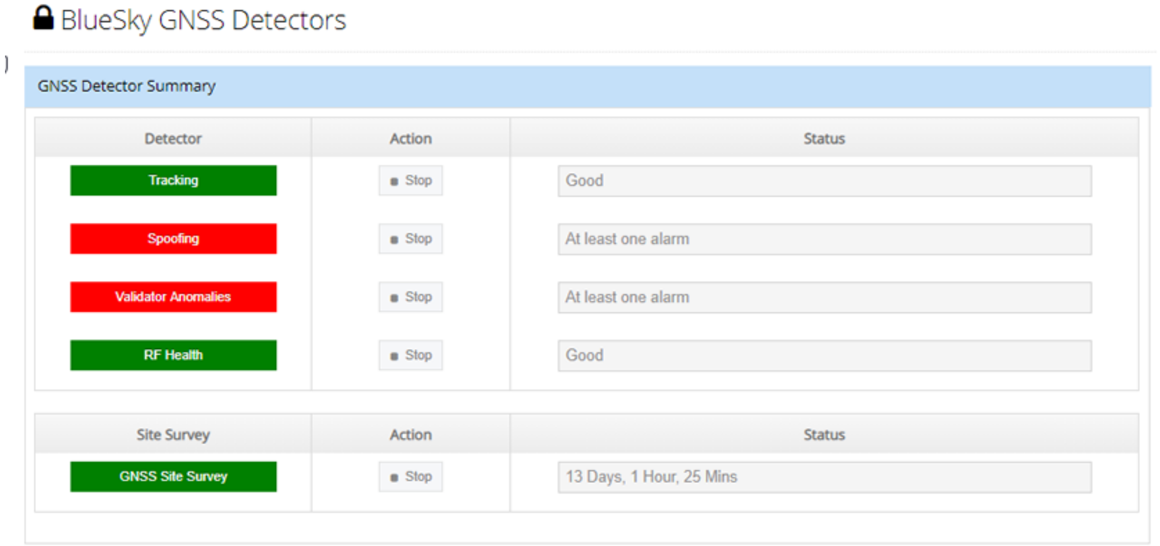
5.2.8 Jamming/Spoofing Windows

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.

5.2.8.1 Jamming/Spoofing—Detectors

Use this window to start/stop GNSS detectors and view status of these detectors.
Note: If the validator detector is running, the maximum NTP load is reduced to 6000 requests/s.

Figure 5-59. Jamming/Spoofing—Detectors Window



BlueSky GNSS Detectors

GNSS Detector Summary

Detector	Action	Status
Tracking	■ Stop	Good
Spoofing	■ Stop	At least one alarm
Validator Anomalies	■ Stop	At least one alarm
RF Health	■ Stop	Good

Site Survey	Action	Status
GNSS Site Survey	■ Stop	13 Days, 1 Hour, 25 Mins

5.2.8.2 Jamming/Spoofing—Configuration

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

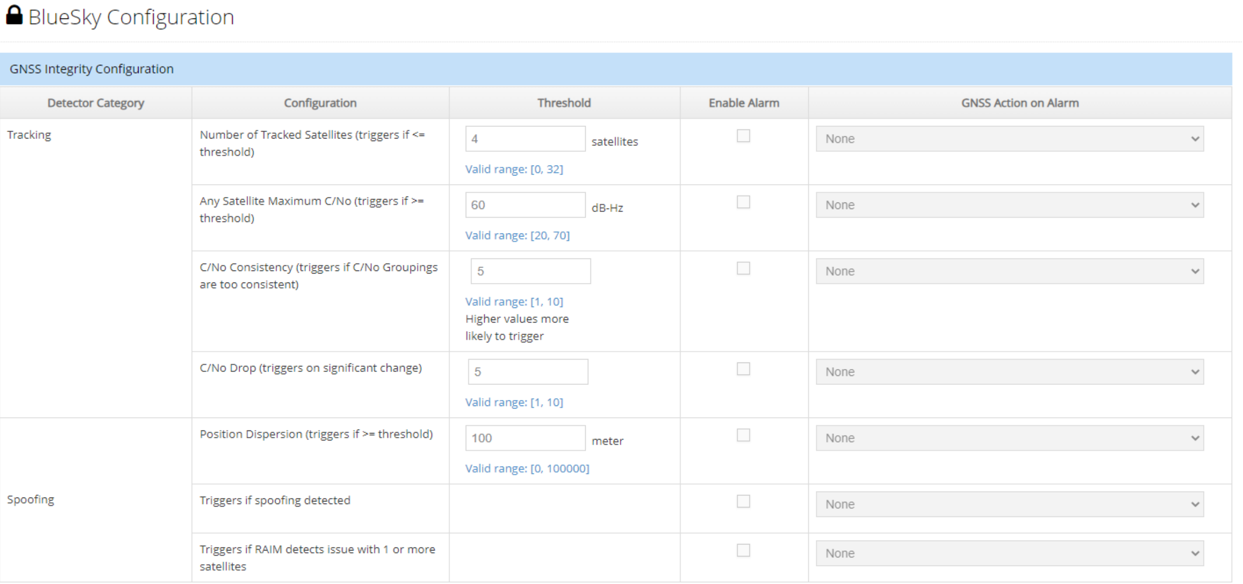
In addition to setting thresholds, alarms can be enabled or disabled for a detector. Also, a system action can be configured for each of the detectors, as listed in the following table:

Table 5-15. System Action

Action	Explanation
None	No system action if detector triggers.
Disqualify GNSS only while alarmed	If detector alarm is active, then system disqualifies GNSS reference input until the alarm is cleared.
Disqualify GNSS on alarm, toggle alarm to reset	If alarm becomes active, then GNSS reference input is disqualified and stays disqualified even after the alarm goes inactive. To allow GNSS to be used, you must disable and then re-enable the alarm for the appropriate detector.

Note: If a satellite is unhealthy, especially for maintenance or commissioning, then you might want to not configure validator rules to disqualify GNSS, as validator rules might be violated during maintenance.

Figure 5-60. Jamming/Spoofing—Top of Configuration Window

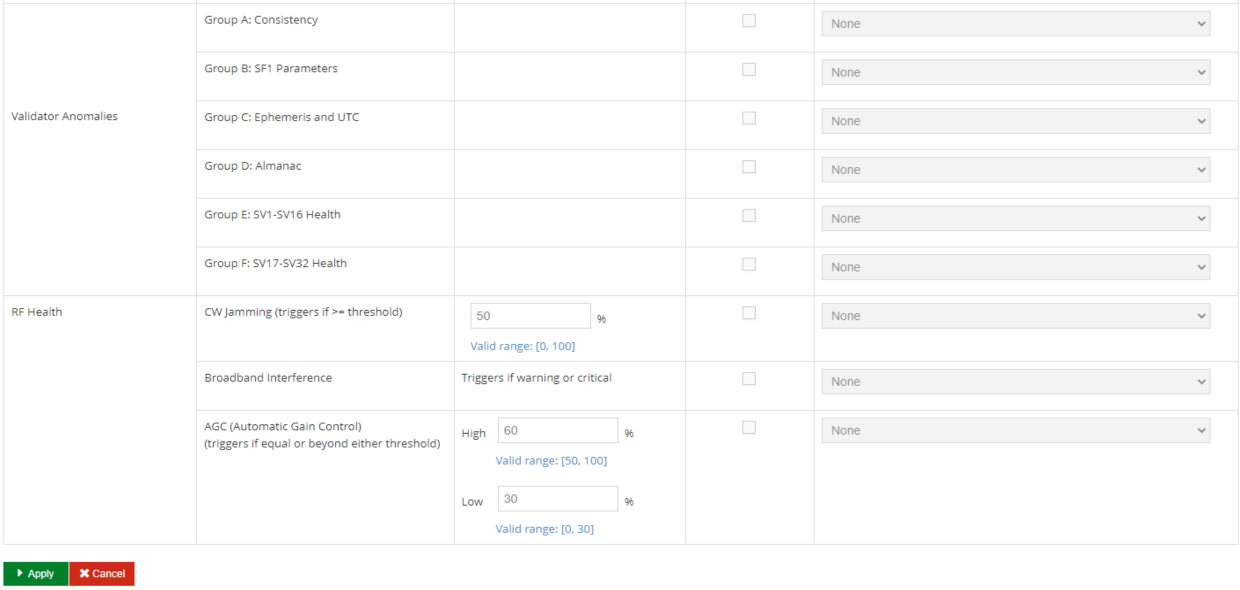


BlueSky Configuration

GNSS Integrity Configuration

Detector Category	Configuration	Threshold	Enable Alarm	GNSS Action on Alarm
Tracking	Number of Tracked Satellites (triggers if <= threshold)	4 satellites Valid range: [0, 32]	□	None
	Any Satellite Maximum C/No (triggers if >= threshold)	60 dB-Hz Valid range: [20, 70]	□	None
	C/No Consistency (triggers if C/No Groupings are too consistent)	5 Valid range: [1, 10] Higher values more likely to trigger	□	None
	C/No Drop (triggers on significant change)	5 Valid range: [1, 10]	□	None
Spoofing	Position Dispersion (triggers if >= threshold)	100 meter Valid range: [0, 100000]	□	None
	Triggers if spoofing detected		□	None
	Triggers if RAIM detects issue with 1 or more satellites		□	None

Figure 5-61. Jamming/Spoofing—Bottom View of Configuration Window

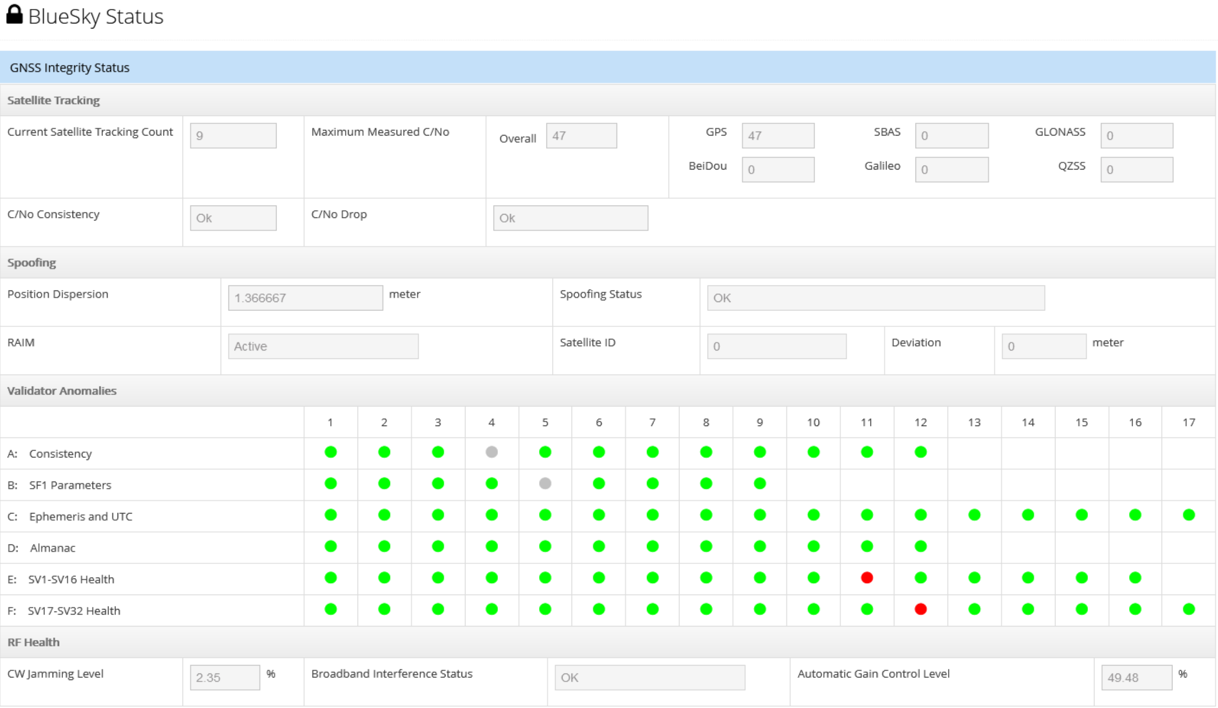


Detector Category	Configuration	Threshold	Enable Alarm	GNSS Action on Alarm
Validator Anomalies	Group A: Consistency		□	None
	Group B: SF1 Parameters		□	None
	Group C: Ephemeris and UTC		□	None
	Group D: Almanac		□	None
	Group E: SV1-SV16 Health		□	None
	Group F: SV17-SV32 Health		□	None
RF Health	CW Jamming (triggers if >= threshold)	50 % Valid range: [0, 100]	□	None
	Broadband Interference	Triggers if warning or critical	□	None
	AGC (Automatic Gain Control) (triggers if equal or beyond either threshold)	High 60 % Valid range: [50, 100] Low 30 % Valid range: [0, 30]	□	None

5.2.8.3 Jamming/Spoofing—Status

Use this window to view the status of GNSS integrity. You can get the GPS constellation status, including planned outages, at: www.navcen.uscg.gov/?Do=constellationStatus.

Figure 5-62. Jamming/Spoofing—Status Window



BlueSky Status

GNSS Integrity Status

Satellite Tracking

Current Satellite Tracking Count	9	Maximum Measured C/No	Overall	47	GPS	47	SBAS	0	GLONASS	0
					BeiDou	0	Galileo	0	QZSS	0
C/No Consistency	Ok	C/No Drop	Ok							

Spoofing

Position Dispersion	1.366667 meter	Spoofing Status	OK				
RAIM	Active	Satellite ID	0	Deviation	0 meter		

Validator Anomalies

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
A: Consistency	🟢	🟢	🟢	⚪	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢					
B: SF1 Parameters	🟢	🟢	🟢	🟢	⚪	🟢	🟢	🟢	🟢								
C: Ephemeris and UTC	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
D: Almanac	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢					
E: SV1-SV16 Health	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	
F: SV17-SV32 Health	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢

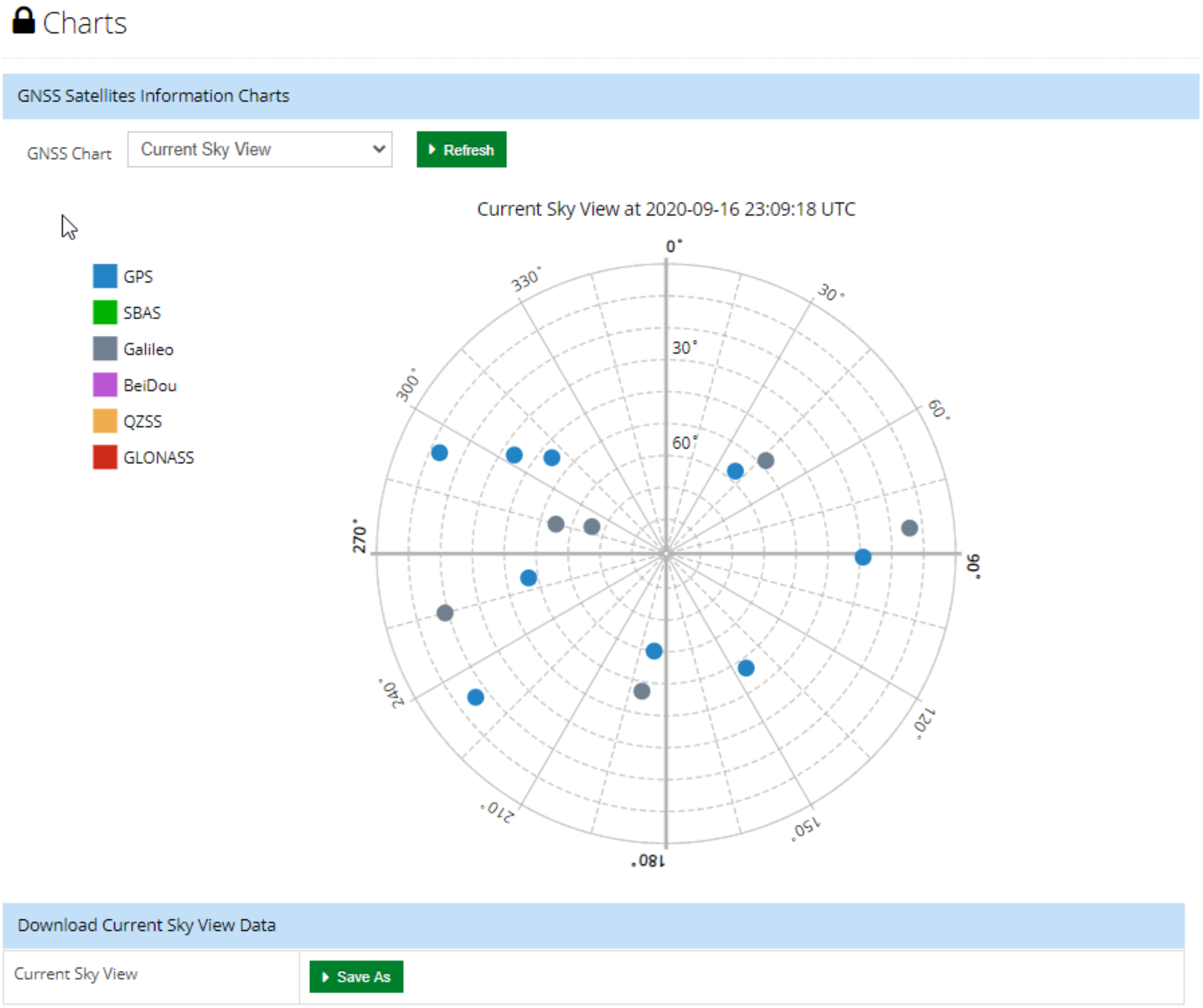
RF Health

CW Jamming Level	2.35 %	Broadband Interference Status	OK	Automatic Gain Control Level	49.48 %

5.2.8.4 Jamming/Spoofing—Charts

Use this window to view the GNSS Satellite Information charts.

Figure 5-63. Jamming/Spoofing—Charts Window (Current Sky View)



Charts

GNSS Satellites Information Charts

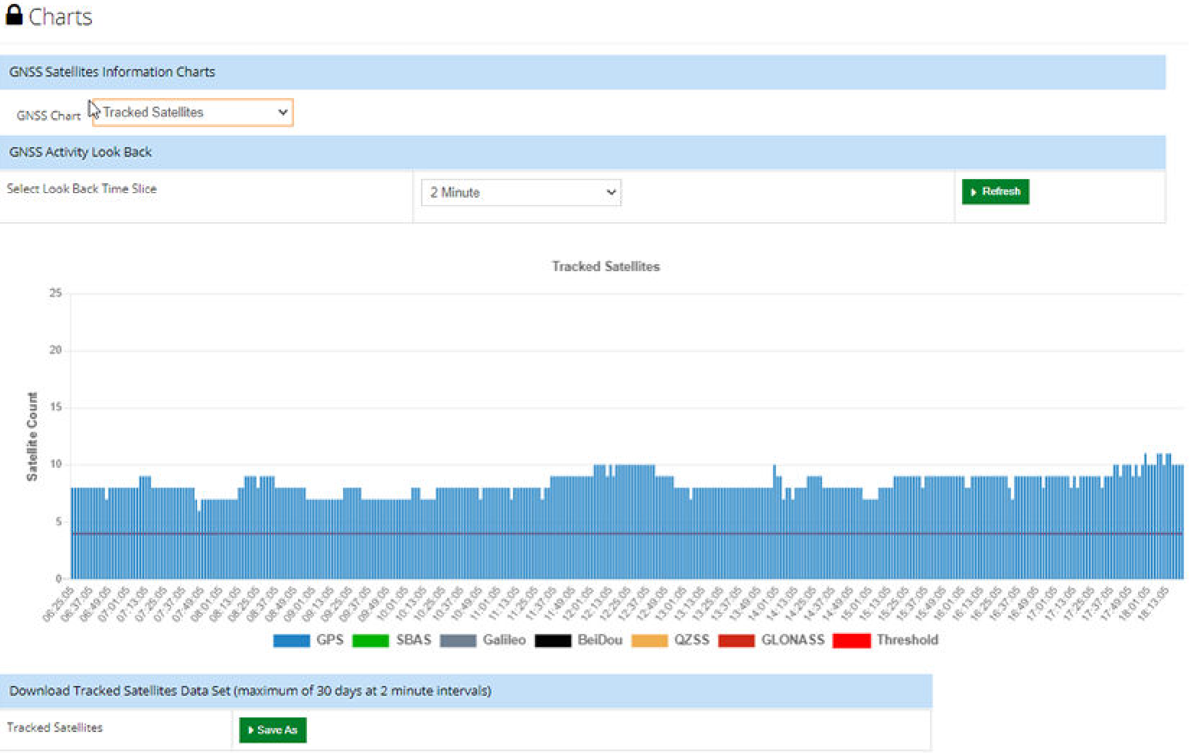
GNSS Chart: Current Sky View

Current Sky View at 2020-09-16 23:09:18 UTC

Download Current Sky View Data

Current Sky View

Figure 5-64. Jamming/Spoofing—Charts Window (Tracked Satellites)



Charts

GNSS Satellites Information Charts

GNSS Chart: Tracked Satellites

GNSS Activity Look Back

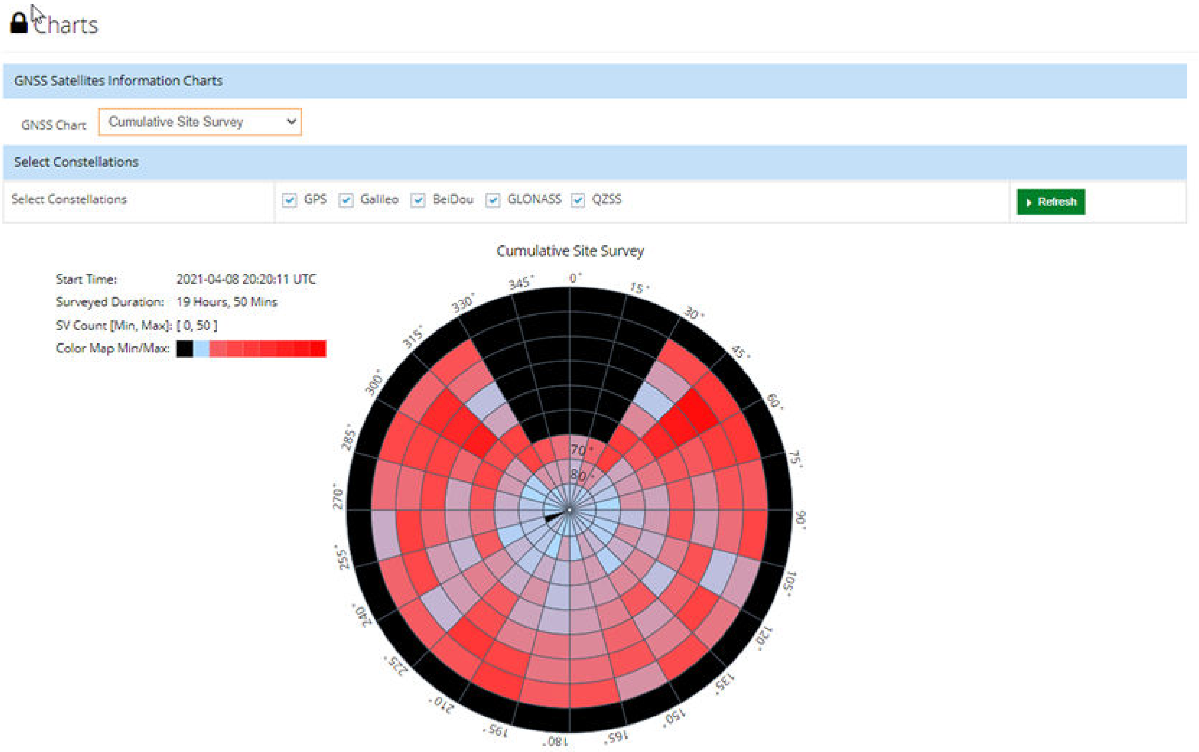
Select Look Back Time Slice: 2 Minute

▸ Refresh

Download Tracked Satellites Data Set (maximum of 30 days at 2 minute intervals)

Tracked Satellites: ▸ Save As

Figure 5-65. Jamming/Spoofing—Charts Window (Cumulative Site Survey)



Charts

GNSS Satellites Information Charts

GNSS Chart: Cumulative Site Survey

Select Constellations

Select Constellations: ☑ GPS ☑ Galileo ☑ BeiDou ☑ GLONASS ☑ QZSS

▸ Refresh

Cumulative Site Survey

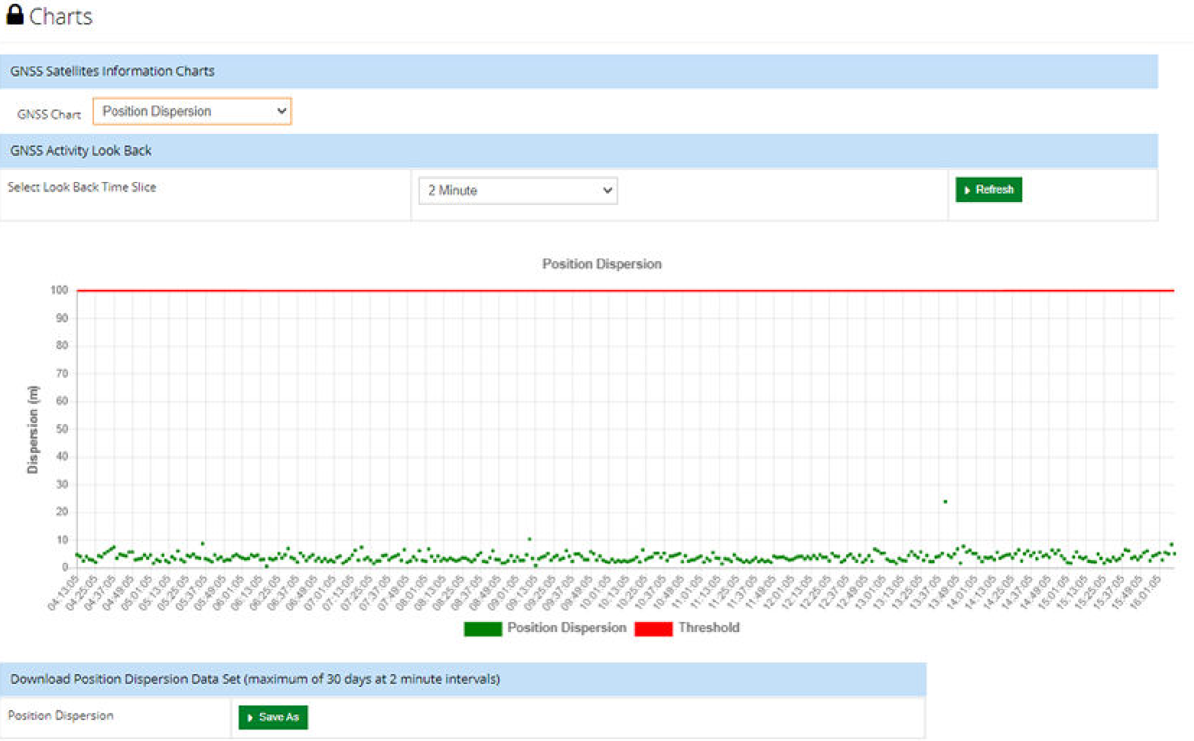
Start Time: 2021-04-08 20:20:11 UTC

Surveyed Duration: 19 Hours, 50 Mins

SV Count [Min, Max]: [0, 50]

Color Map Min/Max:

Figure 5-66. Jamming/Spoofing—Charts Window (Position Dispersion)



Charts

GNSS Satellites Information Charts

GNSS Chart: Position Dispersion

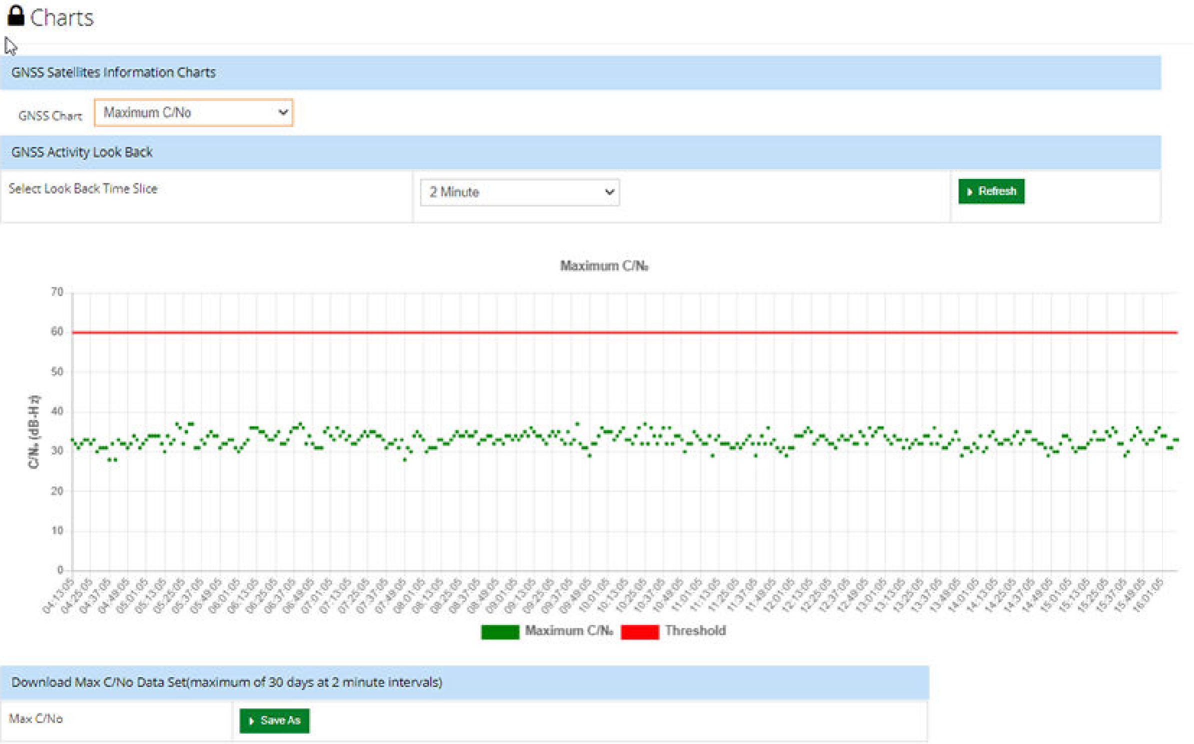
GNSS Activity Look Back

Select Look Back Time Slice: 2 Minute

Download Position Dispersion Data Set (maximum of 30 days at 2 minute intervals)

Position Dispersion

Figure 5-67. Jamming/Spoofing—Charts Window (Maximum C/No)



Charts

GNSS Satellites Information Charts

GNSS Chart: Maximum C/No

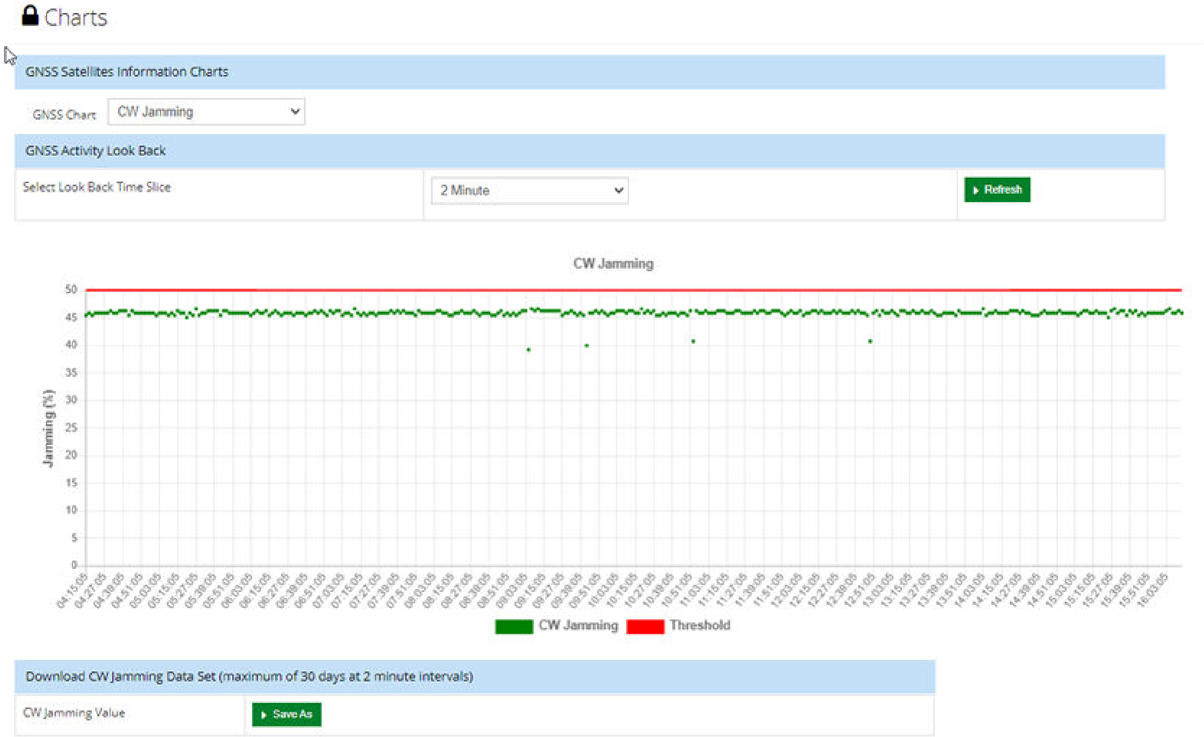
GNSS Activity Look Back

Select Look Back Time Slice: 2 Minute

Download Max C/No Data Set(maximum of 30 days at 2 minute intervals)

Max C/No

Figure 5-68. Jamming/Spoofing—Charts Window (CW Jamming)



Charts

GNSS Satellites Information Charts

GNSS Chart: CW Jamming

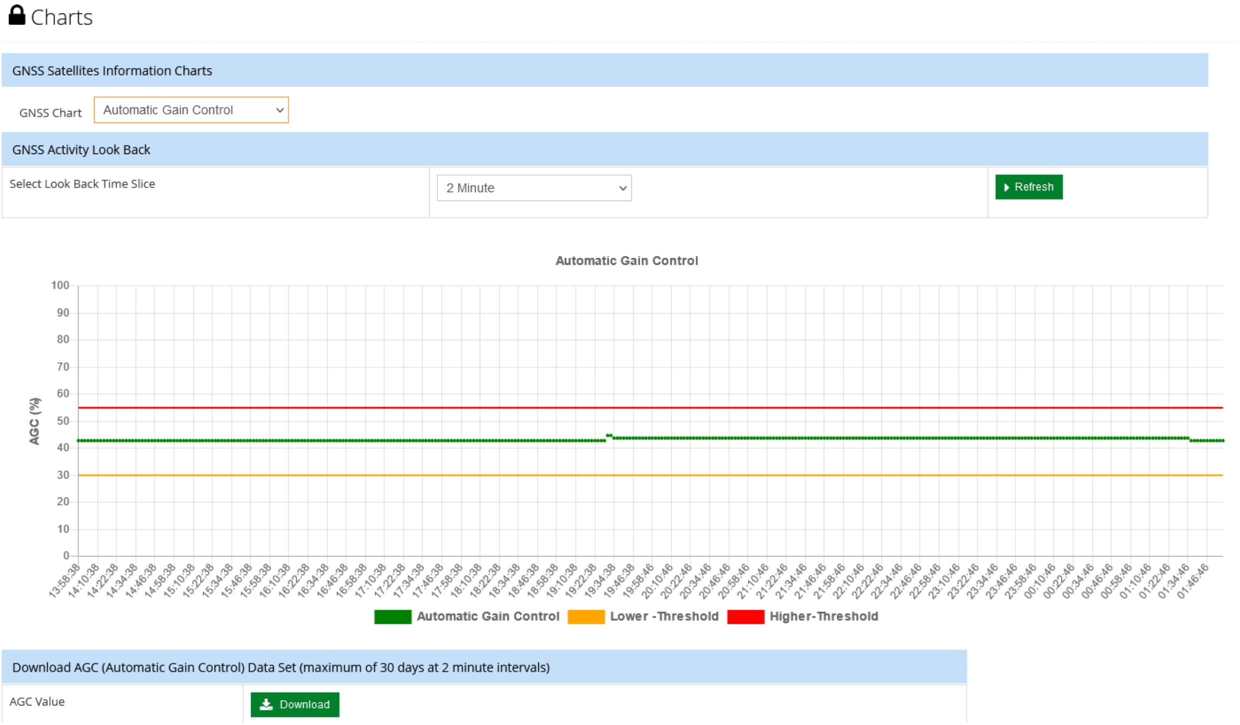
GNSS Activity Look Back

Select Look Back Time Slice: 2 Minute

Download CW Jamming Data Set (maximum of 30 days at 2 minute intervals)

CW Jamming Value

Figure 5-69. Jamming/Spoofing—Charts Window (Automatic Gain Control)



Charts

GNSS Satellites Information Charts

GNSS Chart: Automatic Gain Control

GNSS Activity Look Back

Select Look Back Time Slice: 2 Minute

Download AGC (Automatic Gain Control) Data Set (maximum of 30 days at 2 minute intervals)

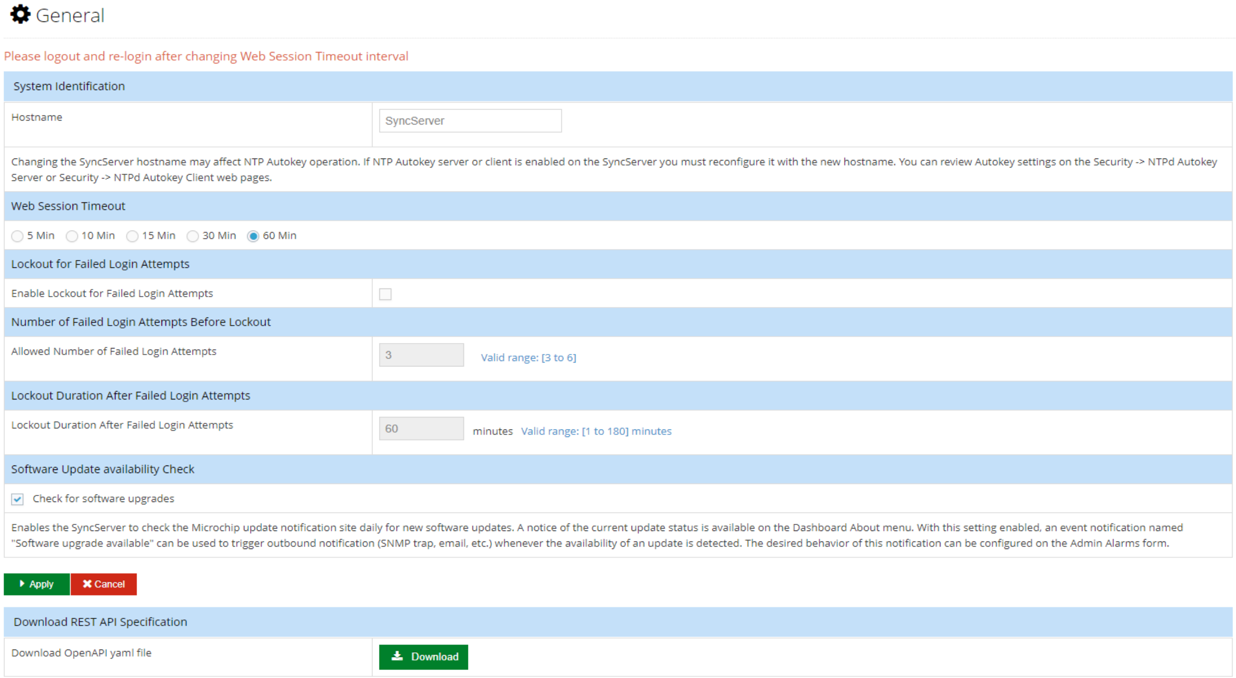
AGC Value

5.3 Admin Configuration Windows

5.3.1 Admin—General Configuration Window

Use this window to configure system identification and to check for software updates.

Figure 5-70. Admin—General Configuration Window



General

Please logout and re-login after changing Web Session Timeout interval

System Identification	
Hostname	SyncServer
Changing the SyncServer hostname may affect NTP Autokey operation. If NTP Autokey server or client is enabled on the SyncServer you must reconfigure it with the new hostname. You can review Autokey settings on the Security -> NTPd Autokey Server or Security -> NTPd Autokey Client web pages.	
Web Session Timeout	
○ 5 Min ○ 10 Min ○ 15 Min ○ 30 Min ● 60 Min	
Lockout for Failed Login Attempts	
Enable Lockout for Failed Login Attempts	□
Number of Failed Login Attempts Before Lockout	
Allowed Number of Failed Login Attempts	3 Valid range: [3 to 6]
Lockout Duration After Failed Login Attempts	
Lockout Duration After Failed Login Attempts	60 minutes Valid range: [1 to 180] minutes
Software Update availability Check	
☑ Check for software upgrades	
Enables the SyncServer to check the Microchip update notification site daily for new software updates. A notice of the current update status is available on the Dashboard About menu. With this setting enabled, an event notification named "Software upgrade available" can be used to trigger outbound notification (SNMP trap, email, etc.) whenever the availability of an update is detected. The desired behavior of this notification can be configured on the Admin Alarms form.	

Download REST API Specification	
Download OpenAPI yaml file	Download

For new software updates, this page enables SyncServer to check the Microchip upgrade notification site every day at noon local time at the following: SyncServer S600, SyncServer S650, and SyncServer S650i.

It displays a notice on the Status page and can send and SNMP trap when an upgrade is available.

This page requires that SyncServer management port have firewall access to the internet.

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

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

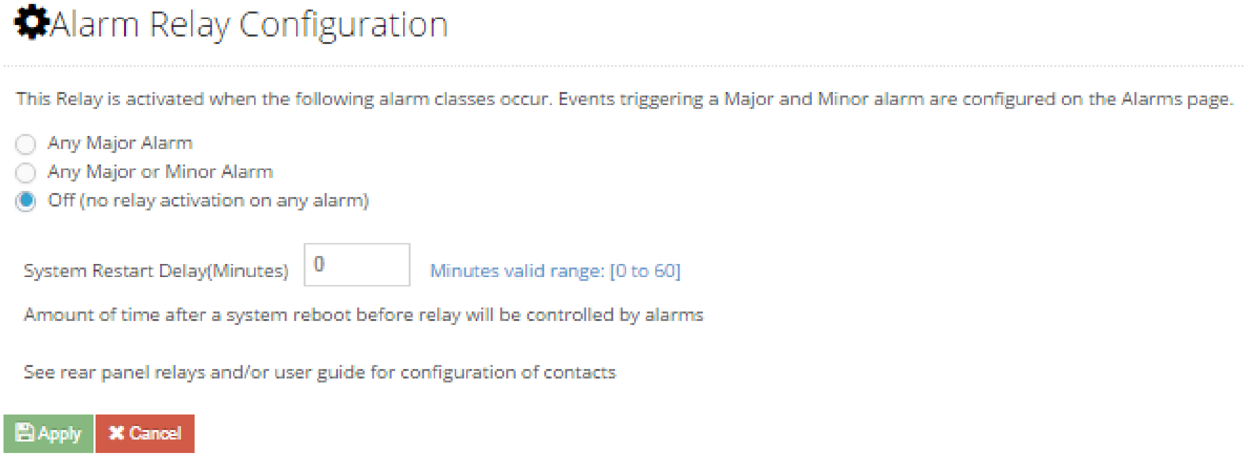
- abcdefghijklmnopqrstuvwxyz
- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- 0123456789
- -_

The system supports REST API. This provides a network-based programmatic interface. A compressed archive file can be downloaded from this page. The archive contains YAML specification files, examples, starting guide, release notes, and documentation. This documentation assumes that the user is familiar with REST API.
Note: The software update availability feature uses IPv4. An IPv4 address and DNS server must be configured on the `Network->Ethernet` page to use this feature.

5.3.2 Admin—Alarm Relay Configuration Window

Use this window to configure system alarm relay details.

Figure 5-71. Admin—Alarm Relay Configuration Window



Alarm Relay Configuration

This Relay is activated when the following alarm classes occur. Events triggering a Major and Minor alarm are configured on the Alarms page.

○ Any Major Alarm
○ Any Major or Minor Alarm
● Off (no relay activation on any alarm)

System Restart Delay(Minutes) 0 Minutes valid range: [0 to 60]

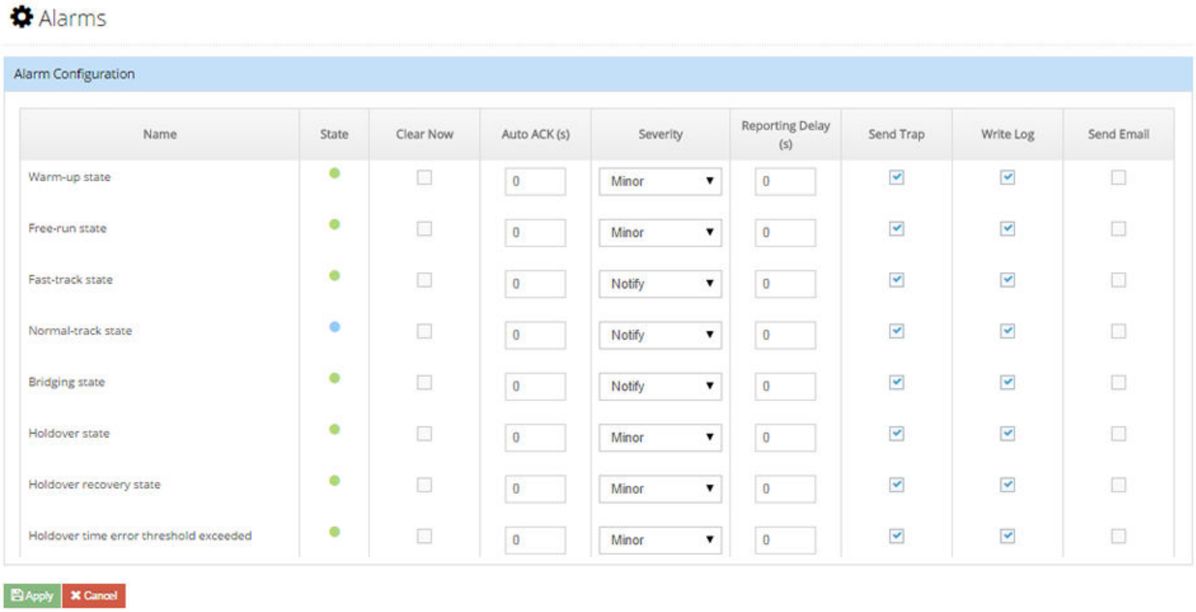
Amount of time after a system reboot before relay will be controlled by alarms

See rear panel relays and/or user guide for configuration of contacts

5.3.3 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. The following table lists the descriptions of Alarm Configuration parameters.

Figure 5-72. Admin—Alarm Configuration Window



Alarms

Alarm Configuration

Name	State	Clear Now	Auto ACK (s)	Severity	Reporting Delay (s)	Send Trap	Write Log	Send Email
Warm-up state	●	□	0	Minor	0	☑	☑	□
Free-run state	●	□	0	Minor	0	☑	☑	□
Fast-track state	●	□	0	Notify	0	☑	☑	□
Normal-track state	●	□	0	Notify	0	☑	☑	□
Bridging state	●	□	0	Notify	0	☑	☑	□
Holdover state	●	□	0	Minor	0	☑	☑	□
Holdover recovery state	●	□	0	Minor	0	☑	☑	□
Holdover time error threshold exceeded	●	□	0	Minor	0	☑	☑	□

Table 5-16. 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 (for example, Excessive Traffic on Ethernet port has a secondary field that identifies the port), these settings are global to all the secondary cases.

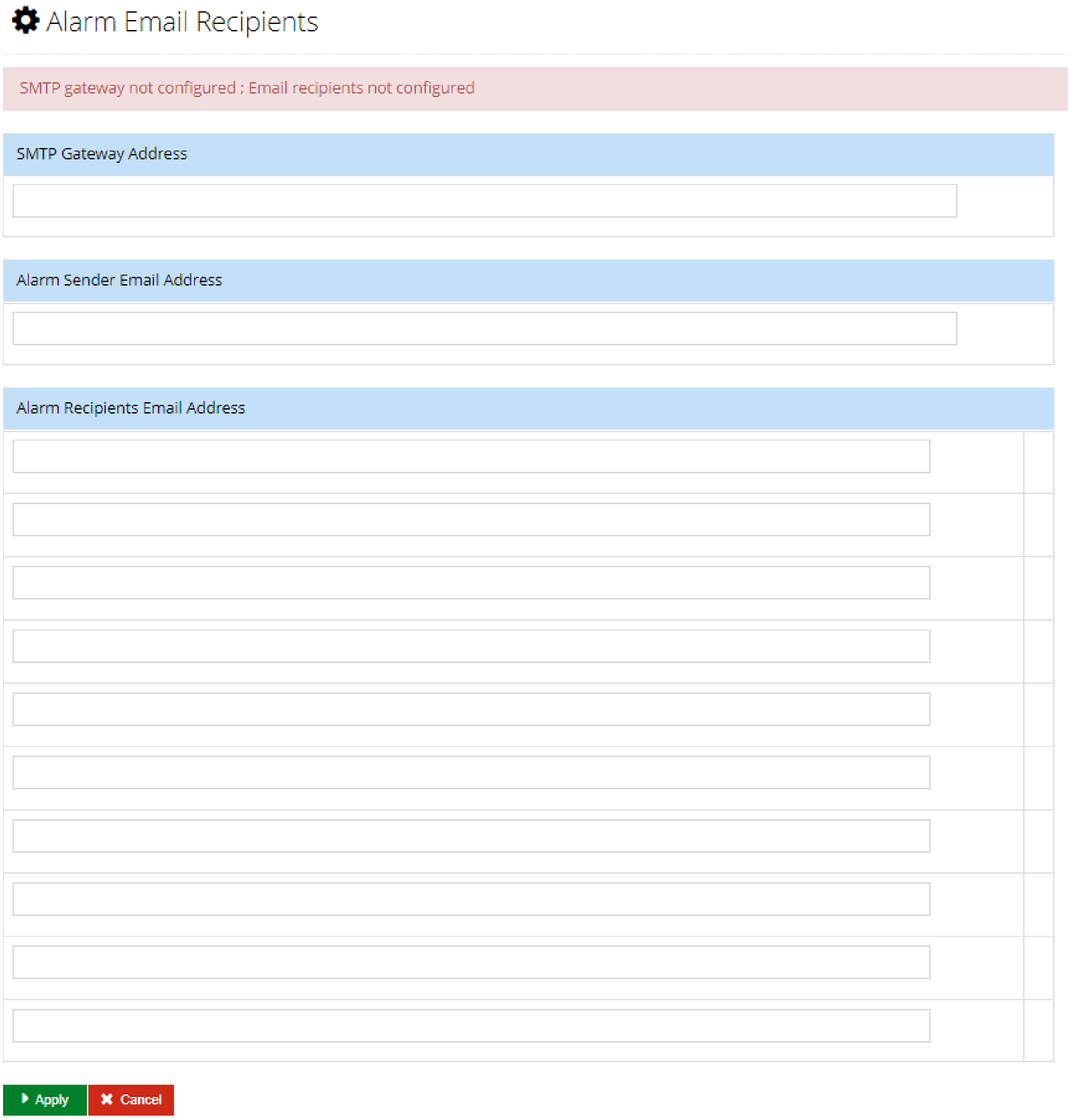
...........continued

Parameter	Description
State	Indicates the current status of the alarm based on color. • **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.
Clear Now	This is a user-control to cause some of the alarm report mechanisms to extinguish that 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 acknowledgment of the alarm, and has no impact on the underlying condition.
Auto ACK	This is the same as Clear Now except that it provides an automatic clearing action after a user-defined time, 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.

5.3.4 Admin—Email Configuration Window

Use this window to set, modify or delete email addresses for alarm email recipients.

Figure 5-73. Admin—Email Configuration Window

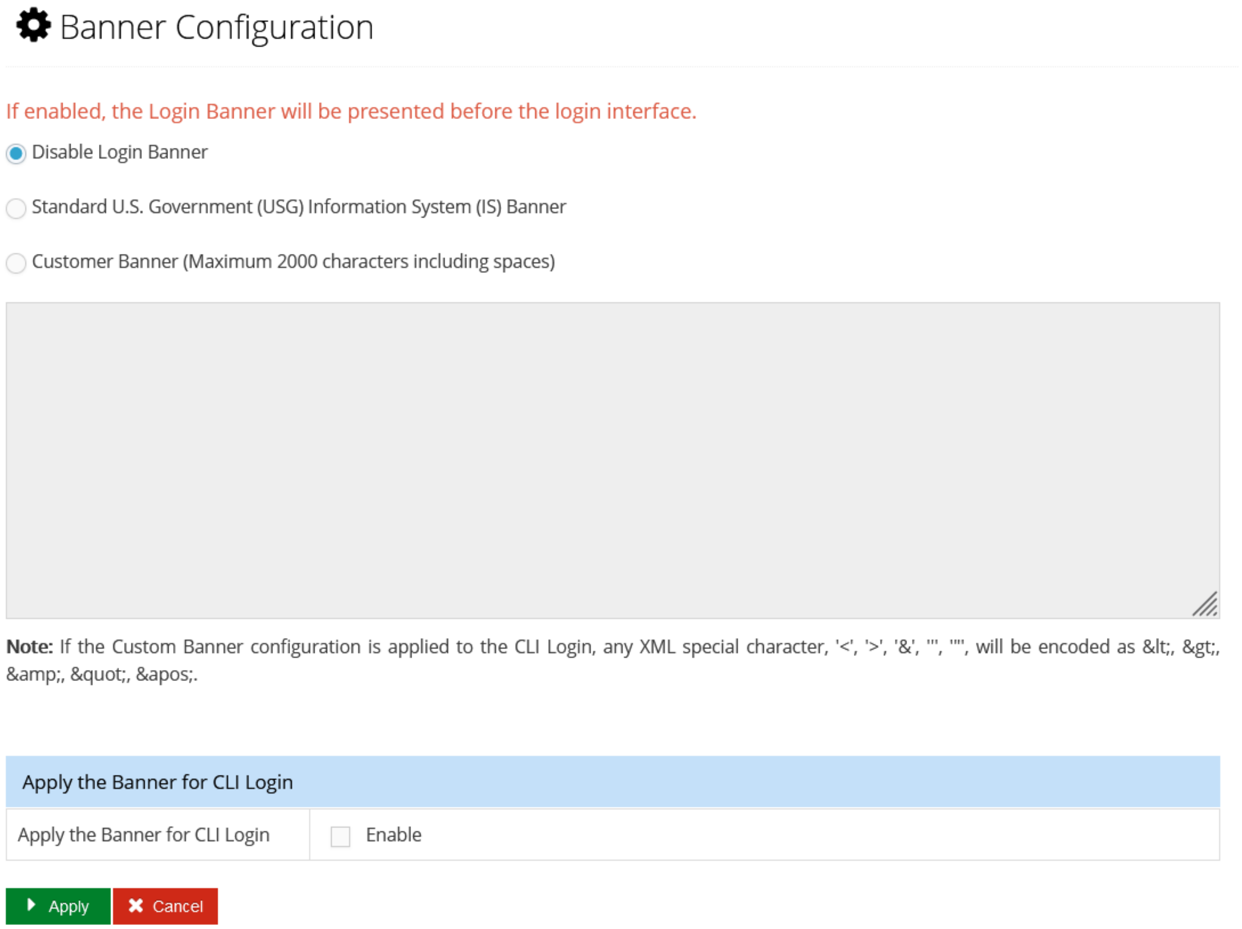


SMTP gateway not configured ; Email recipients not configured

5.3.5 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. The banner text can also be configured to be displayed for the CLI login.

Figure 5-74. Admin—Banner Configuration Window



Banner Configuration

If enabled, the Login Banner will be presented before the login interface.

● Disable Login Banner

○ Standard U.S. Government (USG) Information System (IS) Banner

○ Customer Banner (Maximum 2000 characters including spaces)

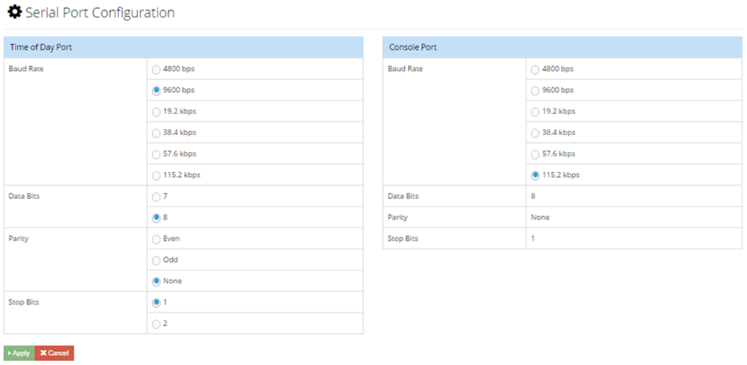
Note: If the Custom Banner configuration is applied to the CLI Login, any XML special character, '<', '>', '&', ''', '"', will be encoded as &lt;, &gt;, &amp;, &quot;, &apos;.

Apply the Banner for CLI Login	
Apply the Banner for CLI Login	□ Enable

5.3.6 Admin—Serial Port Configuration Window

Use this window to configure the parameters for the ToD port and for the console Serial port.

Figure 5-75. Admin - Serial Port Configuration Window



Serial Port Configuration

Time of Day Port	
Baud Rate	○ 4800 bps ● 9600 bps ○ 19.2 kbps ○ 38.4 kbps ○ 57.6 kbps ○ 115.2 kbps
Data Bits	○ 7 ● 8
Parity	○ Even ○ Odd ● None
Stop Bits	● 1 ○ 2

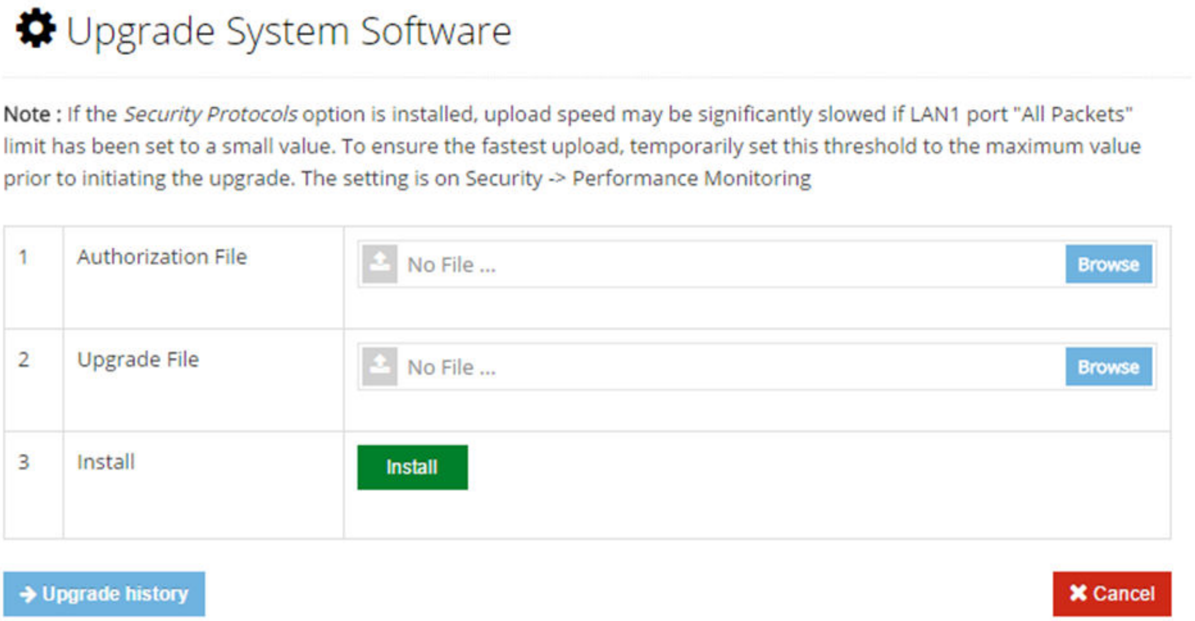
Console Port	
Baud Rate	○ 4800 bps ○ 9600 bps ○ 19.2 kbps ○ 38.4 kbps ○ 57.6 kbps ● 115.2 kbps
Data Bits	8
Parity	None
Stop Bits	1

5.3.7 Admin—Upgrade System Software Window

Use this window to upgrade system software.

Note:
The system reboots after the software is upgraded.

Figure 5-76. Admin—Upgrade System Software Window



Upgrade System Software

Note : If the *Security Protocols* option is installed, upload speed may be significantly slowed if LAN1 port "All Packets" limit has been set to a small value. To ensure the fastest upload, temporarily set this threshold to the maximum value prior to initiating the upgrade. The setting is on Security -> Performance Monitoring

1	Authorization File	No File ...
2	Upgrade File	No File ...
3	Install	

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.

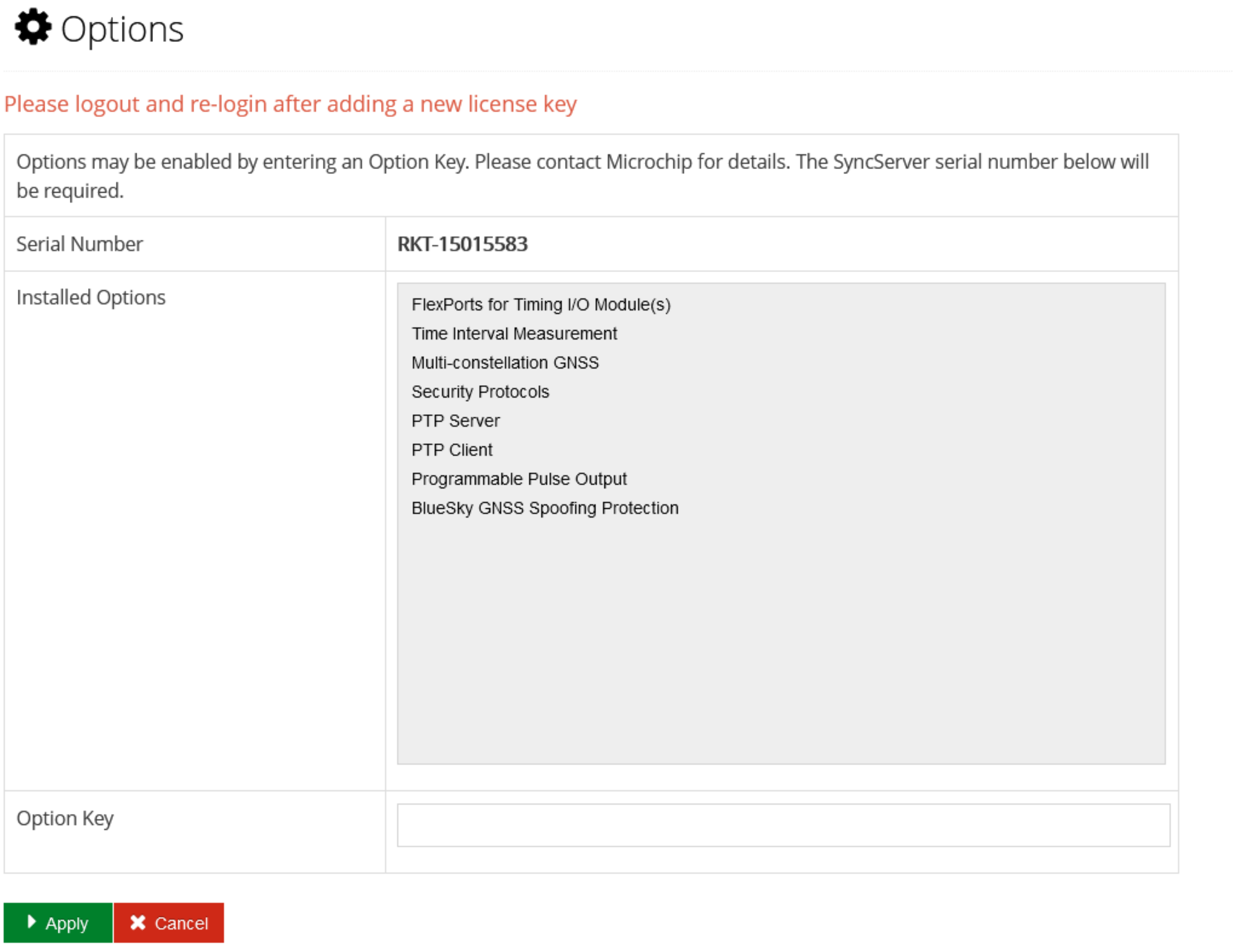
Notes:

- 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.
- 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.

5.3.8 Admin—Options Configuration Window

Use this window to view installed options and to enter option keys to enable SyncServer options.

Figure 5-77. Admin—Options Configuration Window



Options

Please logout and re-login after adding a new license key

Options may be enabled by entering an Option Key. Please contact Microchip for details. The SyncServer serial number below will be required.	
Serial Number	**RKT-15015583**
Installed Options	FlexPorts for Timing I/O Module(s) Time Interval Measurement Multi-constellation GNSS Security Protocols PTP Server PTP Client Programmable Pulse Output BlueSky GNSS Spoofing Protection
Option Key	

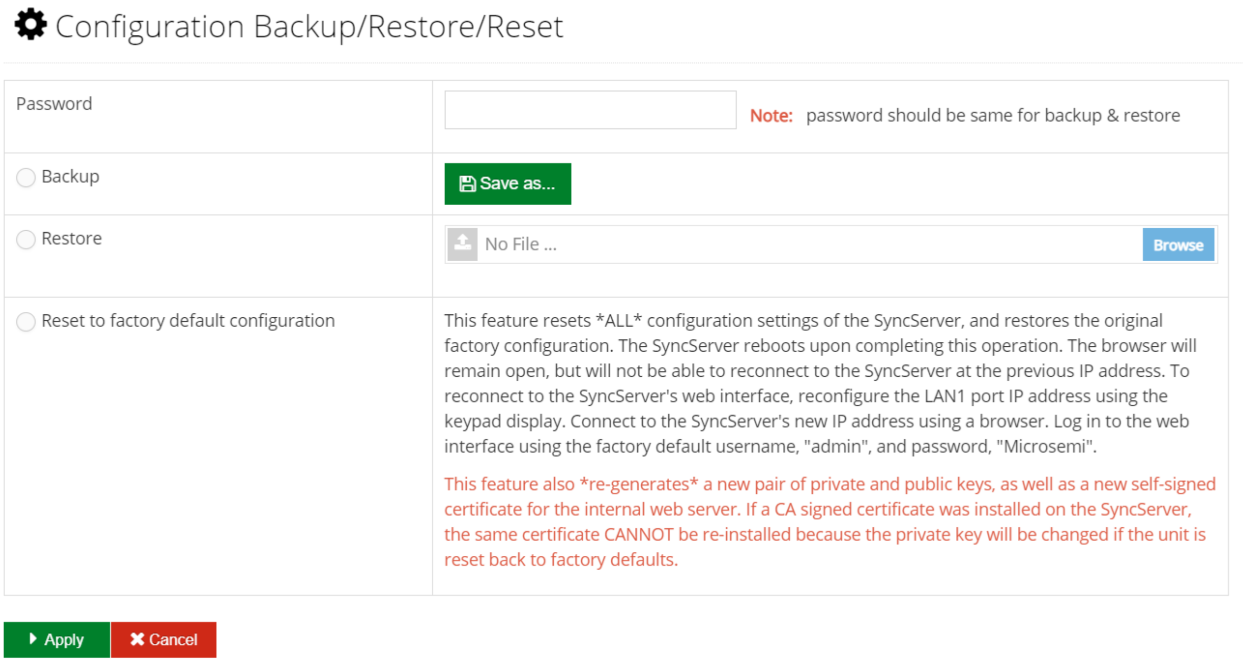
5.3.9 Admin—Configuration Backup/Restore/Reset

Use this window to back up, restore, or reset SyncServer S6x0 to factory configuration.

Notes:

- 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. Certificates are not saved in a backup file and are not affected by a configuration restore.
- If an HTTPS certificate was installed, the system will return to using the self-signed HTTPS certificate after a configuration reset to factory default. All self-signed, signed, and user-installed CA certificates are deleted during the factory default.

Figure 5-78. Admin—Factory Reset Window



Configuration Backup/Restore/Reset

Password	Note: password should be same for backup & restore
○ Backup	Save as...
○ Restore	No File ... Browse
○ Reset to factory default configuration	This feature resets *ALL* configuration settings of the SyncServer, and restores the original factory configuration. The SyncServer reboots upon completing this operation. The browser will remain open, but will not be able to reconnect to the SyncServer at the previous IP address. To reconnect to the SyncServer's web interface, reconfigure the LAN1 port IP address using the keypad display. Connect to the SyncServer's new IP address using a browser. Log in to the web interface using the factory default username, "admin", and password, "Microsemi". This feature also *re-generates* a new pair of private and public keys, as well as a new self-signed certificate for the internal web server. If a CA signed certificate was installed on the SyncServer, the same certificate CANNOT be re-installed because the private key will be changed if the unit is reset back to factory defaults.

5.4 Logs Configuration Windows

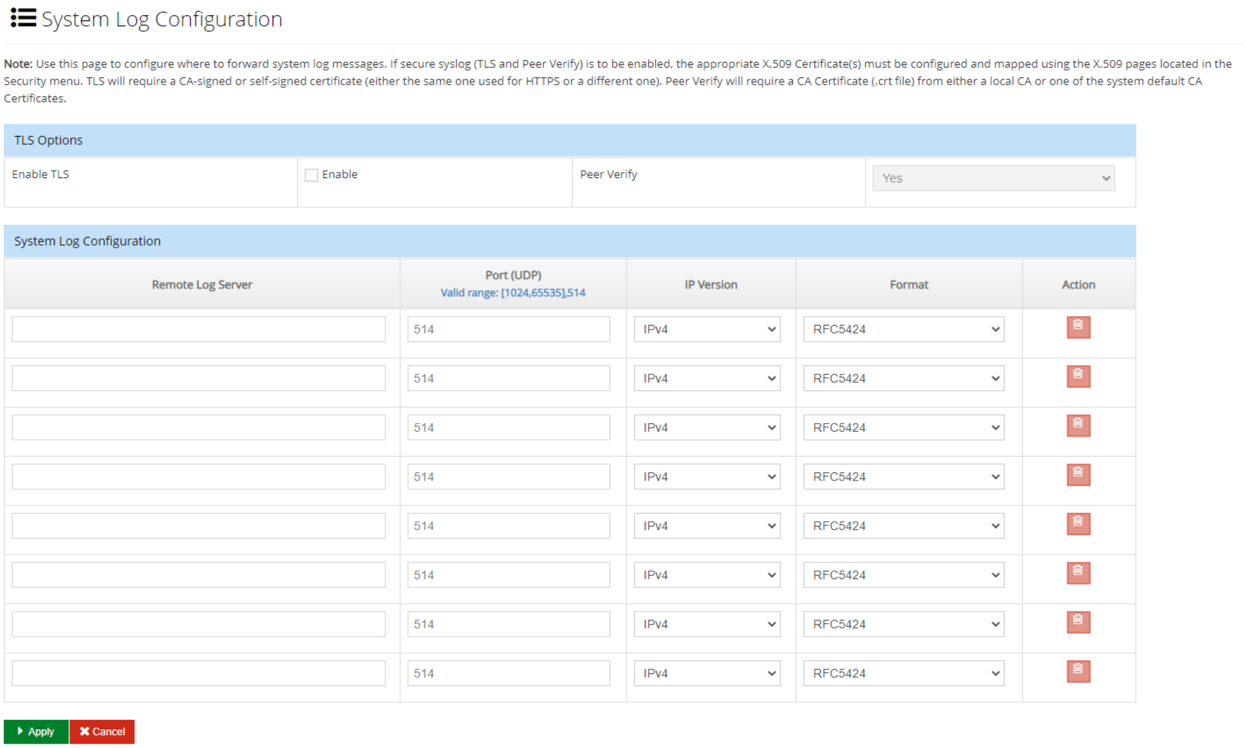
The logs rotate, and up to seven logs are kept. In release 2.0 or later, individual rotated log files can be selected. When seven logs have been created, the oldest is overwritten. The log rotate depends on size of 100k, but this is subject to change without notice.

5.4.1 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. The IP port, IP version (IPv4 or IPv6), and format (RFC5424 or RFC3164) can also be configured.
For secure syslog, TLS can be enabled. If peer-verify is enabled, then both the syslog server and SyncServer (syslog client) will both authenticate each other. If secure syslog (TLS and Peer Verify) is enabled, then the appropriate X.509 certificates must be configured and mapped using the X.509 pages on the Security menu. TLS requires a CA-signed or self-signed certificate. This can be shared with HTTPS or a separate one can be mapped. Peer Verify requires a CA certificate from either a local CA or one of the system default CA certifcates. These can be installed/viewed on the X.509 Certificate Authorities web page.

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 5-79. Logs—System Log Configuration Window



System Log Configuration

Note: Use this page to configure where to forward system log messages. If secure syslog (TLS and Peer Verify) is to be enabled, the appropriate X.509 Certificate(s) must be configured and mapped using the X.509 pages located in the Security menu. TLS will require a CA-signed or self-signed certificate (either the same one used for HTTPS or a different one). Peer Verify will require a CA Certificate (.crt file) from either a local CA or one of the system default CA Certificates.

TLS Options

Enable TLS	□ Enable	Peer Verify	Yes

System Log Configuration

Remote Log Server	Port (UDP) Valid range: [1024,65535],514	IP Version	Format	Action
	514	IPv4	RFC5424	🗑
	514	IPv4	RFC5424	🗑
	514	IPv4	RFC5424	🗑
	514	IPv4	RFC5424	🗑
	514	IPv4	RFC5424	🗑
	514	IPv4	RFC5424	🗑
	514	IPv4	RFC5424	🗑
	514	IPv4	RFC5424	🗑

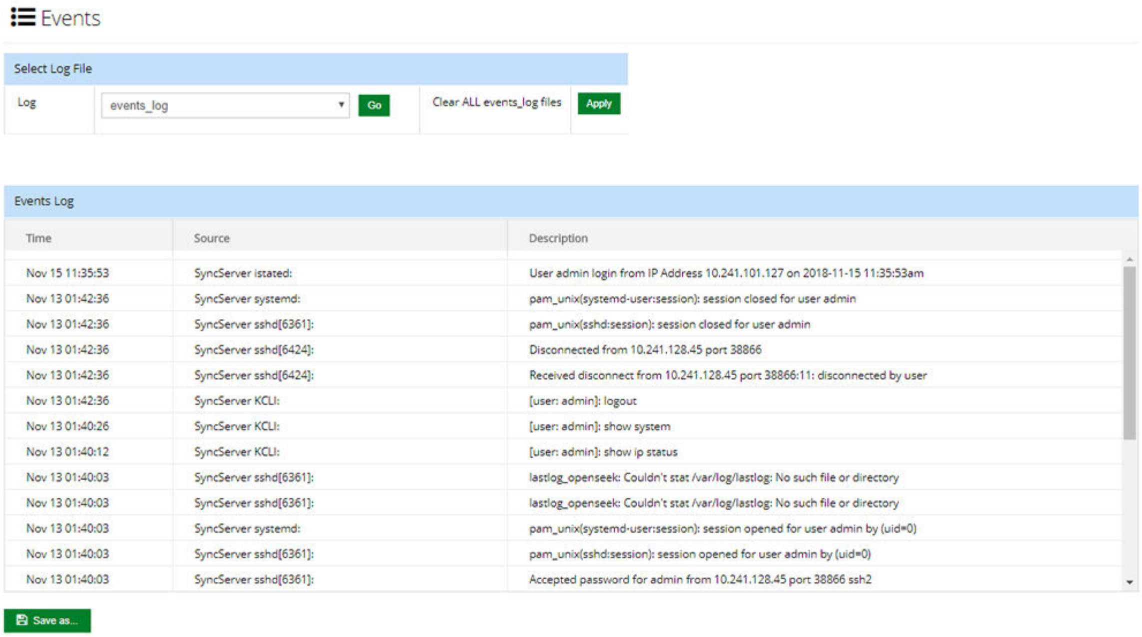
A remote syslog server can be configured with this window and all logs can then be stored on the remote server.

5.4.2 Logs—Events Log Configuration Window

Use this window to view and save the events log.

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

Figure 5-80. Logs—Events Window



Events

Select Log File

Log	events_log	Go	Clear ALL events_log files	Apply

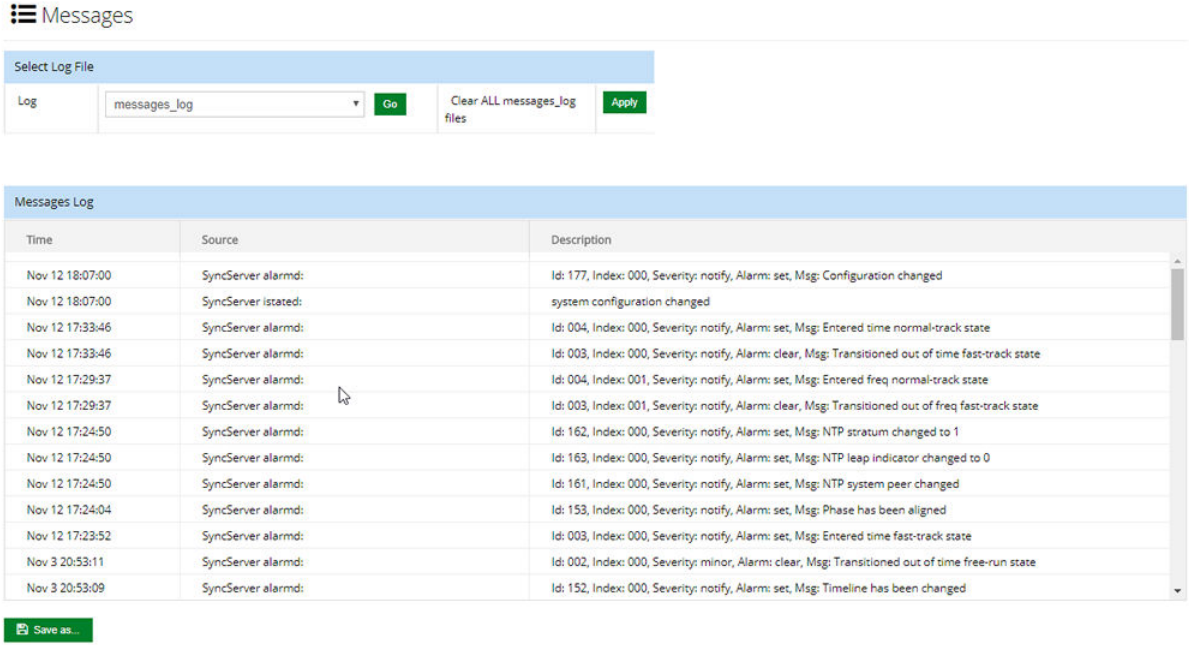
Events Log

Time	Source	Description
Nov 15 11:35:53	SyncServer istated:	User admin login from IP Address 10.241.101.127 on 2018-11-15 11:35:53am
Nov 13 01:42:36	SyncServer systemd:	pam_unix(systemd-user:session): session closed for user admin
Nov 13 01:42:36	SyncServer sshd[6361]:	pam_unix(sshd:session): session closed for user admin
Nov 13 01:42:36	SyncServer sshd[6424]:	Disconnected from 10.241.128.45 port 38866
Nov 13 01:42:36	SyncServer sshd[6424]:	Received disconnect from 10.241.128.45 port 38866:11: disconnected by user
Nov 13 01:42:36	SyncServer KCLI:	[user: admin]: logout
Nov 13 01:40:26	SyncServer KCLI:	[user: admin]: show system
Nov 13 01:40:12	SyncServer KCLI:	[user: admin]: show ip status
Nov 13 01:40:03	SyncServer sshd[6361]:	lastlog_openseek: Couldn't stat /var/log/lastlog: No such file or directory
Nov 13 01:40:03	SyncServer sshd[6361]:	lastlog_openseek: Couldn't stat /var/log/lastlog: No such file or directory
Nov 13 01:40:03	SyncServer systemd:	pam_unix(systemd-user:session): session opened for user admin by (uid=0)
Nov 13 01:40:03	SyncServer sshd[6361]:	pam_unix(sshd:session): session opened for user admin by (uid=0)
Nov 13 01:40:03	SyncServer sshd[6361]:	Accepted password for admin from 10.241.128.45 port 38866 ssh2

5.4.3 Logs—Messages Window

Use this window to view and save the message log.

Figure 5-81. Logs—Messages Window



Time	Source	Description
Nov 12 18:07:00	SyncServer alarmd:	Id: 177, Index: 000, Severity: notify, Alarm: set, Msg: Configuration changed
Nov 12 18:07:00	SyncServer istated:	system configuration changed
Nov 12 17:33:46	SyncServer alarmd:	Id: 004, Index: 000, Severity: notify, Alarm: set, Msg: Entered time normal-track state
Nov 12 17:33:46	SyncServer alarmd:	Id: 003, Index: 000, Severity: notify, Alarm: clear, Msg: Transitioned out of time fast-track state
Nov 12 17:29:37	SyncServer alarmd:	Id: 004, Index: 001, Severity: notify, Alarm: set, Msg: Entered freq normal-track state
Nov 12 17:29:37	SyncServer alarmd:	Id: 003, Index: 001, Severity: notify, Alarm: clear, Msg: Transitioned out of freq fast-track state
Nov 12 17:24:50	SyncServer alarmd:	Id: 162, Index: 000, Severity: notify, Alarm: set, Msg: NTP stratum changed to 1
Nov 12 17:24:50	SyncServer alarmd:	Id: 163, Index: 000, Severity: notify, Alarm: set, Msg: NTP leap indicator changed to 0
Nov 12 17:24:50	SyncServer alarmd:	Id: 161, Index: 000, Severity: notify, Alarm: set, Msg: NTP system peer changed
Nov 12 17:24:04	SyncServer alarmd:	Id: 153, Index: 000, Severity: notify, Alarm: set, Msg: Phase has been aligned
Nov 12 17:23:52	SyncServer alarmd:	Id: 003, Index: 000, Severity: notify, Alarm: set, Msg: Entered time fast-track state
Nov 3 20:53:11	SyncServer alarmd:	Id: 002, Index: 000, Severity: minor, Alarm: clear, Msg: Transitioned out of time free-run state
Nov 3 20:53:09	SyncServer alarmd:	Id: 152, Index: 000, Severity: notify, Alarm: set, Msg: Timeline has been changed

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

5.5 Option Slot A/Slot B Configuration Windows

5.5.1 Options Slot A and B Configuration Window—Timing I/O Module

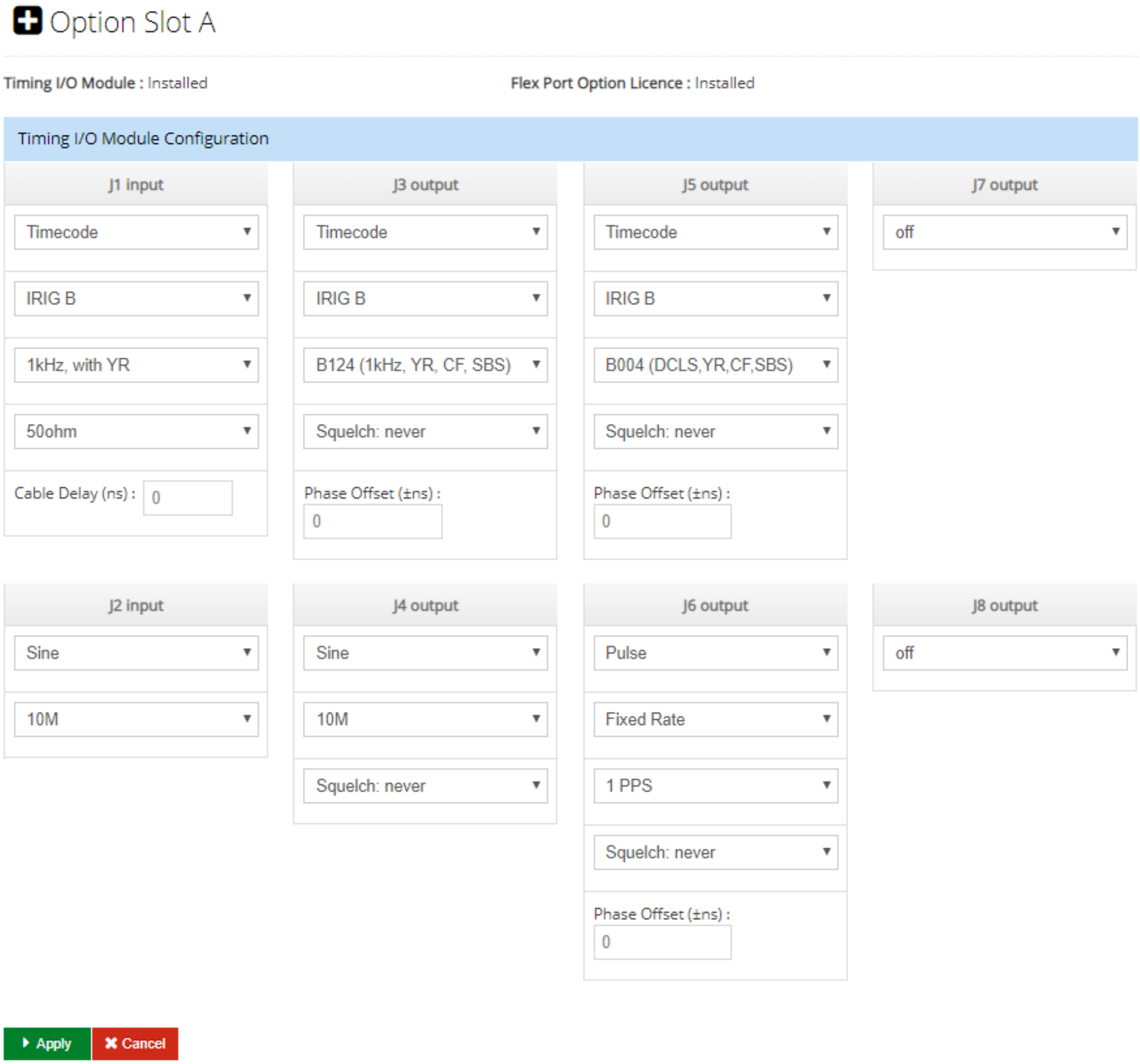
Use this window to configure the module in options slots A and B. See 6.4.2. Provisioning IRIG Inputs on Timing I/O Module, 6.4.3. Provisioning Sine Wave Inputs on Timing I/O Module, and 6.8.9. Provisioning Outputs on Timing I/O Module.

The configurations on the Timing I/O module configuration page are fixed unless the optional flex timing license is installed.

Notes:

- Option slots A and B are only available with SyncServer S650.
- For LPN and ULPN modules, even if 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 1 PPS may have phase adjustments. This impacts the coherency between the 1 PPS and the LPN/ULPN 10 MHz outputs. The LPN/ULPN outputs phase-jam and/or slew to the new 1 PPS phase.
- If the programmable pulse license is installed, then this feature is available on J7.

Figure 5-82. Options Slot A Configuration Window Showing Timing I/O Module



Option Slot A

Timing I/O Module : Installed

Flex Port Option Licence : Installed

Timing I/O Module Configuration

J1 input
- Timecode
- IRIG B
- 1kHz, with YR
- 50ohm
- Cable Delay (ns) : 0

J3 output
- Timecode
- IRIG B
- B124 (1kHz, YR, CF, SBS)
- Squelch: never
- Phase Offset (±ns) : 0

J5 output
- Timecode
- IRIG B
- B004 (DCLS,YR,CF,SBS)
- Squelch: never
- Phase Offset (±ns) : 0

J7 output
- off

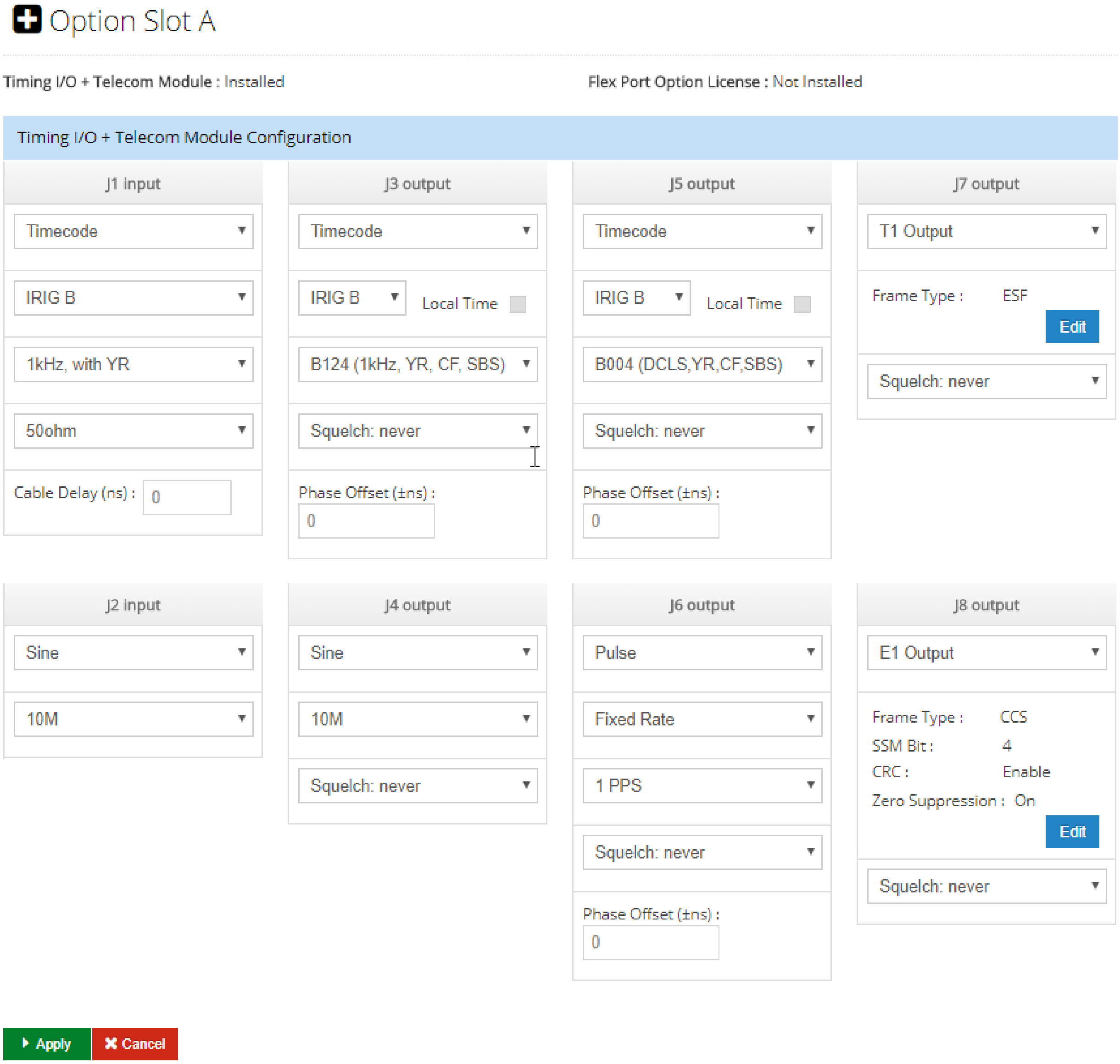
J2 input
- Sine
- 10M

J4 output
- Sine
- 10M
- Squelch: never

J6 output
- Pulse
- Fixed Rate
- 1 PPS
- Squelch: never
- Phase Offset (±ns) : 0

J8 output
- off

Figure 5-83. Options Slot A Configuration Window—Telecom Module Installed



Option Slot A

Timing I/O + Telecom Module : Installed

Flex Port Option License : Not Installed

Timing I/O + Telecom Module Configuration

J1 input
- Timecode
- IRIG B
- 1kHz, with YR
- 50ohm
- Cable Delay (ns) : 0

J3 output
- Timecode
- IRIG B — Local Time □
- B124 (1kHz, YR, CF, SBS)
- Squelch: never
- Phase Offset (±ns) : 0

J5 output
- Timecode
- IRIG B — Local Time □
- B004 (DCLS,YR,CF,SBS)
- Squelch: never
- Phase Offset (±ns) : 0

J7 output
- T1 Output
- Frame Type : ESF
- Squelch: never

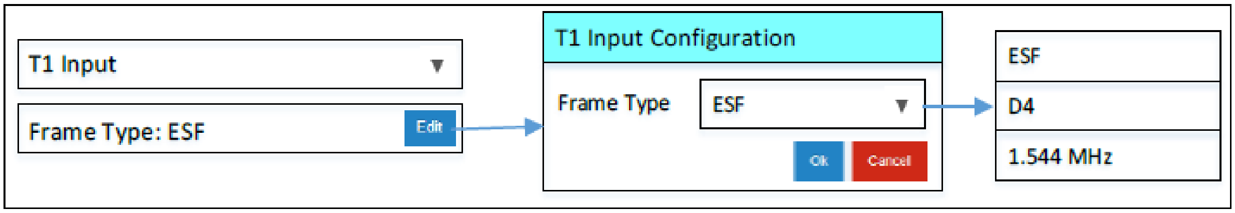
J2 input
- Sine
- 10M

J4 output
- Sine
- 10M
- Squelch: never

J6 output
- Pulse
- Fixed Rate
- 1 PPS
- Squelch: never
- Phase Offset (±ns) : 0

J8 output
- E1 Output
- Frame Type : CCS
- SSM Bit : 4
- CRC : Enable
- Zero Suppression : On
- Squelch: never

Figure 5-84. Options Slot A Configuration Window—Telecom Module–T1 Input Choices



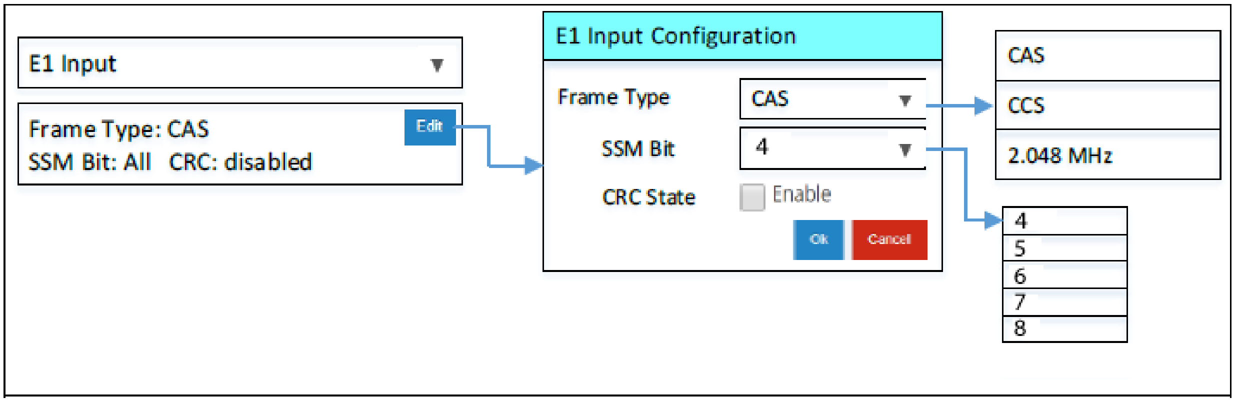
T1 Input

Frame Type: ESF

T1 Input Configuration

Frame Type: ESF

Figure 5-85. Options Slot A Configuration Window—Telecom Module–E1 Input Choices

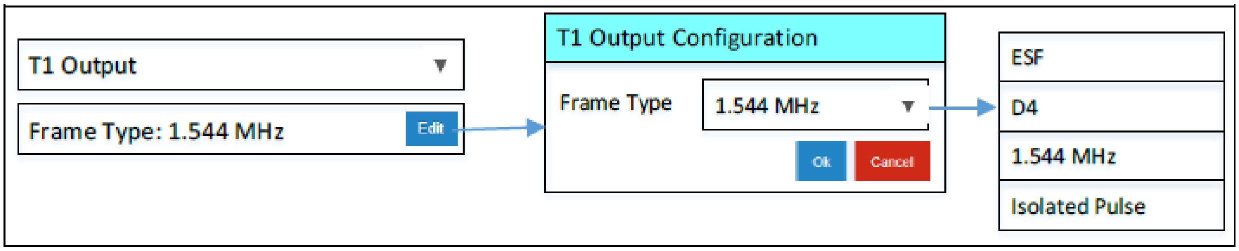

E1 Input

Frame Type: CAS
SSM Bit: All CRC: disabled

E1 Input Configuration

Frame Type: CAS
SSM Bit: 4
CRC State: □ Enable

Figure 5-86. Options Slot A Configuration Window—Telecom Module T1 Output Choices

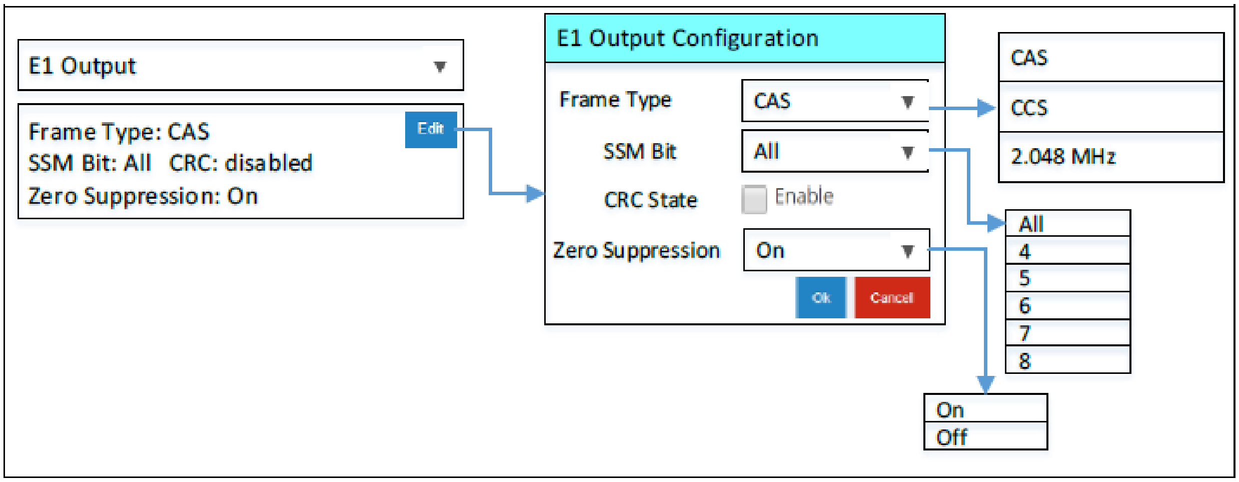

T1 Output

Frame Type: 1.544 MHz

T1 Output Configuration

Frame Type: 1.544 MHz

Figure 5-87. Options Slot A Configuration Window—Telecom Module E1 Output Choices

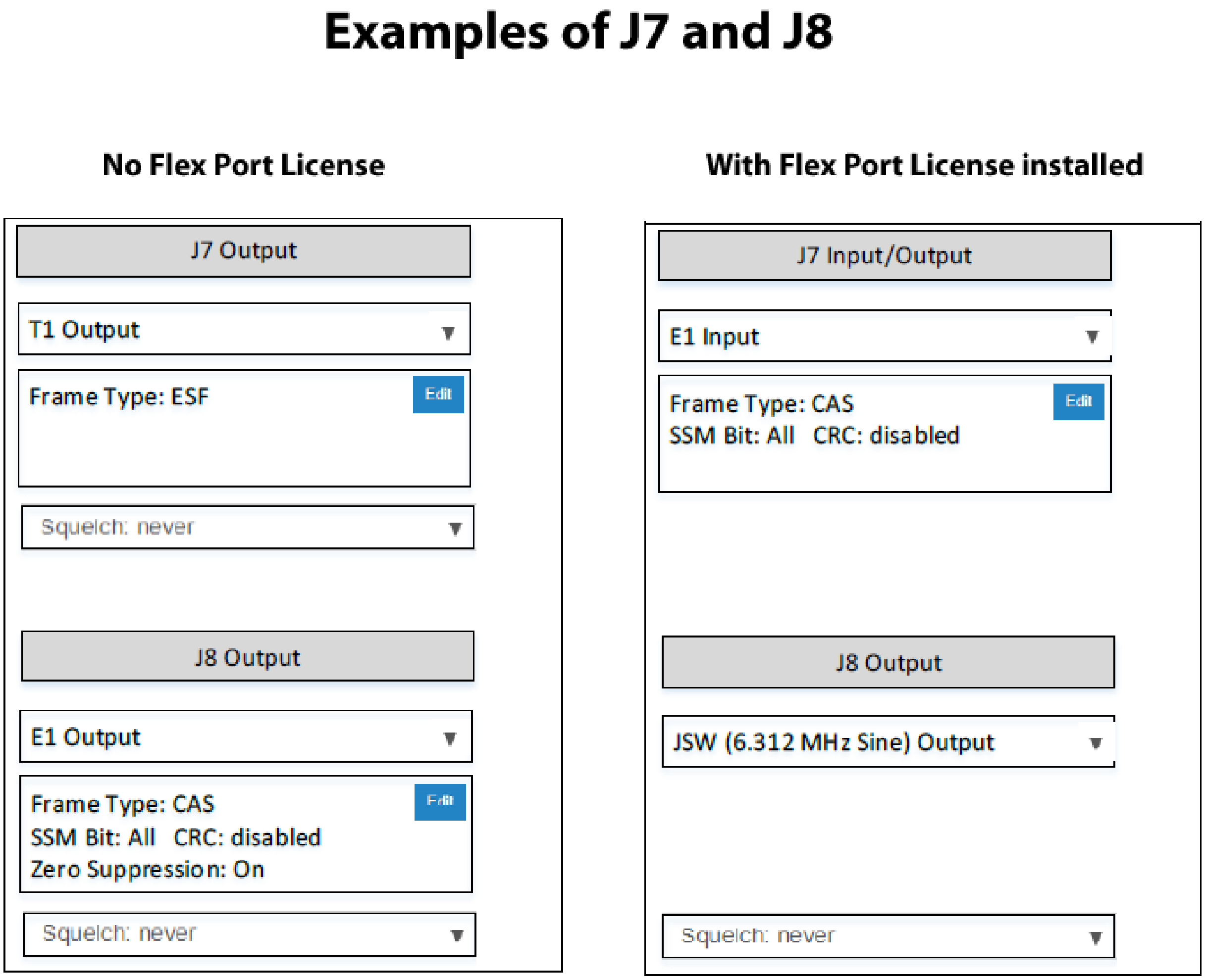

E1 Output

Frame Type: CAS
SSM Bit: All CRC: disabled
Zero Suppression: On

E1 Output Configuration

Frame Type: CAS
SSM Bit: All
CRC State: □ Enable
Zero Suppression: On

Figure 5-88. Telecom Module—J7 and J8 Examples–Flex Port License



Examples of J7 and J8

No Flex Port License

J7 Output

T1 Output ▼

Frame Type: ESF

Squelch: never ▼

J8 Output

E1 Output ▼

Frame Type: CAS
SSM Bit: All CRC: disabled
Zero Suppression: On

Squelch: never ▼

With Flex Port License installed

J7 Input/Output

E1 Input ▼

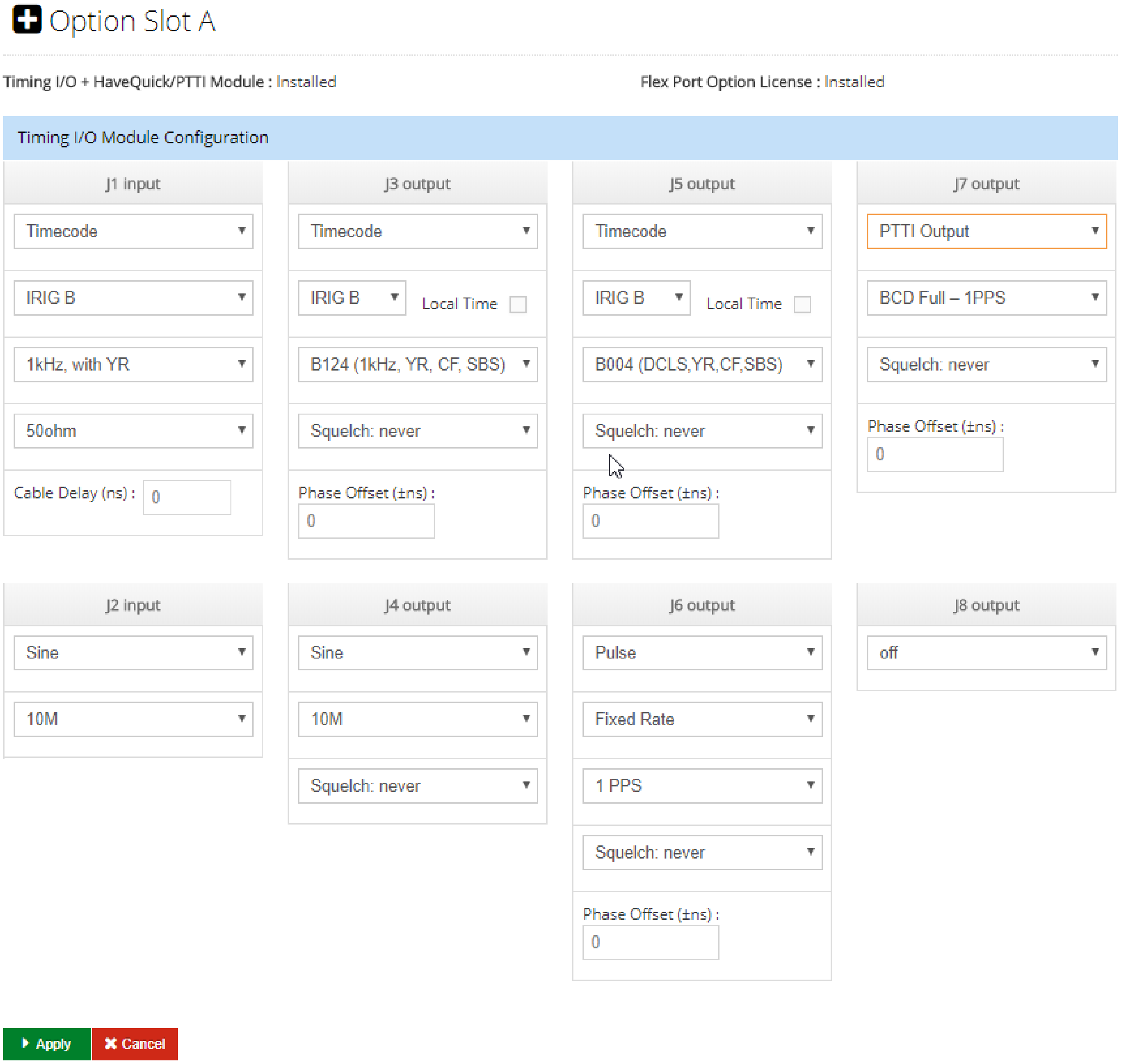
Frame Type: CAS
SSM Bit: All CRC: disabled

J8 Output

JSW (6.312 MHz Sine) Output ▼

Squelch: never ▼

Figure 5-89. Options Slot A Configuration Window—HaveQuick/PTTI Module Installed



Option Slot A

Timing I/O + HaveQuick/PTTI Module : Installed

Flex Port Option License : Installed

Timing I/O Module Configuration

J1 input: Timecode; IRIG B; 1kHz, with YR; 50ohm; Cable Delay (ns) : 0

J3 output: Timecode; IRIG B; Local Time □; B124 (1kHz, YR, CF, SBS); Squelch: never; Phase Offset (±ns) : 0

J5 output: Timecode; IRIG B; Local Time □; B004 (DCLS,YR,CF,SBS); Squelch: never; Phase Offset (±ns) : 0

J7 output: PTTI Output; BCD Full – 1PPS; Squelch: never; Phase Offset (±ns) : 0

J2 input: Sine; 10M

J4 output: Sine; 10M; Squelch: never

J6 output: Pulse; Fixed Rate; 1 PPS; Squelch: never; Phase Offset (±ns) : 0

J8 output: off

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 5-17. Squelch Settings

Squelch Setting	Function	Notes
Never	Clock state does not cause squelch.	—
If not locked	Output occurs only 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 occurs only when appropriate clock state is “Locked”, “Bridging”, or “Holdover”	—
In warmup	Squelch output from power-up until unit comes out of warmup. It is not squelched after that.	Output first turns on when “freerun” is entered.
In warmup / freerun	Prevent output from power-up until the unit comes out of freerun. Once (if) it does, it stays on as these states can never be re-entered.	Output is turned on when “Locking” is entered.
In warmup / freerun/ locking	Prevent output from power-up until unit comes out of “Locking” (internal state = “fast”). In other words, do not output until first lock from power-up, but thereafter always output.	These three states are only encountered following power-up or reboot. Once Locked state is attained, none of these states ever occur again.

Table 5-18. 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 might 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 persists if no qualified 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.

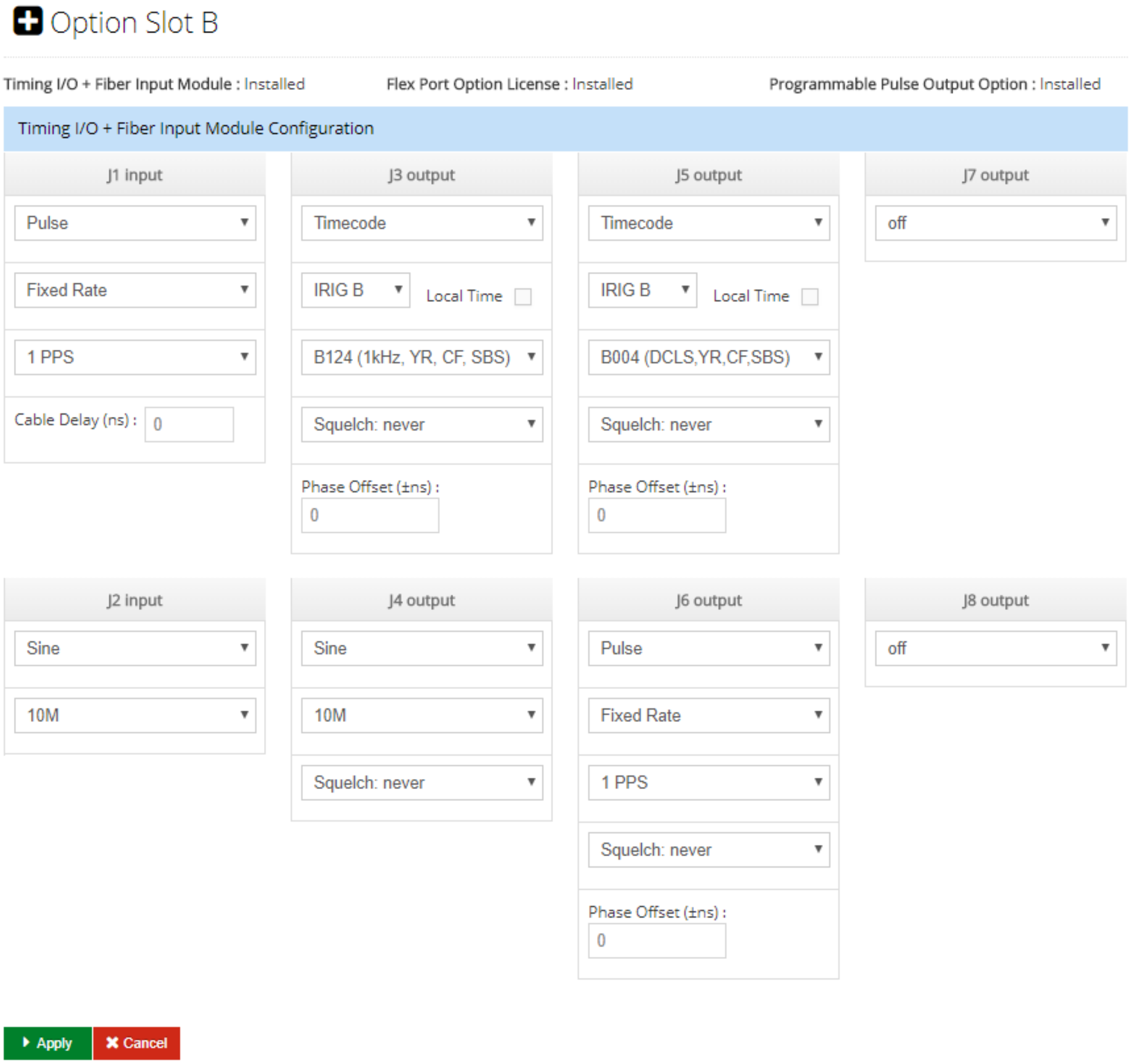
...........continued

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

5.5.2 Options Slot B Configuration Window

Use this window to configure the module in options slot B.

Figure 5-90. Slot B—Fiber Input Module, Flex Port, and Pulse Output Options Installed



Option Slot B

Timing I/O + Fiber Input Module : Installed

Flex Port Option License : Installed

Programmable Pulse Output Option : Installed

Timing I/O + Fiber Input Module Configuration

J1 input
- Pulse
- Fixed Rate
- 1 PPS
- Cable Delay (ns) : 0

J3 output
- Timecode
- IRIG B   Local Time □
- B124 (1kHz, YR, CF, SBS)
- Squelch: never
- Phase Offset (±ns) : 0

J5 output
- Timecode
- IRIG B   Local Time □
- B004 (DCLS,YR,CF,SBS)
- Squelch: never
- Phase Offset (±ns) : 0

J7 output
- off

J2 input
- Sine
- 10M

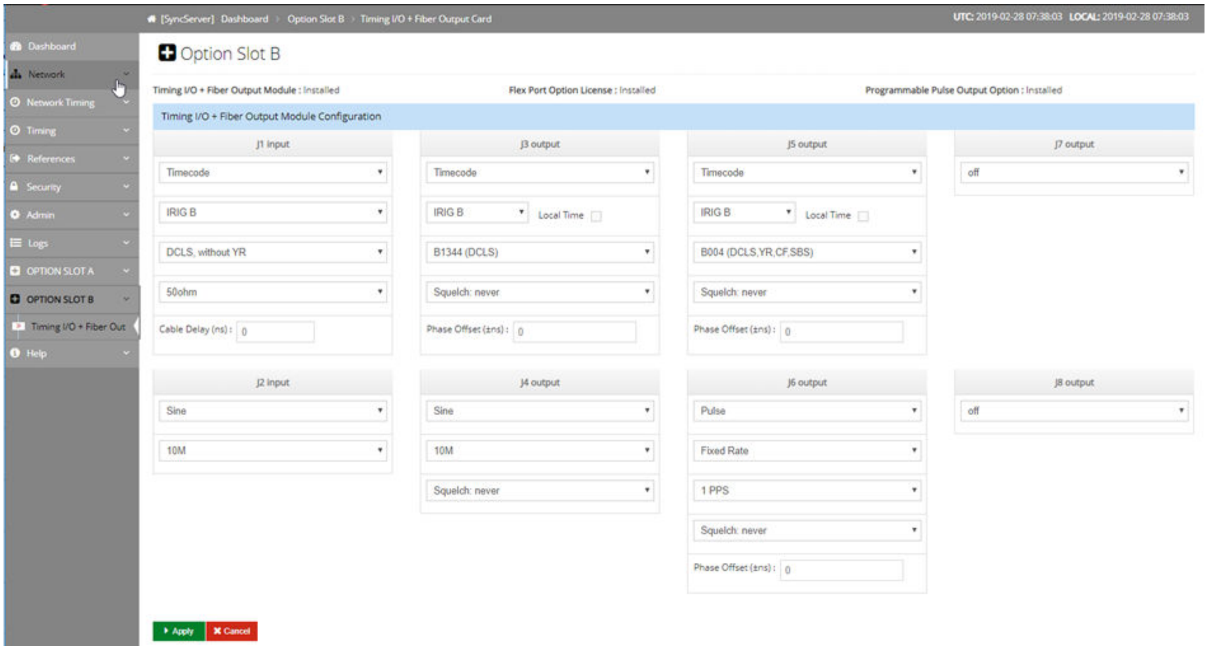
J4 output
- Sine
- 10M
- Squelch: never

J6 output
- Pulse
- Fixed Rate
- 1 PPS
- Squelch: never
- Phase Offset (±ns) : 0

J8 output
- off

Note: Option slot B is available only with SyncServer S650.

Figure 5-91. Slot B—Fiber Output Module, Flex Port, and Pulse Output Options Installed



UTC: 2019-02-28 07:38:03 LOCAL: 2019-02-28 07:38:03

Option Slot B

Timing I/O + Fiber Output Module : Installed

Flex Port Option License : Installed

Programmable Pulse Output Option : Installed

Timing I/O + Fiber Output Module Configuration

J1 input: Timecode; IRIG B; DCLS, without YR; 50ohm; Cable Delay (ns) : 0

J3 output: Timecode; IRIG B; Local Time □; B1344 (DCLS); Squelch: never; Phase Offset (±ns) : 0

J5 output: Timecode; IRIG B; Local Time □; B004 (DCLS,YR,CF,SBS); Squelch: never; Phase Offset (±ns) : 0

J7 output: off

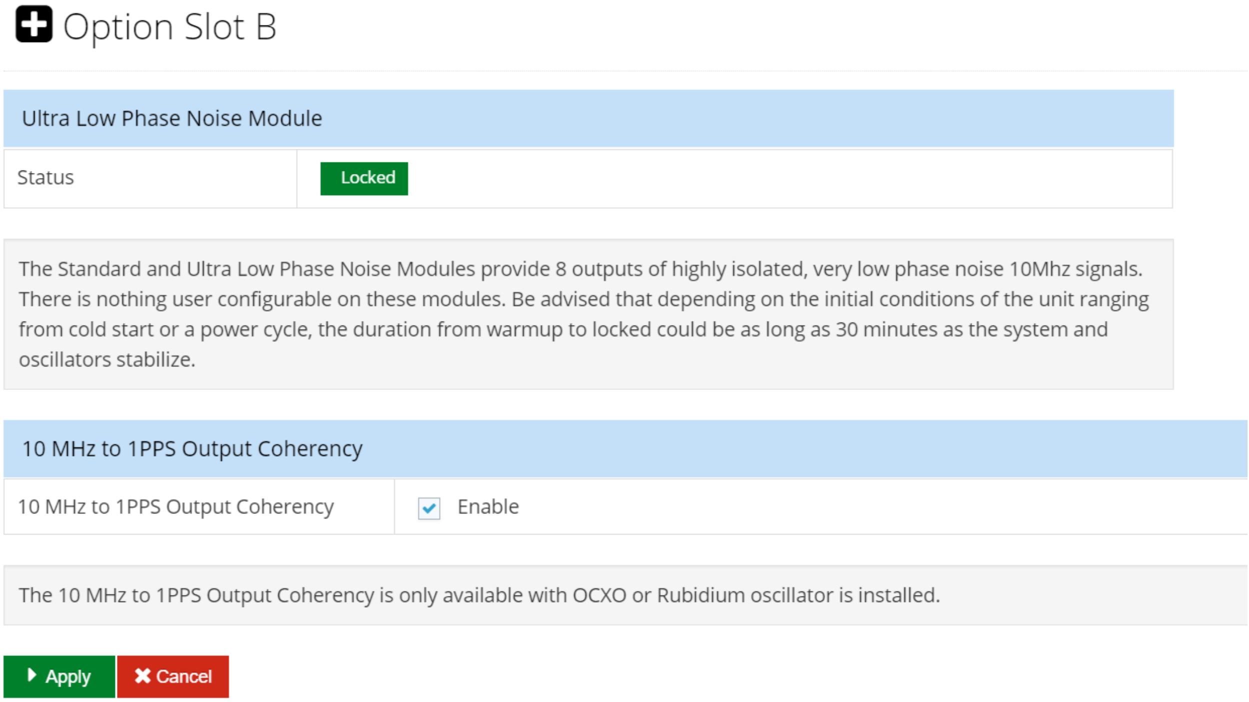
J2 input: Sine; 10M

J4 output: Sine; 10M; Squelch: never

J6 output: Pulse; Fixed Rate; 1 PPS; Squelch: never; Phase Offset (±ns) : 0

J8 output: off

Figure 5-92. Slot B—LPN



Option Slot B

Ultra Low Phase Noise Module

Status	Locked

The Standard and Ultra Low Phase Noise Modules provide 8 outputs of highly isolated, very low phase noise 10Mhz signals. There is nothing user configurable on these modules. Be advised that depending on the initial conditions of the unit ranging from cold start or a power cycle, the duration from warmup to locked could be as long as 30 minutes as the system and oscillators stabilize.

10 MHz to 1PPS Output Coherency

10 MHz to 1PPS Output Coherency	☑ Enable

The 10 MHz to 1PPS Output Coherency is only available with OCXO or Rubidium oscillator is installed.

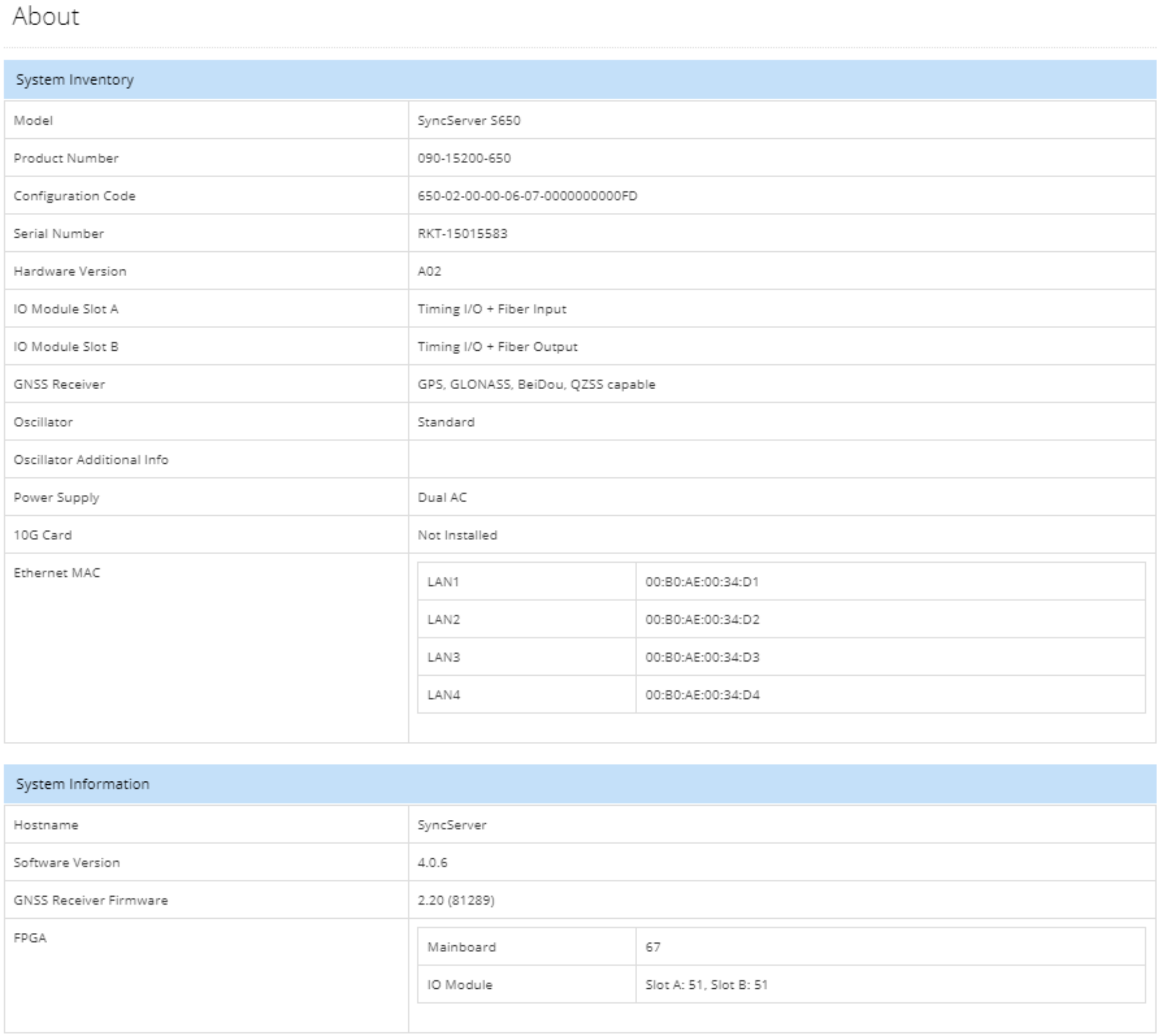
Note: During initial lock and holdover recovery, there might be phase adjustments to the system 1 PPS. The 1 PPS to 10 MHz coherency is affected while the LPN/ULPN outputs slew to the new 1 PPS phase.

5.6 Help Windows

5.6.1 About Window

Use this window to view information about the unit.

Figure 5-93. Help—About Window



About

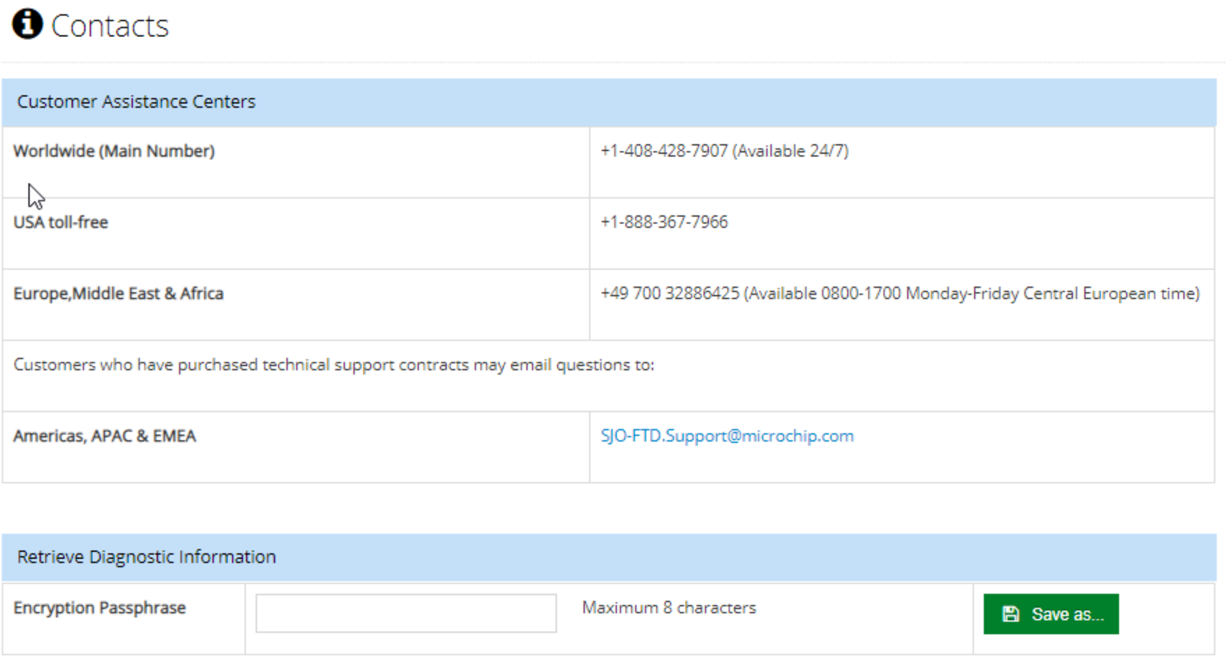
System Inventory	
Model	SyncServer S650
Product Number	090-15200-650
Configuration Code	650-02-00-00-06-07-0000000000FD
Serial Number	RKT-15015583
Hardware Version	A02
IO Module Slot A	Timing I/O + Fiber Input
IO Module Slot B	Timing I/O + Fiber Output
GNSS Receiver	GPS, GLONASS, BeiDou, QZSS capable
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

5.6.2 Contact Window

Use this window to view information about how to contact Customer Assistance Centers.

Figure 5-94. Help—Contacts Window



Contacts

Customer Assistance Centers	
Worldwide (Main Number)	+1-408-428-7907 (Available 24/7)
USA toll-free	+1-888-367-7966
Europe,Middle East & Africa	+49 700 32886425 (Available 0800-1700 Monday-Friday Central European time)
Customers who have purchased technical support contracts may email questions to:	
Americas, APAC & EMEA	SJO-FTD.Support@microchip.com

Retrieve Diagnostic Information			
Encryption Passphrase		Maximum 8 characters	

6. Provisioning

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

6.1 Establishing a Connection to SyncServer S6x0

SyncServer S6x0 can be brought on line in the following ways:

- 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.
- Use the front panel to input the IP address, subnet mask and gateway.
- Use the front panel to turn on DHCP and review the assigned address.
- 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.

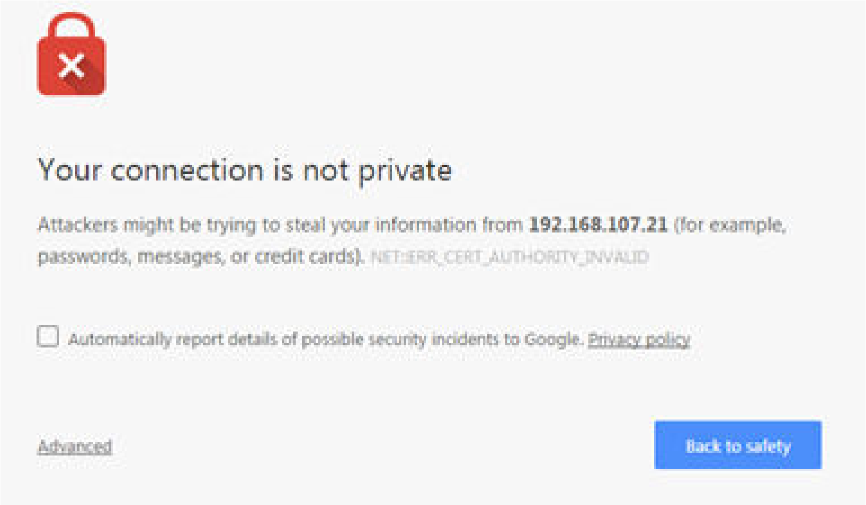
6.1.1.1 HTTPS

A certificate is required with HTTPS. By default, 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 SyncServer S6x0. You must allow the browser to continue. The actual messages and screens are 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.

If you have the security license, you can create a CSR, and then install a signed certificate to eliminate these browser warnings.

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

Figure 6-1. Example—Chrome Browser HTTPS Warning



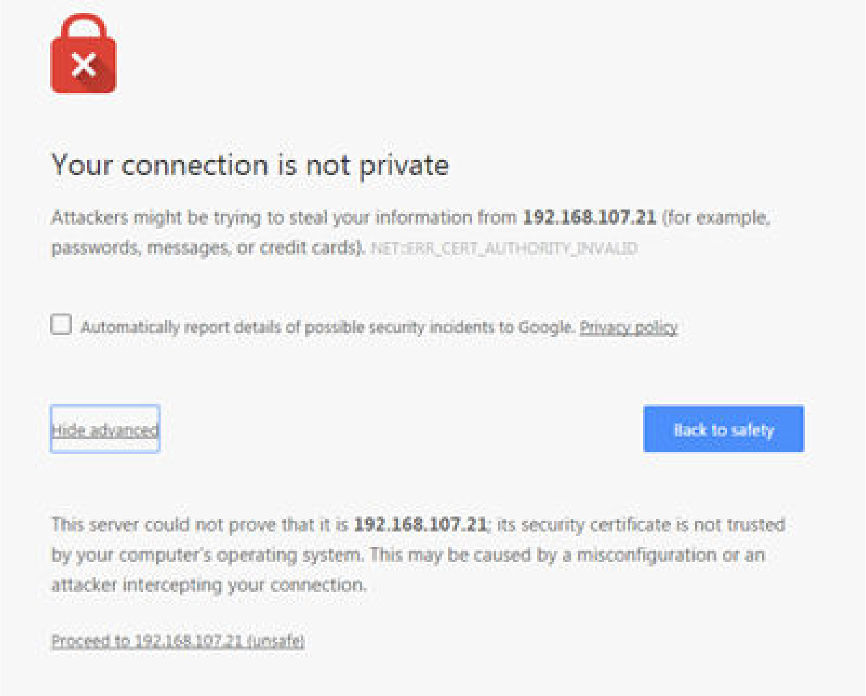
Your connection is not private

Attackers might be trying to steal your information from **192.168.107.21** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically report details of possible security incidents to Google. Privacy policy

Click the **Advanced** button to bring up the message shown in the following figure.

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



Your connection is not private

Attackers might be trying to steal your information from **192.168.107.21** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

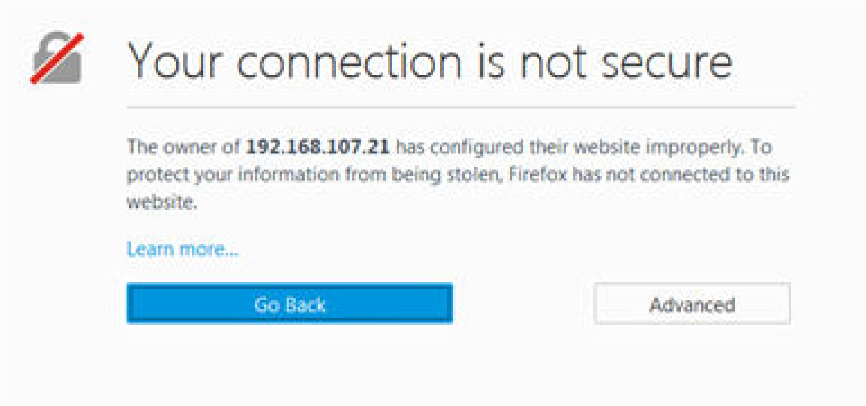
□ Automatically report details of possible security incidents to Google. Privacy policy

This server could not prove that it is **192.168.107.21**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.107.21 (unsafe)

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

Figure 6-3. Example—Firefox Browser HTTPS Warning

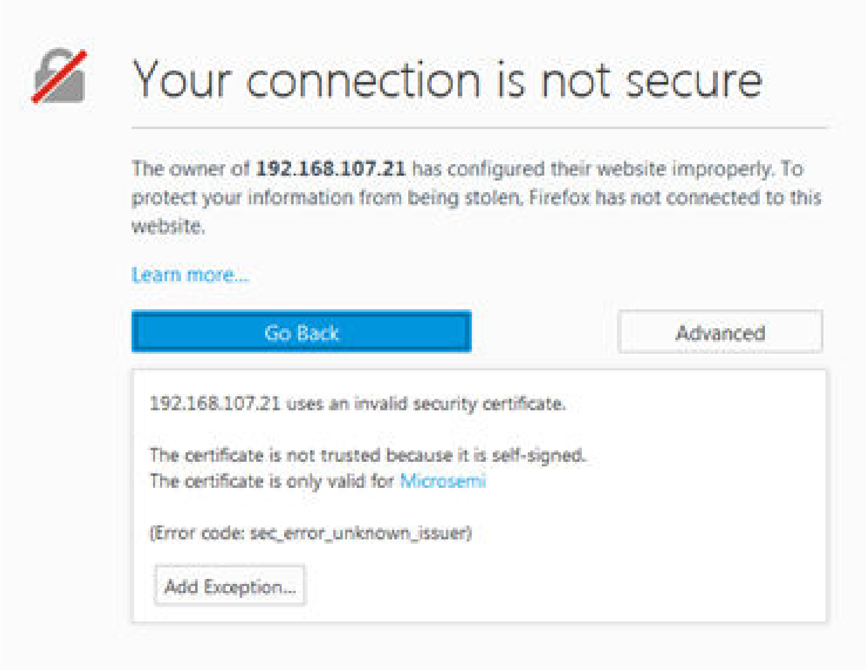


Your connection is not secure

The owner of **192.168.107.21** has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Click the **Advanced** button to bring up the message shown in the following figure.

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



Your connection is not secure

The owner of **192.168.107.21** has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

192.168.107.21 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.
The certificate is only valid for Microsemi

(Error code: sec_error_unknown_issuer)

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 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 SyncServer S6x0 to a terminal or a computer with terminal emulation through a straight through serial cable:

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 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 appears. 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.

The default user name is **admin**. The default password: Microsemi.

To avoid unauthorized access, you must change the default password.

For information on restricting user access, see the following section.

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, including administrators have the same privileges.

Use the procedures in this section to manage user access to 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
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. Usernames must start with an alpha character.

- abcdefghijklmnopqrstuvwxyz
- 0123456789
- _

  There are a maximum of 16 users, including admin user.
- Passwords must be at least eight characters (maximum of 64 characters), and must include at least one upper-case, one lower-case, one number, and one special character.
- The following characters are not allowed: (', “, <, >, &,), and $.

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
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 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
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–LAN4 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 SyncServer S6x0 advertises connection speeds of 100/1000M. You can also select a connection speed for a port of 100M or 1000M to configure the speed used by auto-negotiation.

The optional 10G Ethernet ports LAN5–LAN6 are always 10G.

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

SyncServer S6x0 supports static and 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.

Notes:

- The LAN1 interface must not be configured with the same address as any of the other Ethernet ports. If this is done, then network access can 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, then these interfaces do not function properly.
- If using a gateway, then all IP interfaces must be configured with the proper gateway IP address and subnet mask. If not using a gateway, then configure 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.
- SyncServer does not use a new DHCP server until the current DHCP lease expires. To force 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, 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.

SyncServer 6x0 does not contain a battery-backed real-time clock. Therefore, it always boots up with a default value for the system time. This time is 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 is used for the first log entries when booting up the unit. The time changes to local time during the boot-up process if a time zone has been configured.

The system monitors 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 is used. This is specified on the 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.

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 must 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 (for example, 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.

Important: The cable delay must 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 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 later 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 SyncServer S650.

Notes:

- A Flex Port Option license is required for full configurability of all BNC connectors on the Timing I/O module.
- The system automatically detects and decodes the modulation frequency of AM-modulated IRIG inputs, regardless of the configured AM modulation frequency. The clockAccuracy value is based on the configured AM modulation frequency and not the actual input signal modulation frequency.
- If an IRIG input is not consistently qualified using the 50Ω 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 one of the following IRIG inputs: – DCLS, without YR – DCLS, with YR – 1 kHz, without YR – 10 kHz, with YR – 10 kHz, without YR – 1 kHz, with YR – B1344, DCLS – B1344, 1 kHz – 100 Hz, with YR – C37.118.1 (DCLS) 3. For Pulse, use the dropdown box to select 1 PPS or 10 MPPS. 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 SyncServer S650.

Note: A FlexPort 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/E1 input is available for port J7 of the Timing I/O Telecom module with SyncServer S650.

Notes:

- On E1 or T1 signals that support SSM, SyncServer decodes the SSM. If the SSM corresponds to a value worse than the internal oscillator, then the signal is disqualified. If the input signal does not support SSM, then the highest quality level is assumed for the input. For details, see 13. PQL Mapping.

  The following signals support SSM:
  - T1 with ESF framing
  - E1 with CAS or CCS (CRC enabled).
- A FlexPort 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 FlexPort 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 FlexPort 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 following are the specifically supported HaveQuick codes:

- 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 eight TFOM bits at the end of the code.

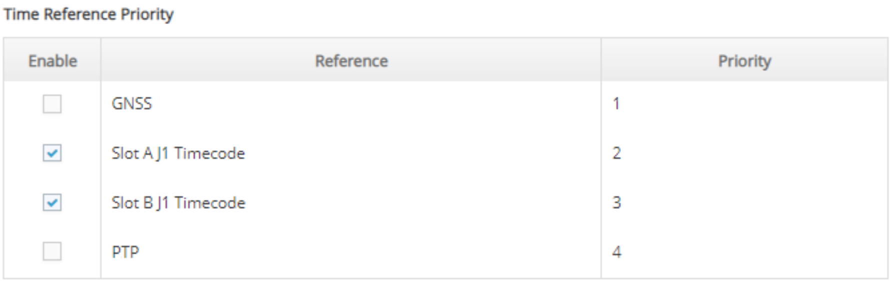
Every selected code is connected to BNC at J1. The function is to provide ToD information into S6xx.

Precise alignment can be 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). If "HaveQuick J1 only" is selected, then only the J1 input must be connected and the system will derive timing from the J1 signal.

Using the Web interface, perform the following steps 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 following figure shows the relevant portion of the form. In this case, as the HaveQuick/PTTI module is in slot A, only the slot A J1 Timecode must be enabled.
   Select **Apply** to complete the configuration.

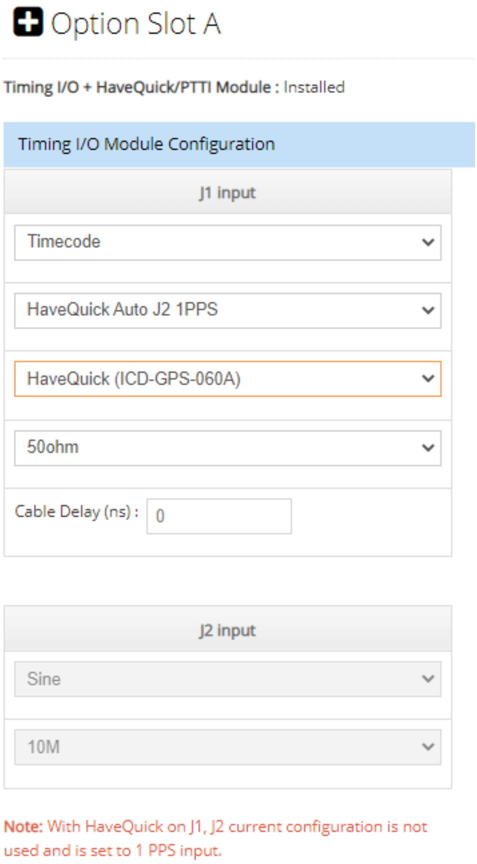
   Note: When J1 is configured for a HaveQuick Auto J2 input, J2 is automatically configured to expect an associated PPS input. There is no need to enable J2 on this form.



Time Reference Priority

Enable	Reference	Priority
□	GNSS	1
☑	Slot A J1 Timecode	2
☑	Slot B J1 Timecode	3
□	PTP	4

2. The specific input configuration is completed on the module configuration form. As the HaveQuick/PTTI module is in slot A on this S6xx, the navigation is `OPTION SLOT A > Timing I/O + HQ/PTTI`. The following figure shows the relevant portions of the form.
   - The top selection for J1 is shown as Timecode. If something else is in this list box, change it to Timecode.
   - The second J1 box shows HaveQuick. If something else is in this list box, change it to HaveQuick.
   - Given that the first and second list boxes are set as shown, the third box can be set to any of the supported HaveQuick codes.
   - The J2 input is grayed out. No selections are possible when HaveQuick Auto J2 is selected for J1 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.
   - As 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, then this causes the synchronization of the J2 PPS to be moved earlier by 100 ns compared to the PPS rising edge arriving at J2.
     Select **Apply** to complete the configuration.



Option Slot A

Timing I/O + HaveQuick/PTTI Module : Installed

Timing I/O Module Configuration

J1 input

Timecode

HaveQuick Auto J2 1PPS

HaveQuick (ICD-GPS-060A)

50ohm

Cable Delay (ns) : 0

J2 input

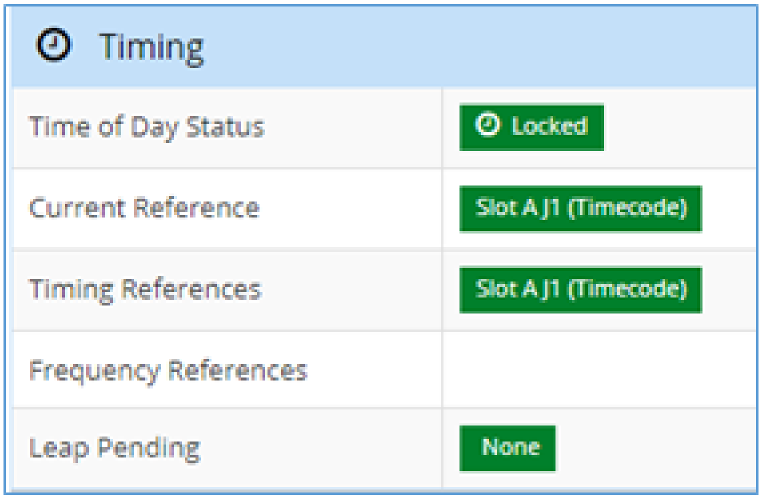
Sine

10M

Note: With HaveQuick on J1, J2 current configuration is not used and is set to 1 PPS input.

If appropriate inputs are being provided to J1 and J2, then S6xx locks to this source of time. The status can be seen on the `References > Status form` and most comprehensively on the `Dashboard > Timing form`, as shown in the following figure.

Note: 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. If there is no J2 PPS, an LOS alarm is set.



Timing

Time of Day Status	Locked
Current Reference	Slot A J1 (Timecode)
Timing References	Slot A J1 (Timecode)
Frequency References	
Leap Pending	None

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 SyncServer S650.

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

Table 6-10. Configure PTP Client Inputs

Method	Steps
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 to open the Configurable Parameters window. 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
Front Panel	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 server and the PTP client in the SyncServer. If asymmetry correction is enabled without GPS, then the PTP client is used only to adjust the system frequency and does not adjust the system time. Calibration takes at least one to two hours.

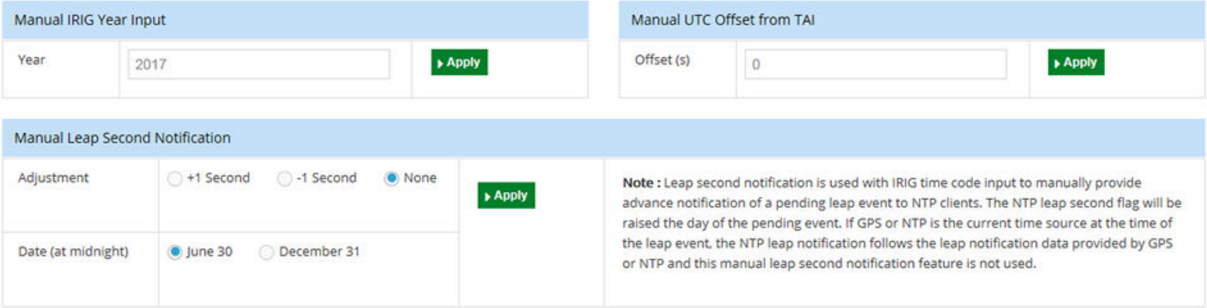
6.5 Provisioning Inputs with Manual Entry Controls

The common purpose for the manual entry controls at the bottom of the Timing > Input Control window, as shown in the following figure, is to provide a method to enable the S6xx to become aware of time-related status information in scenarios where there 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 must report degraded status. Each of these controls exists to “fill in a gap” that otherwise will exist and lead to degraded time output capability. Table 6-12 describes the manual entry controls.

The following table lists 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. Input Control Window —Lower Portion



Manual IRIG Year Input

Year: 2017

Manual UTC Offset from TAI

Offset (s): 0

Manual Leap Second Notification

Adjustment: ○ +1 Second ○ -1 Second ● None

Date (at midnight): ● June 30 ○ December 31

Note : Leap second notification is used with IRIG time code input to manually provide advance notification of a pending leap event to NTP clients. The NTP leap second flag will be raised the day of the pending event. If GPS or NTP is the current time source at the time of the leap event, the NTP leap notification follows the leap notification data provided by GPS or NTP and this manual leap second notification feature is not used.

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: • cannot set TAI timescale • cannot set UTCoffsetValid flag • cannot indicate pending leap NTP: • cannot indicate pending leap IRIG1344/C37.118: • cannot 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: • cannot set TAI timescale • cannot set UTCoffsetValid flag • cannot indicate pending leap NTP: • can't provide UTC time • cannot indicate pending leap IRIG1344/C37.118: • cannot provide UTC time • cannot 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, then 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: • cannot set TAI timescale • cannot 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. Here, manual use of pending leap can help.
NTP	• No UTC offset from TAI	PTP: • cannot set TAI timescale • cannot set UTCoffsetValid flag	Manually set: • utc offset	
GNSS without GPS in the constellation configuration	• No UTC offset from TAI • No Pending leap	PTP: • cannot set TAI timescale • cannot set UTCoffsetValid flag • can't indicated pending leap NTP: • cannot indicate pending leap • IRIG1344/C37.118: • cannot indicate pending leap	Manually set: • utc offset	

For example, if the only available time input is an IRIG1344 and S6xx is supporting a PTP (IEEE-1588) Server function. As the IRIG input provides UTC timescale and PTP uses TAI timescale, S6xx must convert from UTC time to get to TAI time. However, this conversion requires awareness of the current accumulated leap seconds, information the IRIG input does not supply. Without an auxiliary method for learning this value, the PTP output encodes the Announce message with the ptpTimescale flag set to false, which means that PTP clients using this S6xx PTP server 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 encode TAI time, and the ptpTimescale flag is set to true.

The following table lists functions that are 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”) an indication that a leap is pending (due to manual entry) appears on the Dashboard's Timing form. • Leap pending notifications are 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 is no longer showing as pending.

6.5.1 General Behavior Associated with Manual Entry

The following behaviors apply to all the manual entries:

- If there is currently a qualified time reference that can provide that particular information, then a manual entry supplying that information is not 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.
- Similar 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 (that is, 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 increments 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.

- When 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 is turned off. If on a subsequent power-up, a time reference is provided that can supply leap pending status, then the condition is entirely based upon that status.
- If using a manually entered UTC offset, this value is updated in the appropriate direction if a leap event occurs (that is, 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 following example shows 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 are shown in Figure 6-6 (access this form through `References > Status`).
Note: 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 supplied (this is why it is green and the slot B J1 input is red). Figure 6-7 shows the status from the `Dashboard > Timing form`. As 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 these values. For this example, they are intentionally provided with wrong values to illustrate the behavior when inputs are added later that provide the correct information. In actual usage (where only the input shown is available), the correct information must be provided.

With only the IRIG no-year input qualified (Figure 6-7), the values shown in Figure 6-8 are 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) server capability. If a PTP server 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 > NTPr/PTP Status form`. For this example, LAN2 had been configured for PTP server 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: 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 shows that all qualified inputs are used for extraction of the items shown in 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: The year might not be immediately adjusted upon qualification of the IRIG that supplies the year, but it will happen within a few minutes. The message log provides an entry when the timeline shift occurs.

Following is an example:

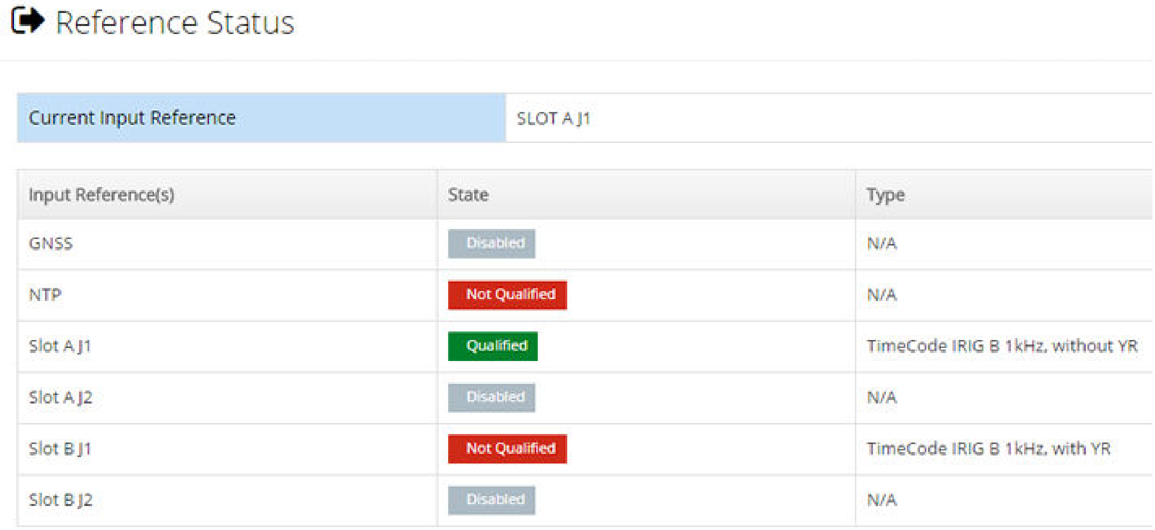
```
Jan 30 18:46:28 SyncServer alarmd: id 152, index 000, severity Notify ALARM SET:
Timeline has been changed
```

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. As GPS provides all the information, if we provide GPS as an input, then these remaining items will be driven by the status provided via GPS. As the manual values are intentionally set incorrectly for this example, they must 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

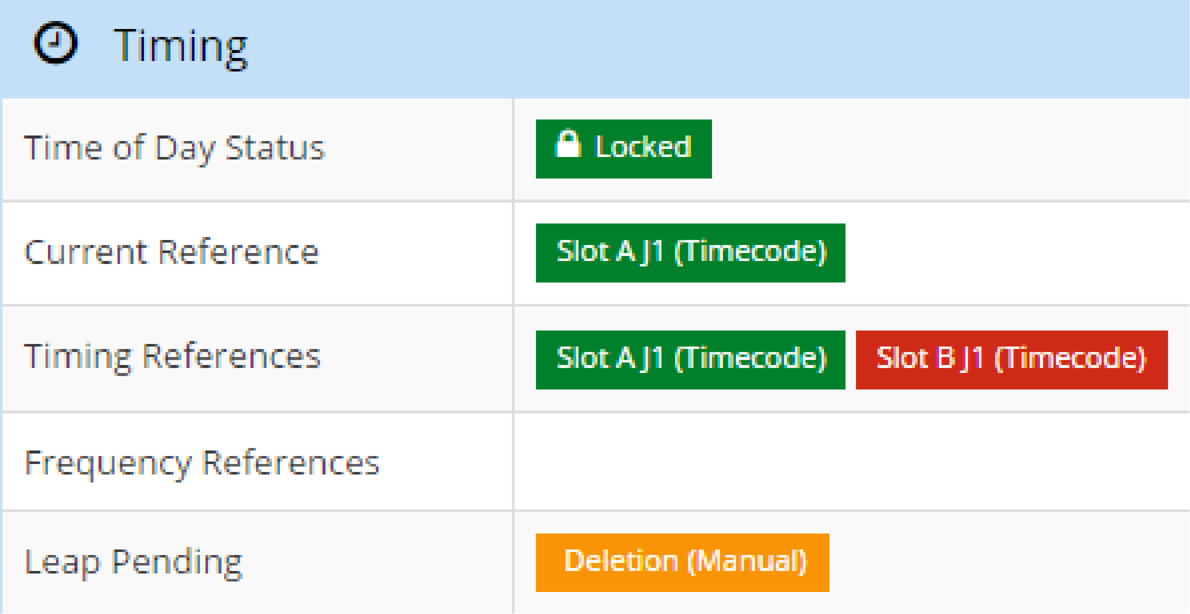


Reference Status

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

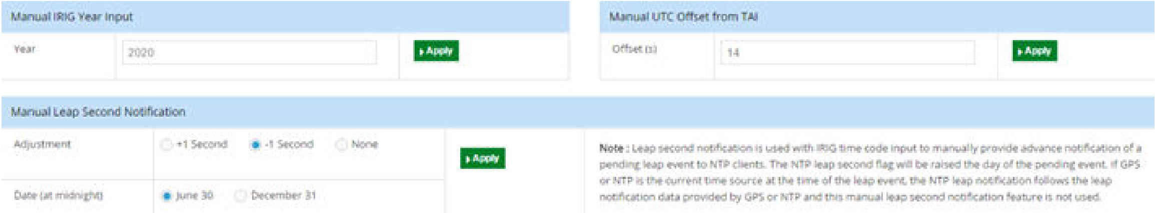
Figure 6-7. The Qualified (and Selected) Input does not Provide Year (or Leap) Information



Timing

Time of Day Status	Locked
Current Reference	Slot A J1 (Timecode)
Timing References	Slot A J1 (Timecode) Slot B J1 (Timecode)
Frequency References	
Leap Pending	Deletion (Manual)

Figure 6-8. Example of User-Entry of all Manual Inputs



Manual IRIG Year Input

Year: 2020

Manual UTC Offset from TAI

Offset (s): 14

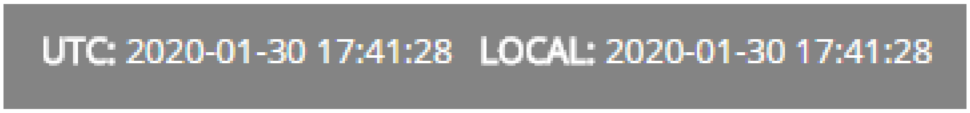
Manual Leap Second Notification

Adjustment: ○ +1 Second ● -1 Second ○ None

Date (at midnight): ● June 30 ○ December 31

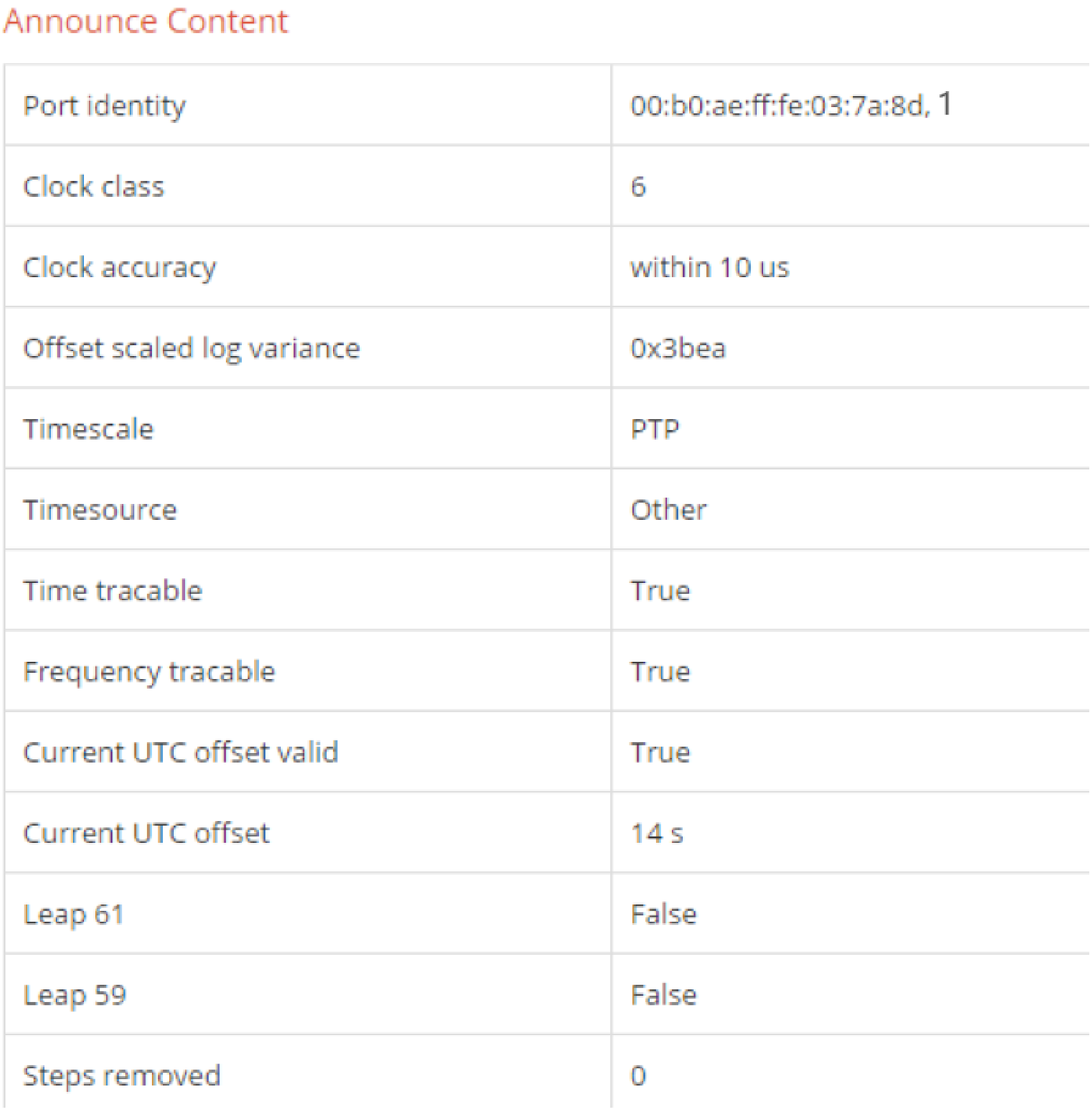
Note : Leap second notification is used with IRIG time code input to manually provide advance notification of a pending leap event to NTP clients. The NTP leap second flag will be raised the day of the pending event. If GPS or NTP is the current time source at the time of the leap event, the NTP leap notification follows the leap notification data provided by GPS or NTP and this manual leap second notification feature is not used.

Figure 6-9. Use of Manually Entered Year



UTC: 2020-01-30 17:41:28 LOCAL: 2020-01-30 17:41:28

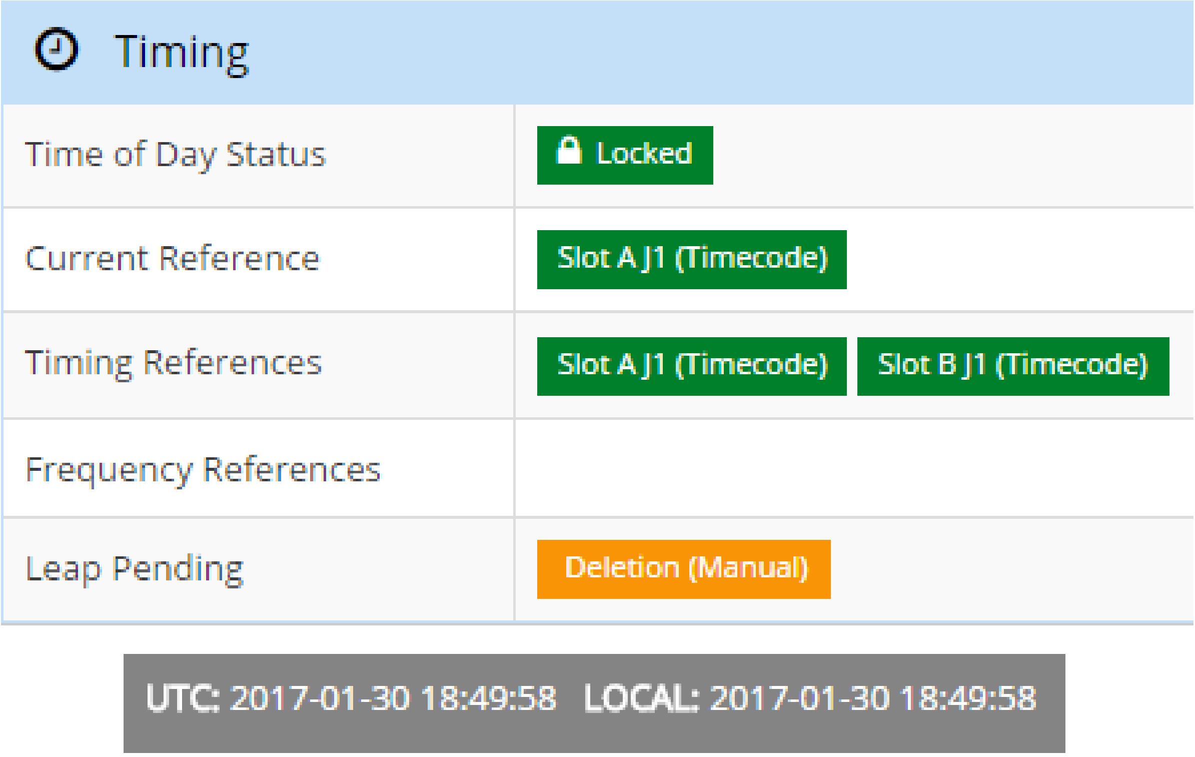
Figure 6-10. Portion of PTP Status



Announce Content

Port identity	00:b0:ae:ff:fe:03:7a:8d, 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

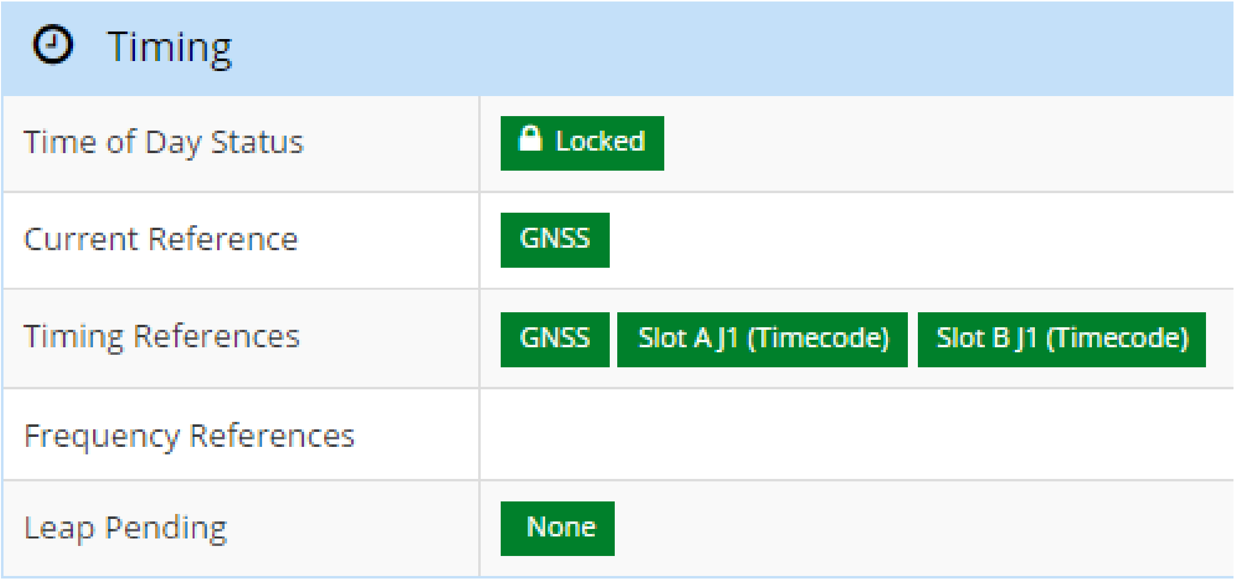


Timing

Time of Day Status	Locked
Current Reference	Slot A J1 (Timecode)
Timing References	Slot A J1 (Timecode) Slot B J1 (Timecode)
Frequency References	
Leap Pending	Deletion (Manual)

UTC: 2017-01-30 18:49:58 LOCAL: 2017-01-30 18:49:58

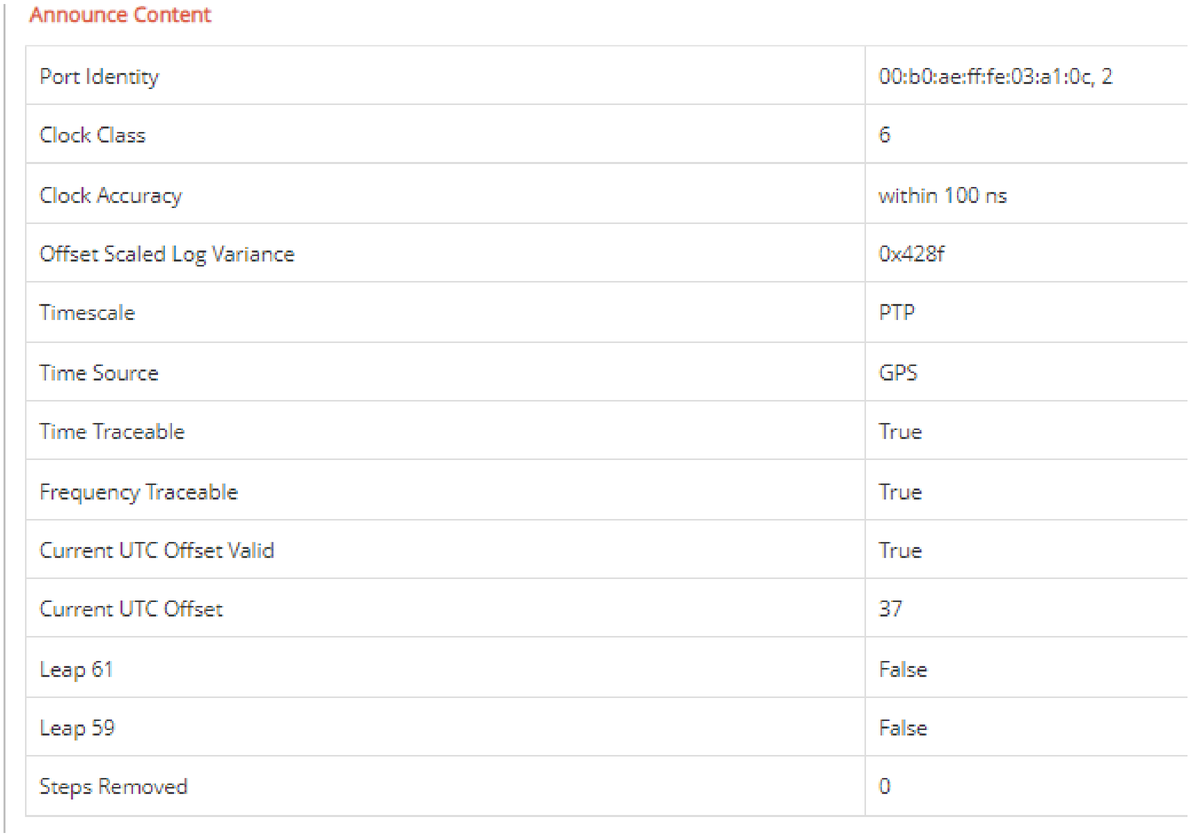
Figure 6-12. Adding GPS Clears Pending Leap



Timing

Time of Day Status	Locked
Current Reference	GNSS
Timing References	GNSS Slot A J1 (Timecode) Slot B J1 (Timecode)
Frequency References	
Leap Pending	None

Figure 6-13. Adding GPS Provides Correct UTC Offset Value



Announce Content

Port Identity	00:b0:ae:ff:fe:03:a1:0c, 2
Clock Class	6
Clock Accuracy	within 100 ns
Offset Scaled Log Variance	0x428f
Timescale	PTP
Time Source	GPS
Time Traceable	True
Frequency Traceable	True
Current UTC Offset Valid	True
Current UTC Offset	37
Leap 61	False
Leap 59	False
Steps Removed	0

6.5.2 Reporting of Leap Second Pending

The ability to provide manual entry of pending leap seconds (see Figure 6-5) 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 is do with the varying rules (based on signal type) about when a pending leap must be declared in relation to the planned moment of the actual leap event.

Figure 6-14 shows the following concepts:

- A timeline that terminates with the application of a leapsecond.
- All time inputs/outputs supported in release 2.0 that can provide indication of a pending leap second. Specifically, the following:
  - 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 (through GPS) to downstream devices from the S6xx that there is a pending leap second. For this reason, there is no limitation on how early a leapsecond might be encoded in GPS or on how early S6xx indicates it. This gets at a basic point that when S6xx is aware of a pending leapsecond (from any source, including manual entry), this condition will be shown on the Dashboard Timing form. For example, in Figure 6-14, a pending leap is indicated because it is entered manually (and accepted).

    Note: Release 2.0 supports multiple satellite constellation configuration.

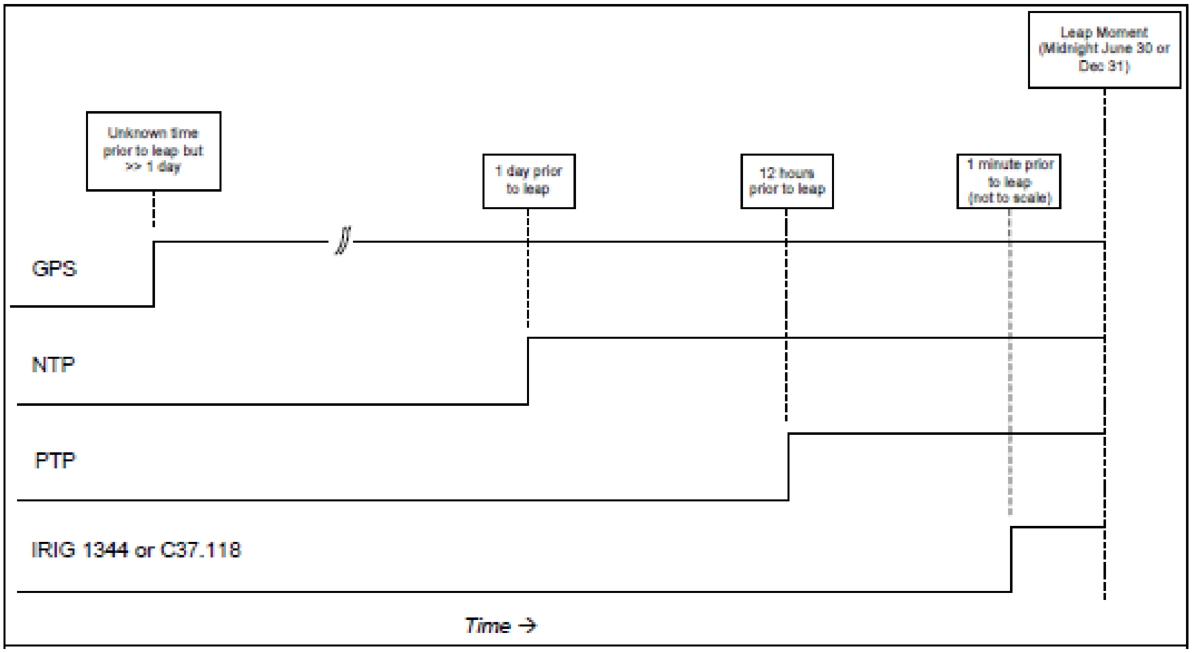
    Any GNSS input whose configuration does not include GPS is not capable of learning about pending leapseconds or the current UTC offset. Therefore, the preceding discussion is applicable only to combinations that included the GPS constellation. When GPS is not included, the manual methods for indicating 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. Therefore, 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 must 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.
- S6xx always does its best on its outputs to fulfill the complete timeframe for that output. However, the following example shows what happens when the input providing the pending leap has a shorter pre-notification period than an output that is configured: If the incoming signal that provides the leap notification is an IRIG 1344 and S6xx is configured to function as an NTP Primary Server, the pre-notification of the pending leap on NTP is (at best) one minute because the IRIG 1344 does not inform 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


Leap Moment (Midnight June 30 or Dec 31)
Unknown time prior to leap but >> 1 day
1 day prior to leap
12 hours prior to leap
1 minute prior to leap (not to scale)
GPS
NTP
PTP
IRIG 1344 or C37.118
Time →

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 states the following:

- If there is currently a qualified time reference that can provide that particular information, then a manual entry supplying that information is not used.

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

- If there is currently a qualified time reference that can provide 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 is not 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 is 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 overrules (if needed) the manual setting.

Examples

- If GPS is a qualified reference, manual leap pending input is never accepted as GPS provides leap pending status (typically) many months prior to the leap moment. No formal definition for the time frame is available but for there is sufficient notice. Therefore, there is no reason to accept a manual entry.
- If GPS is not a qualified reference, then manual control of leap is allowed at any time except when the remaining time until leap is within the timeframe of the qualified time input shown in Figure 6-14 that has the longest timeframe. In this region, the inputs 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 S6xx is operating as a PTP GrandMaster. As 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. As S6xx knows that the IRIG input does not provide any information until the last minute, the manual input is accepted. There is no problem providing the manual notification early because S6xx knows to hold off based on the appropriate timeframe for the signal type. In this case, with the PTP output, the notification appears in the PTP Announce messages a 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

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 lists the method to add a new NTP association.
Table 6-14 lists the method to modify an existing NTP association.
Table 4-7 lists 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 must consider adding NTP servers available on the local network to the list of current NTP associations. If the system is using NTP as the reference and the NTP server is performing a leap smear, then all of the non-NTP outputs of the system are degraded, especially outputs on the optional I/O modules.

6.6.1 NTP Prefer Selection

By default, SyncServer S6x0 Series has the NTP Prefer selected for the local hardware reference clock. In most of the operating scenarios, the local hardware reference clock (which often tracks GNSS) is the only reference being used. With the Prefer being selected, and no statistically better reference available, the time server achieves 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 goes through a standard validation procedure for a reference clock. This procedure takes several minutes and must 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 Configuration 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. The system generates 10 keys each with MD5, SHA, and SHA512 algorithms.
- Upload a file containing keys from a local PC drive to SyncServer. Maximum key file size is 2400 characters.
- Download 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) Autokeys for NTP associations where SyncServer is an NTP server.

Note: Hostname of Autokey server and Autokey client must be different. Use the #unique_234 to set the 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 **Download** 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) Autokeys for NTP associations where SyncServer is an NTP client.

Note: Hostname of Autokey server and Autokey client must be different. Use the 5.3.1. Admin—General Configuration Window to set the 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 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 the **Auto** option from the 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 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 the **Auto** option 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 the newly added NTPd is 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

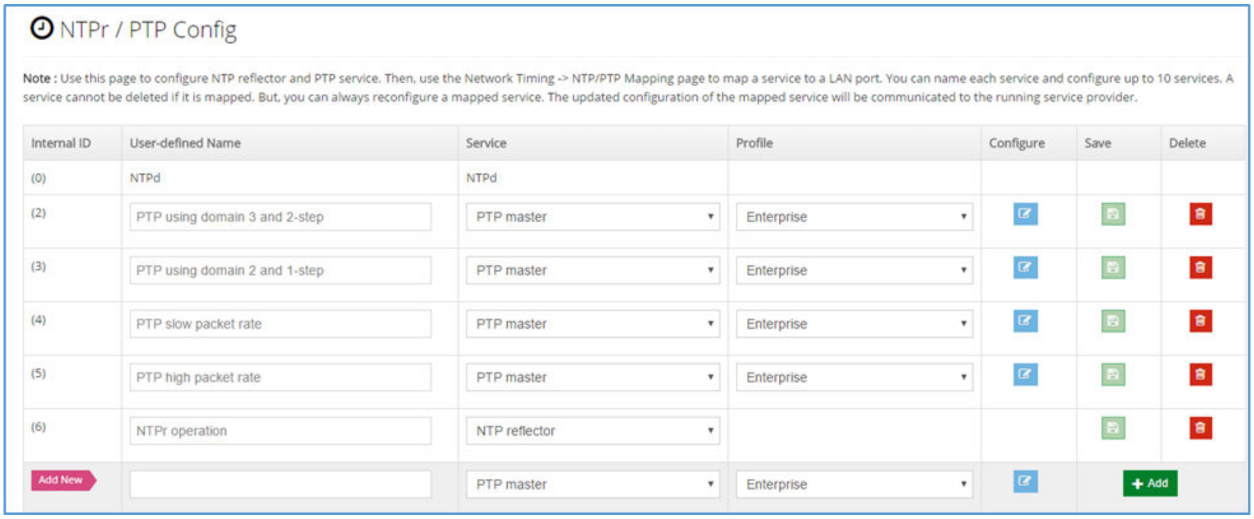
The `Network Timing > NTPr/PTP Config` form supports generalized configuration of network timing services. The concept is that the ability to create and retain definitions for specific services independently of the connection method, provides a useful way to aggregate within S6x0 all the network timing services that are of interest for that particular unit. As added services are provided in future releases, this form evolves 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 must run. This is accomplished on the `Network Timing > NTP/PTP Mapping` form.

6.8.1.1 Example—Creating a Network Timing Service

The following figure shows the timing services configuration form. Five services have been previously 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



NTPr / PTP Config

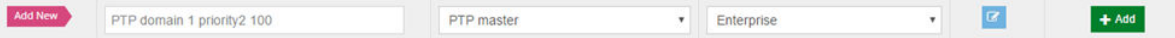
Note : Use this page to configure NTP reflector and PTP service. Then, use the Network Timing -> NTP/PTP Mapping page to map a service to a LAN port. You can name each service and configure up to 10 services. A service cannot be deleted if it is mapped. But, you can always reconfigure a mapped service. The updated configuration of the mapped service will be communicated to the running service provider.

Internal ID	User-defined Name	Service	Profile	Configure	Save	Delete
(0)	NTPd	NTPd				
(2)	PTP using domain 3 and 2-step	PTP master	Enterprise			
(3)	PTP using domain 2 and 1-step	PTP master	Enterprise			
(4)	PTP slow packet rate	PTP master	Enterprise			
(5)	PTP high packet rate	PTP master	Enterprise			
(6)	NTPr operation	NTP reflector				
Add New		PTP master	Enterprise		+ Add	

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

For example, to use 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 Best Master Clock Algorithm (BMCA) executing at the downstream PTP clients will choose this S6x0 because of its better priority. Following are the steps:

1. 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 are accomplished later in this example.

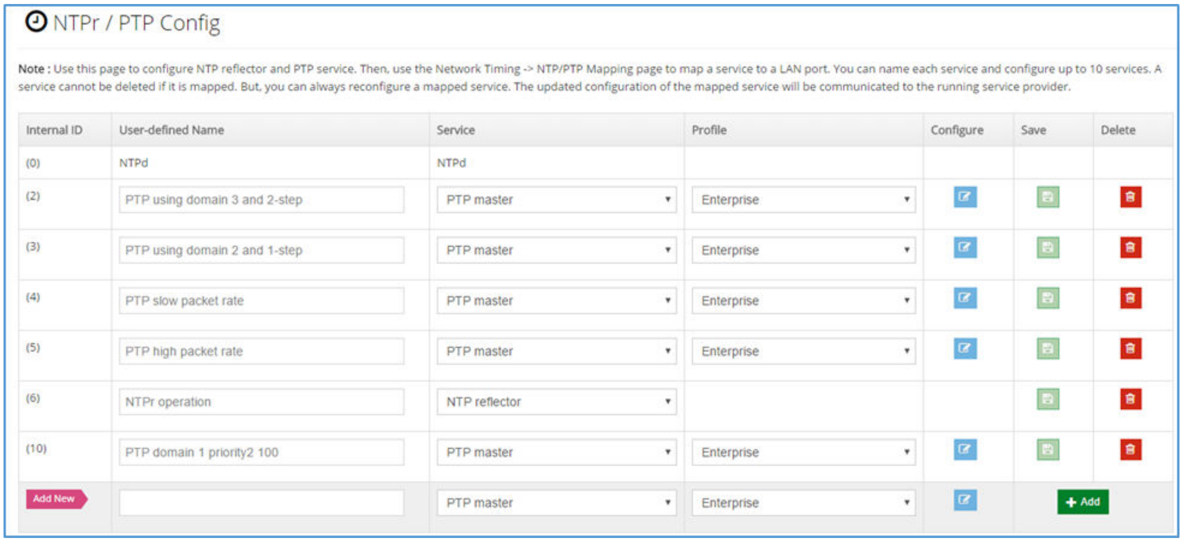
Add New	PTP domain 1 priority2 100	PTP master	Enterprise		+ Add

2. – At this point there are following two 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, as shown in the following figure:

Figure 6-16. Example—New Timing Service Configuration



NTPr / PTP Config

Note : Use this page to configure NTP reflector and PTP service. Then, use the Network Timing -> NTP/PTP Mapping page to map a service to a LAN port. You can name each service and configure up to 10 services. A service cannot be deleted if it is mapped. But, you can always reconfigure a mapped service. The updated configuration of the mapped service will be communicated to the running service provider.

Internal ID	User-defined Name	Service	Profile	Configure	Save	Delete
(0)	NTPd	NTPd				
(2)	PTP using domain 3 and 2-step	PTP master ▾	Enterprise ▾	✎	🖫	🗑
(3)	PTP using domain 2 and 1-step	PTP master ▾	Enterprise ▾	✎	🖫	🗑
(4)	PTP slow packet rate	PTP master ▾	Enterprise ▾	✎	🖫	🗑
(5)	PTP high packet rate	PTP master ▾	Enterprise ▾	✎	🖫	🗑
(6)	NTPr operation	NTP reflector ▾			🖫	🗑
(10)	PTP domain 1 priority2 100	PTP master ▾	Enterprise ▾	✎	🖫	🗑
Add New		PTP master ▾	Enterprise ▾	✎	+ Add	

The new timing service is shown on the bottom row.

Note: It is auto-assigned ID = 10 and the actual value is not important. S6x0 assures that it is unique. The Save control is grayed out, indicating that there is nothing to save. However, as we have not yet completed all the desired configurations, there is still work to do.

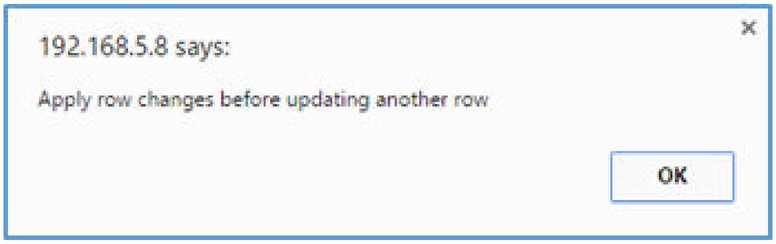
As the default values for Service and Profile columns happen to be what we want for this service, there is no need to change them. In general, if the values are required to be changed from the default, they must be done in the following left-to-right order as the columns to the right adapt based on selections to the left:

a. Service

b. Profile

c. Configure

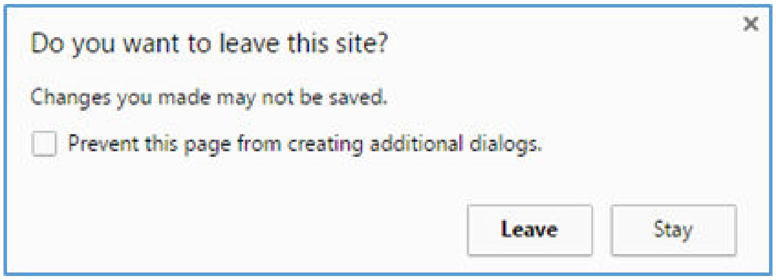
3. Select the Configure control (Figure 6-17) which always begins with default values the first time a new service is created. For this example, we need to change the Domain and the Priority2 values. Set Domain = 1 and Priority2 = 100, then OK. Figure 6-17 shows the configuration with these changes, just before selecting OK. This action returns to Figure 6-16. Now, the detailed configuration matches the desired setup, as described in the User-Defined Name.
4. 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:
5. Figure 6-18 shows the **Save** button is active and the entire row associated with the new service is highlighted. These are clues that the full configuration has not been completed 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** button is inactive because there are no pending changes (this was before the changes were made on the configuration form).
6. If pending (unsaved) changes have been made to any row and an action is taken to make changes on a different row, a box appears indicating that there are unsaved changes:



192.168.5.8 says:

Apply row changes before updating another row

Similarly, if there are pending changes and a new form is selected, this form ensures that the action is intended.

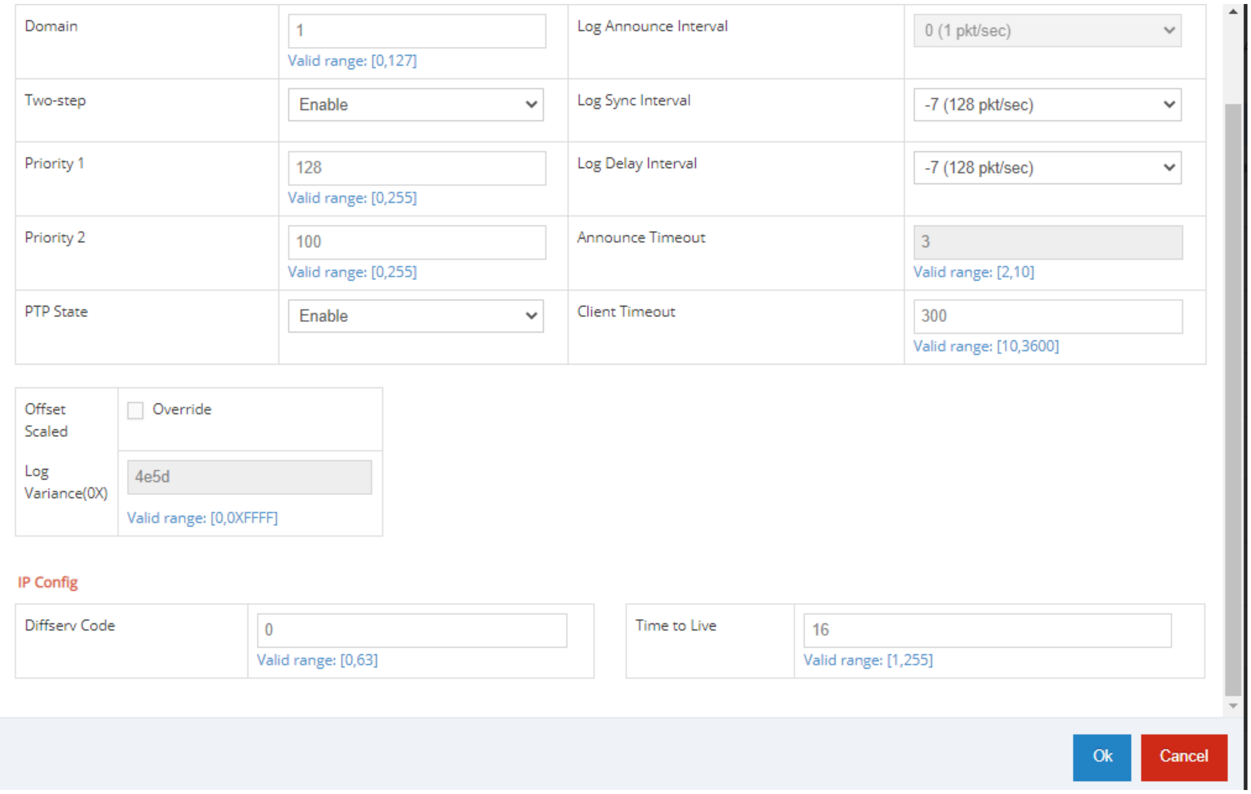


Do you want to leave this site?

Changes you made may not be saved.

□ Prevent this page from creating additional dialogs.

Figure 6-17. Modified Configuration for “PTP domain 1 priority2 100” Before OK Selection



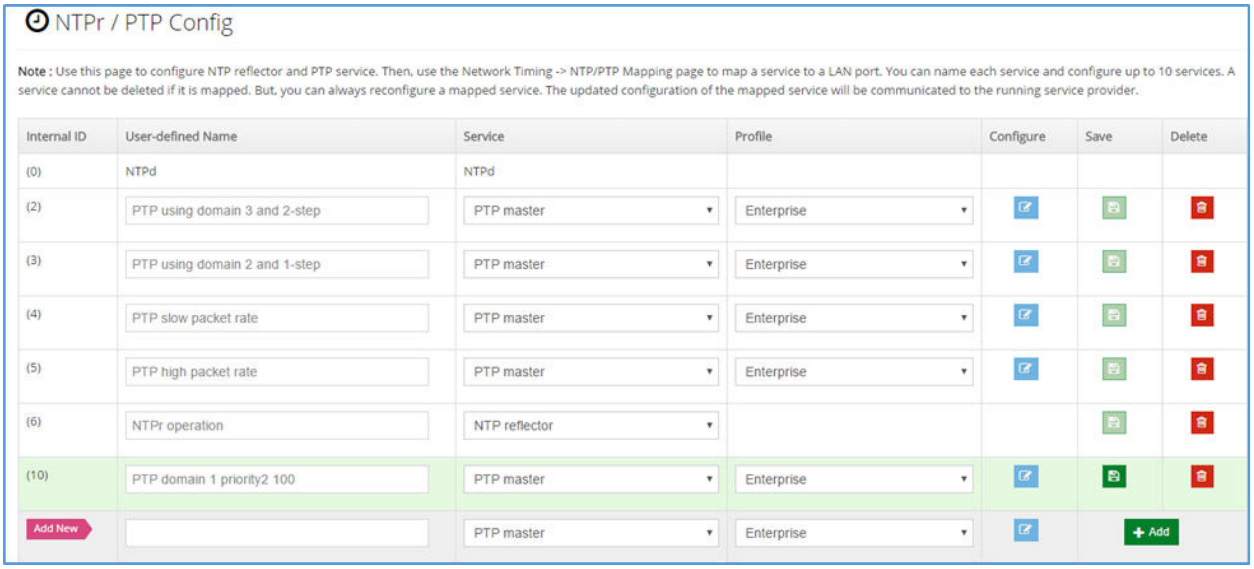
Domain	1 Valid range: [0,127]	Log Announce Interval	0 (1 pkt/sec)
Two-step	Enable	Log Sync Interval	-7 (128 pkt/sec)
Priority 1	128 Valid range: [0,255]	Log Delay Interval	-7 (128 pkt/sec)
Priority 2	100 Valid range: [0,255]	Announce Timeout	3 Valid range: [2,10]
PTP State	Enable	Client Timeout	300 Valid range: [10,3600]

Offset Scaled	□ Override
Log Variance(0X)	4e5d Valid range: [0,0XFFFF]

IP Config

Diffserv Code	0 Valid range: [0,63]	Time to Live	16 Valid range: [1,255]

Figure 6-18. New Timing Service Before Final Save



NTPr / PTP Config

Note : Use this page to configure NTP reflector and PTP service. Then, use the Network Timing -> NTP/PTP Mapping page to map a service to a LAN port. You can name each service and configure up to 10 services. A service cannot be deleted if it is mapped. But, you can always reconfigure a mapped service. The updated configuration of the mapped service will be communicated to the running service provider.

Internal ID	User-defined Name	Service	Profile	Configure	Save	Delete
(0)	NTPd	NTPd				
(2)	PTP using domain 3 and 2-step	PTP master	Enterprise			
(3)	PTP using domain 2 and 1-step	PTP master	Enterprise			
(4)	PTP slow packet rate	PTP master	Enterprise			
(5)	PTP high packet rate	PTP master	Enterprise			
(6)	NTPr operation	NTP reflector				
(10)	PTP domain 1 priority2 100	PTP master	Enterprise			
Add New		PTP master	Enterprise		+ Add	

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.

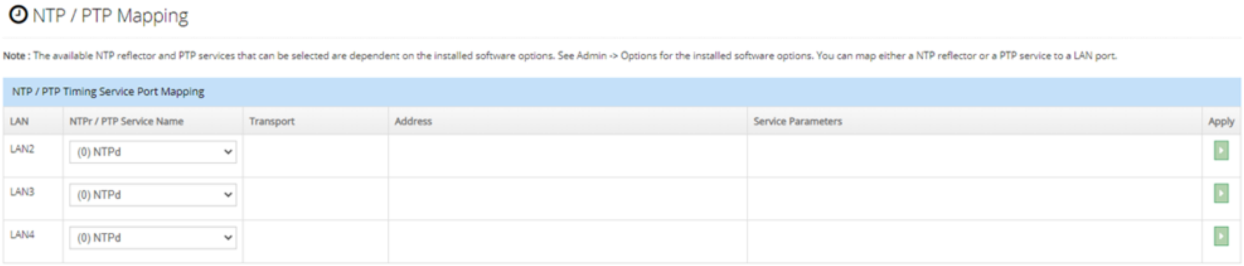
Note: There is a predefined row with internal ID = (0) at the top of the row portion of the following figure, named NTPd. The NTPd service has always been available on S6x0 and is supported on all physical network ports. NTPd configuration is accomplished on the Network Timing'NTPd Config form. Rather than create a new method for its configuration, the existing method remains. However, as is seen in the following section, 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 Network Timing Service to LAN Port

Creation of network timing services, as shown in 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. The following figure shows this form as it appears at 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 following table lists the service choices and allowed mapping rules. The behavior listed in this table is enforced by the form controls.

Figure 6-19. Factory Preset Mapping Form



NTP / PTP Mapping

Note : The available NTP reflector and PTP services that can be selected are dependent on the installed software options. See Admin -> Options for the installed software options. You can map either a NTP reflector or a PTP service to a LAN port.

NTP / PTP Timing Service Port Mapping

LAN	NTPr / PTP Service Name	Transport	Address	Service Parameters	Apply
LAN2	(0) NTPd				
LAN3	(0) NTPd				
LAN4	(0) NTPd				

Table 6-18. Network Timing Service Mapping

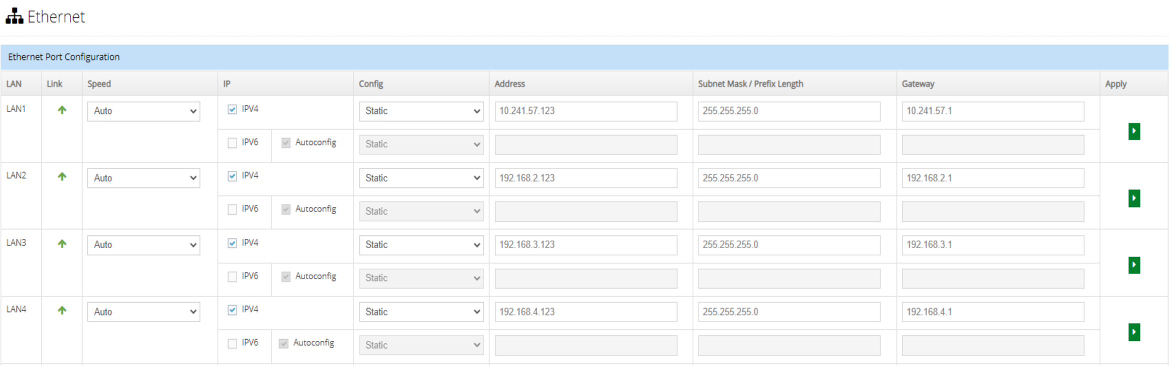
Network Timing Service	Individual Mapping Rules	Combined Mapping Rules
NTPd	Supported on LAN1, LAN2, LAN3, LAN4, LAN5, LAN6	Always mapped to LAN1. Can be mapped to any combination of other ports if no other timing service is mapped to that port.
PTP Server	Can be mapped to any of these physical ports: LAN2, LAN3, LAN4, LAN5, LAN6	Can be mapped to any combination of ports if 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 any combination of ports if no other timing service is mapped to that port.
PTP Client	Can be mapped to any of these physical ports: LAN2, LAN3, LAN4, LAN5, LAN6	Can be mapped to any port if no other timing service is mapped to that port, and none of the other PTP clients are mapped.

6.8.2.1 Example—Mapping Network Timing Service

Perform the following steps if, for example, the goal is to provide the PTP Server service that was created (Figure 6-18) on LAN4:

1. Configure (if not already done) LAN4 with a network configuration. This is accomplished on the `Network > Ethernet form`. The following figure shows an example where LAN4 has been configured to IPv4 address 192.168.4.123.

   Figure 6-20. Example Configuration on Network > Ethernet Form

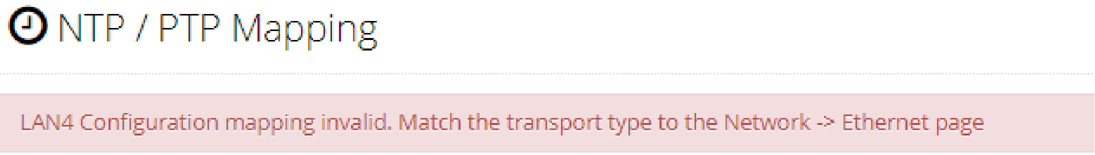
   

   Ethernet

   Ethernet Port Configuration

LAN	Link	Speed	IP		Config	Address	Subnet Mask / Prefix Length	Gateway	Apply
LAN1	↑	Auto	☑ IPV4		Static	10.241.57.123	255.255.255.0	10.241.57.1	▶
			☐ IPV6	☑ Autoconfig	Static				
LAN2	↑	Auto	☑ IPV4		Static	192.168.2.123	255.255.255.0	192.168.2.1	▶
			☐ IPV6	☑ Autoconfig	Static				
LAN3	↑	Auto	☑ IPV4		Static	192.168.3.123	255.255.255.0	192.168.3.1	▶
			☐ IPV6	☑ Autoconfig	Static				
LAN4	↑	Auto	☑ IPV4		Static	192.168.4.123	255.255.255.0	192.168.4.1	▶
			☐ IPV6	☑ Autoconfig	Static				

   Attempting to complete a service mapping to a LAN that has not been configured results in the following message:

   NTP / PTP Mapping

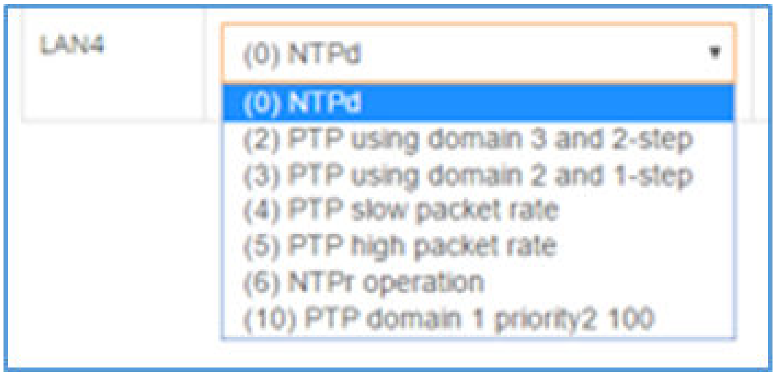
   LAN4 Configuration mapping invalid. Match the transport type to the Network -> Ethernet page

2. Select the desired service from the list box in the Service Name column. As this example maps the service to LAN4, the list box from that row is used. Figure 6-21 shows the selection set. This list always shows the first two columns of the configurations done in Figure 6-18. The list does not filter out selections that may not actually be allowed per the combined mapping rules column of Table 6-18; the list always shows all the services that can possibly be assigned to that port.
3. Select the service associated with internal ID (10) (Figure 6-22).
   Note: This row is highlighted as indication that this assignment is not actually complete. The **Apply** button on the right of this row is now active to indicate that something needs to be saved.

4. Selection of apply attempts to complete the mapping. This action causes any specific mapping rules (see Table 6-18) to be enforced, which could lead to non-acceptance of the candidate entry. 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 preceding example. This form also shows LAN1 which is always mapped to NTPd in 2.0 release.

Figure 6-21. Timing Services Choices List Box

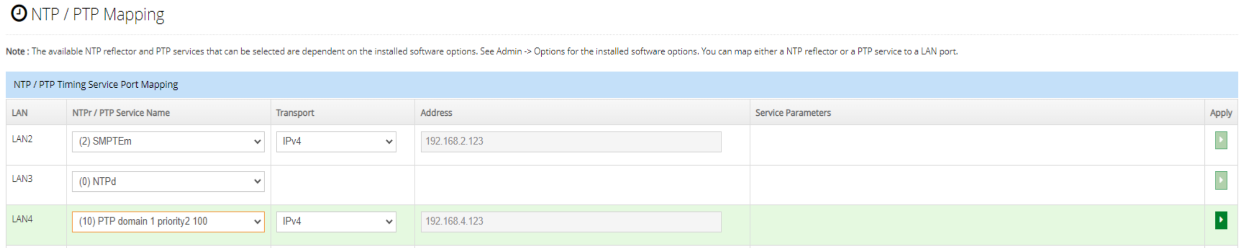


LAN4

(0) NTPd ▾

- (0) NTPd
- (2) PTP using domain 3 and 2-step
- (3) PTP using domain 2 and 1-step
- (4) PTP slow packet rate
- (5) PTP high packet rate
- (6) NTPr operation
- (10) PTP domain 1 priority2 100

Figure 6-22. PTP Server Timing Service Being Mapped to LAN4



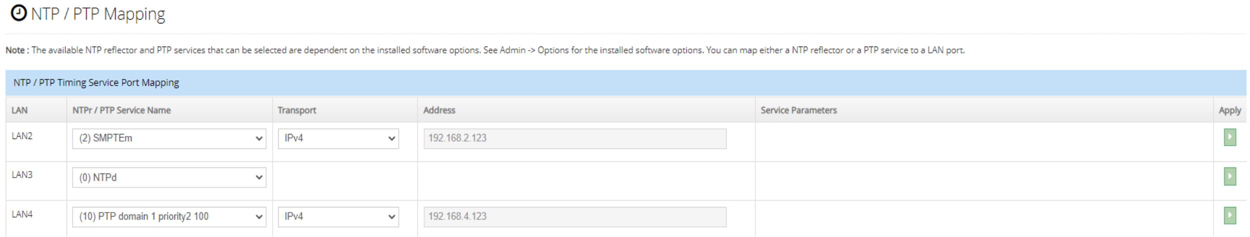
NTP / PTP Mapping

Note : The available NTP reflector and PTP services that can be selected are dependent on the installed software options. See Admin -> Options for the installed software options. You can map either a NTP reflector or a PTP service to a LAN port.

NTP / PTP Timing Service Port Mapping

LAN	NTPr / PTP Service Name	Transport	Address	Service Parameters	Apply
LAN2	(2) SMPTEm	IPv4	192.168.2.123		▶
LAN3	(0) NTPd				▶
LAN4	(10) PTP domain 1 priority2 100	IPv4	192.168.4.123		▶

Figure 6-23. Successful Completion of Mapping New Timing Service to LAN4



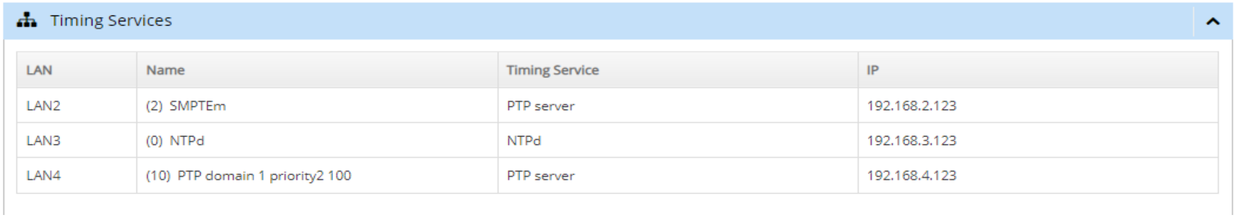
NTP / PTP Mapping

Note : The available NTP reflector and PTP services that can be selected are dependent on the installed software options. See Admin -> Options for the installed software options. You can map either a NTP reflector or a PTP service to a LAN port.

NTP / PTP Timing Service Port Mapping

LAN	NTPr / PTP Service Name	Transport	Address	Service Parameters	Apply
LAN2	(2) SMPTEm	IPv4	192.168.2.123		▶
LAN3	(0) NTPd				▶
LAN4	(10) PTP domain 1 priority2 100	IPv4	192.168.4.123		▶

Figure 6-24. Dashboard Timing Services Shows Current Mapping



Timing Services

LAN	Name	Timing Service	IP
LAN2	(2) SMPTEm	PTP server	192.168.2.123
LAN3	(0) NTPd	NTPd	192.168.3.123
LAN4	(10) PTP domain 1 priority2 100	PTP server	192.168.4.123

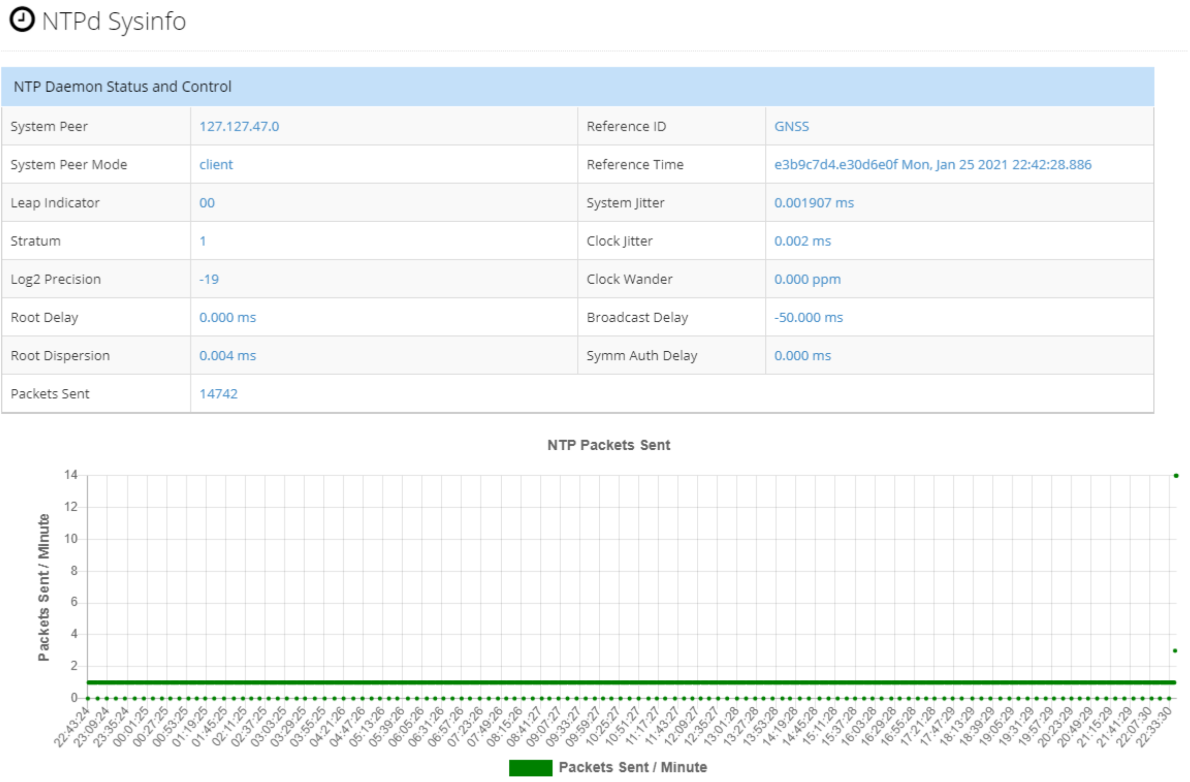
6.8.3 Observing Status of Network Timing Services

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 (Figure 6-15) is only actually in use when it is mapped to a physical network port, accomplished in Figure 6-19. Therefore, the set of services that have status are those that have been mapped to a LAN port.

Following are the two areas on the Web interface where timing service status can be observed for NTPd:

- `Network Timing > Sysinfo` provides complete status, showing standard NTP parameter values. The following figure 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

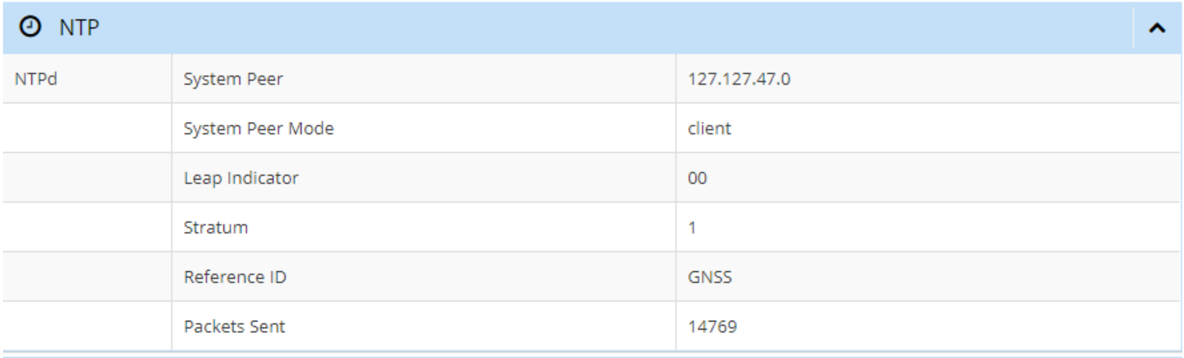


NTPd Sysinfo

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		

- The following figure shows a summarized status available on `Dashboard > NTP`.

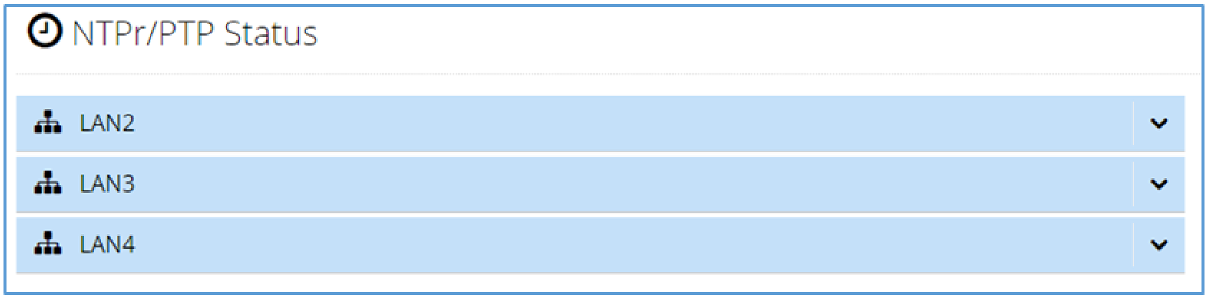
Figure 6-26. Summarized NTPd Status Example



NTP

NTPd	System Peer	127.127.47.0
	System Peer Mode	client
	Leap Indicator	00
	Stratum	1
	Reference ID	GNSS
	Packets Sent	14769

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 shown in Figure 6-23). In release 2.0 due to the rules described in Table 6-18, only one of the LANs contain the status. This form prepares for expanded capability.



NTPr/PTP Status

LAN2

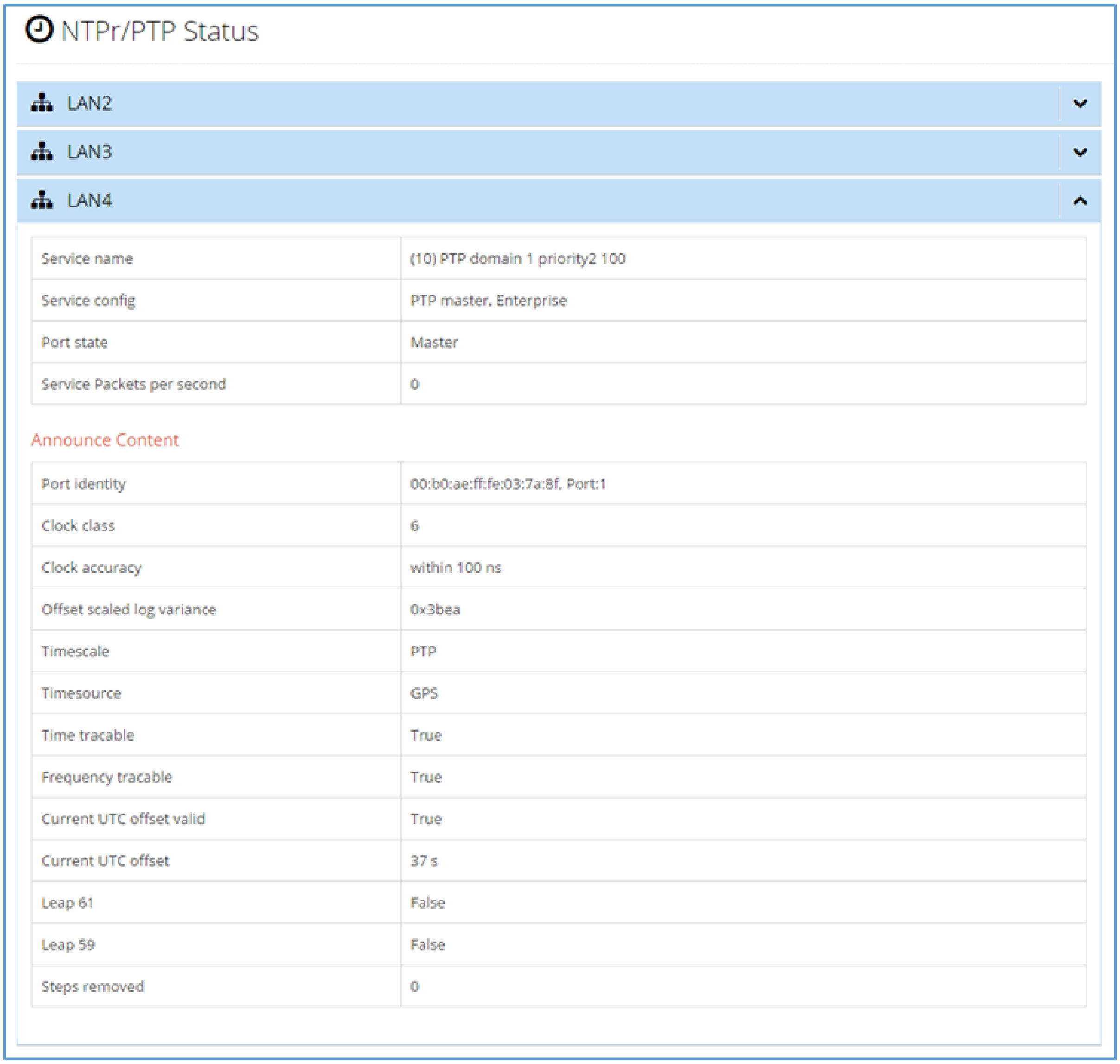
LAN3

LAN4

Using the setup from Figure 6-23 where we have mapped a PTP server onto LAN4, select LAN4 to observe its status. As the following figure shows, the specific service in use is identified (fully configured in 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 6-30.

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 the preceding figure, where the NTPr service is mapped to LAN2, the status examples are shown in Figure 6-29 and Figure 6-30.

Figure 6-27. Example Status on Network Timing > NTPr/PTP Status Form (PTP Server)



NTPr/PTP Status

LAN2

LAN3

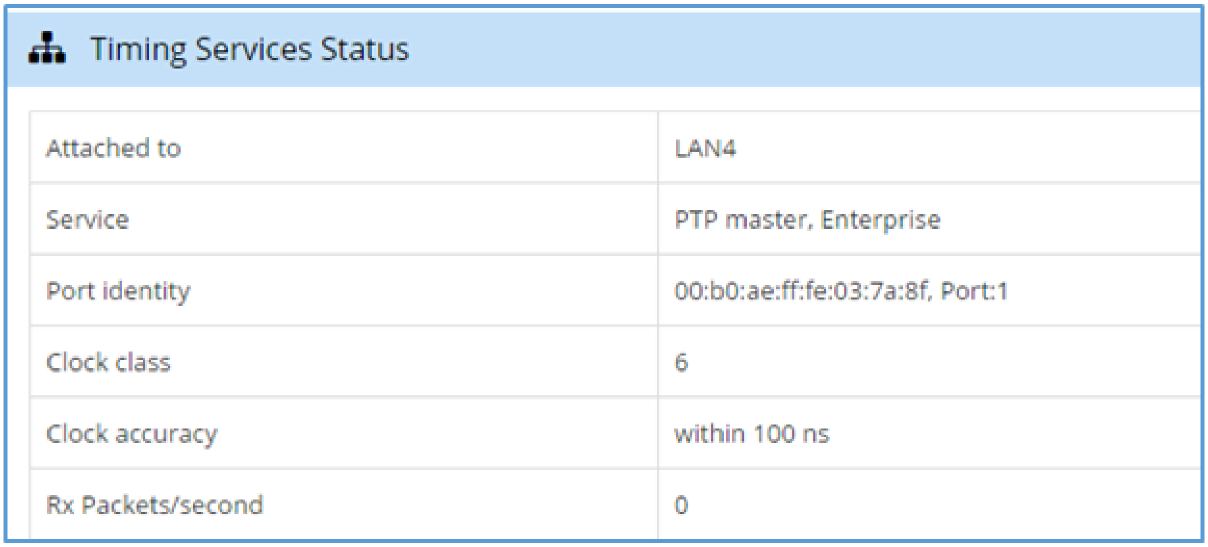
LAN4

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

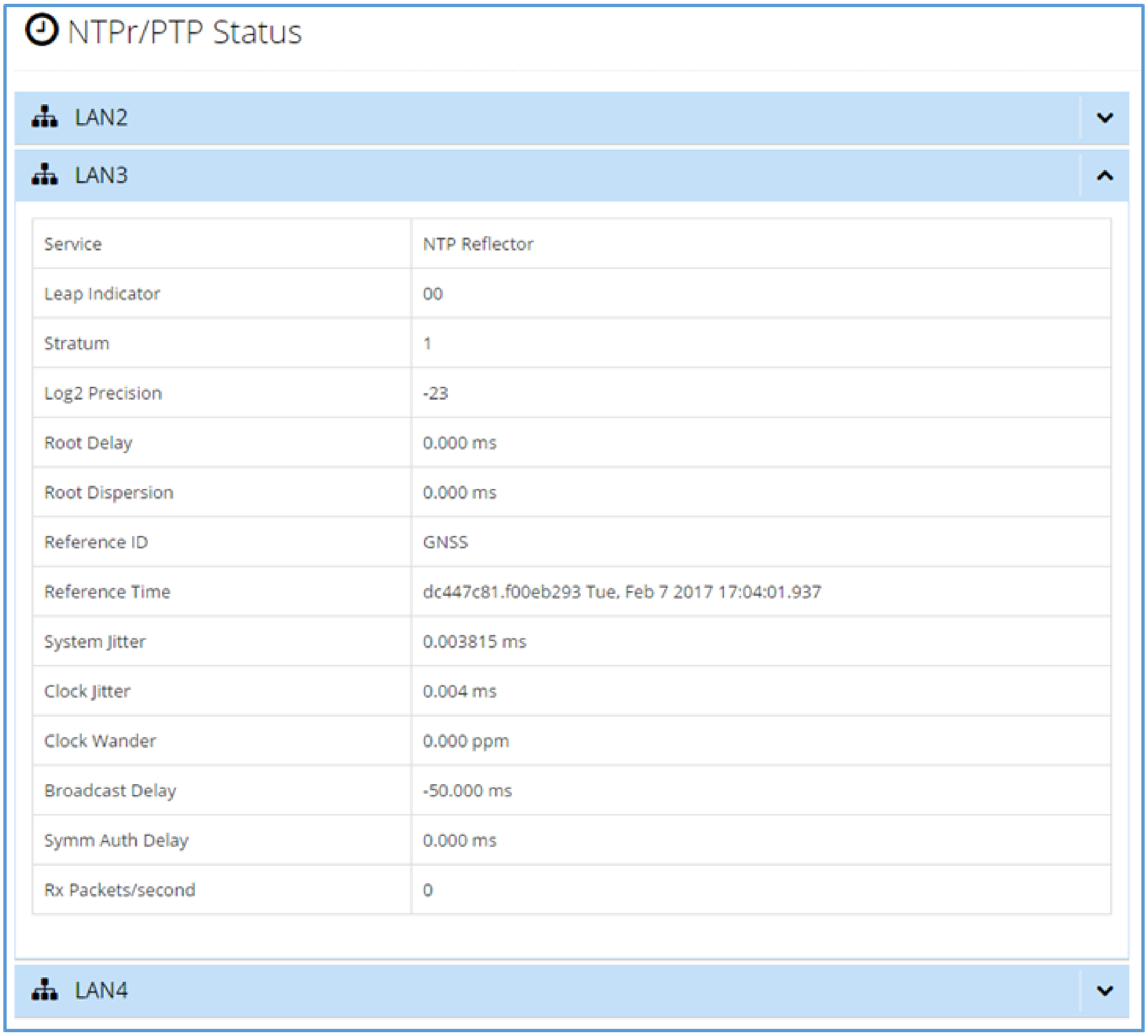
Figure 6-28. Timing Service Status on Dashboard > Timing Services Status (PTP Server)



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

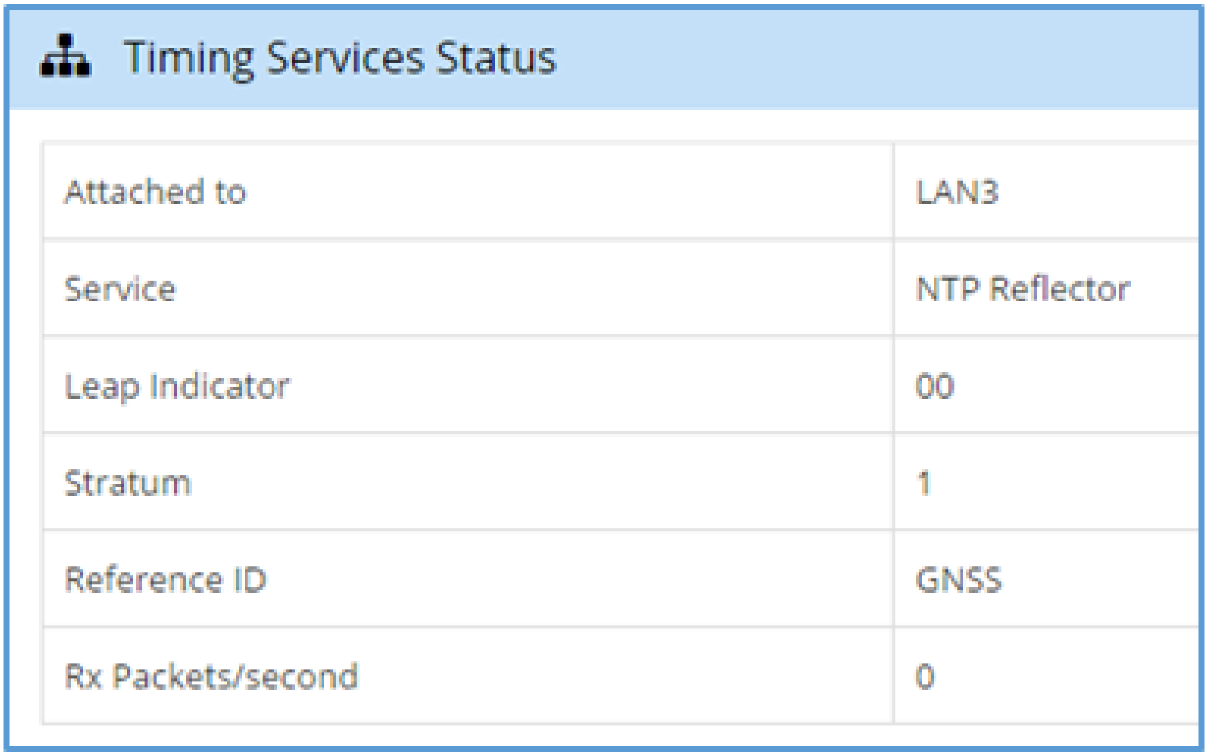
Figure 6-29. Example Status on Network Timing > NTPr/PTP Status Form (NTPr)



NTPr/PTP Status

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

Figure 6-30. Timing Service Status on Dashboard > Timing Services Status (NTPr)



Timing Services Status

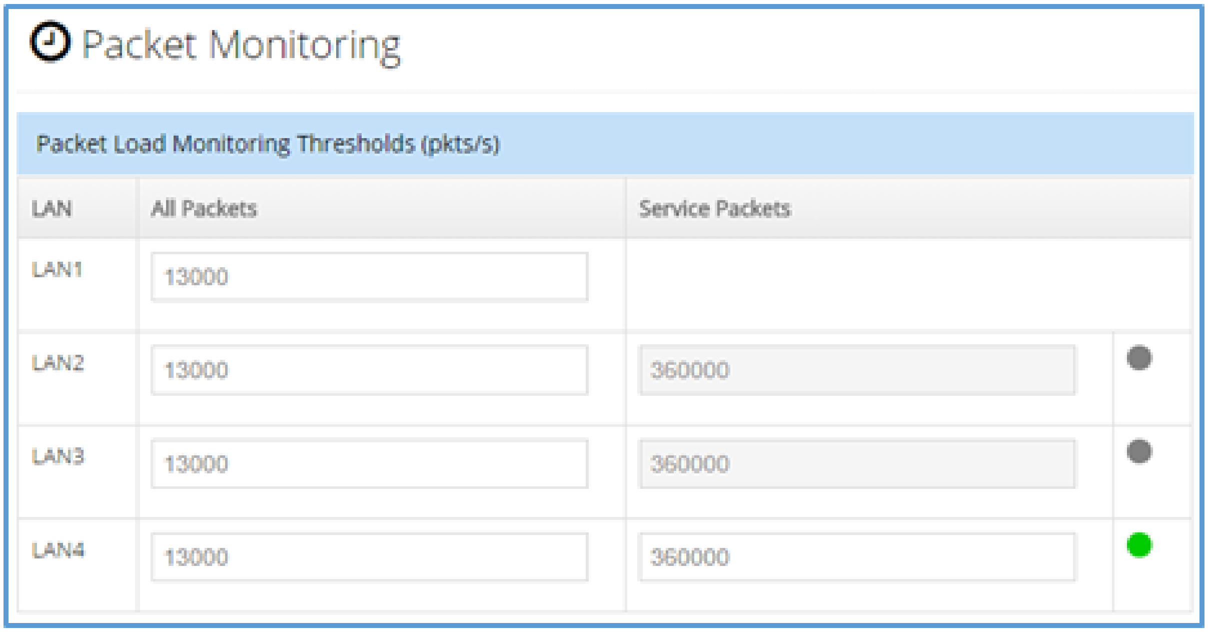
Attached to	LAN3
Service	NTP Reflector
Leap Indicator	00
Stratum	1
Reference ID	GNSS
Rx Packets/second	0

6.8.4 Monitoring Network Packets

S6x0 provides capability to monitor and limit incoming packets on each of its LAN ports (see 5.2.5.12. 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 server 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 can 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.

Figure 6-31. Configuring Packet Monitoring Thresholds



Packet Monitoring

Packet Load Monitoring Thresholds (pkts/s)

LAN	All Packets	Service Packets	
LAN1	13000		
LAN2	13000	360000	●
LAN3	13000	360000	●
LAN4	13000	360000	●

6.8.5 Provisioning 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 server 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 server 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 server 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.	—
	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 server to the desired LAN port.
CLI	n/a	n/a
Front Panel	n/a	n/a

SyncServer only support TAI timescale. The ARB timescale is not used.

Per the enterprise profile specification, the PTP output is not enabled until the UTC offset is known. This must be manually entered on the 5.2.3.1. 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 must only be configured for the PTP server configuration when it is used with a 1588 2.1 client.

6.8.6 Provisioning PTP Server-PTP Output Power Profiles

Three types of PTP power profiles for grandmaster operations are supported. As with all PTP Server functionality, the PTP Server 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

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 server, which when selected, allows each of these power profiles to be selected from the Profile selection control in that row (see 6.8.1. 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 6.8.2. Mapping Network Timing Service to LAN Port).

The following is the summary of basic similarities and differences between these profiles. It might 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 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 the C37.238 profiles include configuration (where appropriate) for both the messages. Following are the 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 organization ID for both the C37.238 profiles is 0x1C129D. This is not user-configurable. This value is always automatically encoded for this field.
  - The organization SubType is 0x000001 for profile C37.238-2011 and 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 can 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 the 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 that contains the 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 every configured field is incorporated into the outbound TLV. Additionally, an Enable/Disable control is provided to support withholding this TLV, if desired.

SyncServer does not support SNMP MIB for Power Profile.

6.8.7 Viewing PTP Clients for PTP GM Outputs

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 the following:

- 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.	—

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

Method	Steps	Notes
CLI	n/a	n/a
Front Panel	n/a	n/a

6.8.8 Provisioning 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 RMC output – NMEA—0183 GSV output 3. Click the **Apply** button.	Select NMEA output format. See the following table 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 – YYYY DDD HH:MM:SS DZZ – WWW DDMMMYY HH:MM:SS 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 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`
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 1-1 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, and so on) on all configurable ports through the secure Web interface.

Note: SyncServer S6x0 uses IRIG 1344 version C37.118.1-2011. Control bits 14–19 are always zero, and the encoded IRIG time is UTC (if using an input 1344 IRIG as the reference the 2011 rules are applied to get that value). Therefore, any code receiving S6x0 IRIG 1344 output must work regardless of which version they are decoding (as 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

Notes:

- The web page might allow a larger range for the phase offset value, but the supported range is from –0.499999800 to 0.499999800.
- For the 1 PPS falling edge pulse, the maximum supported negative offset is –499,970,000 ns.

During startup and holdover recovery, the fixed-rate pulse count might adjust. For example, if 10 MPPS is configured, there may not be exactly 10 million pulses during every one 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

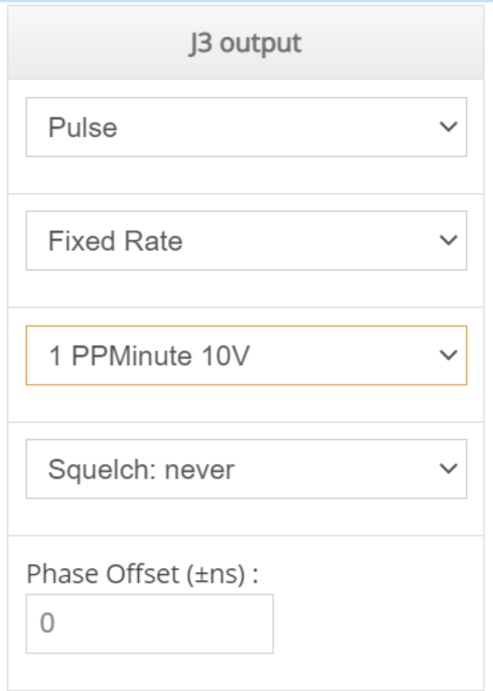
Method	Steps	Notes
Web Interface	Option Slot A > Timing I/O Card T1 Output 1. For T1 output on J7, use dropdown box to select signal type of T1 Output. 2. Click the Edit button. 3. Use the dropdown box to select the frame type of ESF, D4 or freq1544 kHz. 4. Click the **Apply** button. E1 Output 5. For 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 freq2048 khz. 8. Click the **Apply** button. Timing I/O Outputs For other ports, see 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, 1 PPS 10V, and 1 PPS 5V.
  The combined capability for these two specific outputs is thereby extended to three signal levels: TTL (the common setting for all modules) plus the two new that are unique to this module: 5V and 10V, as shown in the following figure.



J3 output

Pulse

Fixed Rate

1 PPMinute 10V

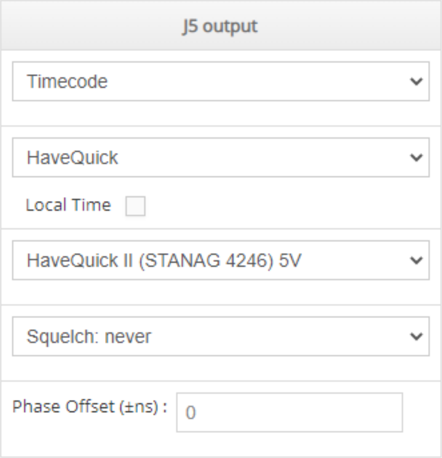
Squelch: never

Phase Offset (±ns) : 0

- A set of HaveQuick codes is supported. Each timecode is provided with two 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 document1. 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. J1 input also supports this timecode.
  - HaveQuick Extended (STANAG 4430). This code adds leap second content (compared to ICD-GPS-060A). 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 ToD. 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 figure. 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 second control.
2. Select HaveQuick from the available list on the second control.
3. Select the desired HaveQuick output code on the third control, in this case HaveQuick II.


J5 output

Timecode

HaveQuick

Local Time □

HaveQuick II (STANAG 4246) 5V

Squelch: never

Phase Offset (±ns) : 0

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 ToD) are meaningful. The remaining bits are set high.

For test purposes a selectable 1 PPS or 1 PPMinute output is also available on the connection. The following table lists the pinouts.

Table 6-26. J7 and J8 Connector Pin Assignments—Timing I/O Module with HaveQuick/PTTI Connections

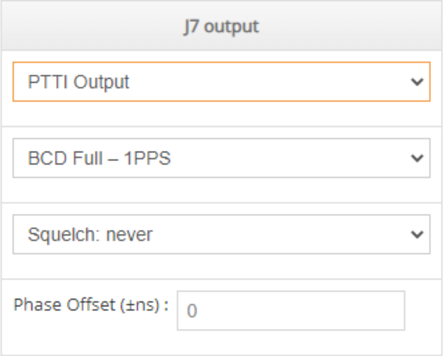
Pin	Signal
1	PTTI BCD Tx+ (code out)
2	PTTI BCD Tx– (code out)
3	1 PPS/PPM out, TTL level (for test purposes only)
4	Ground
5	Reserved, do not connect
6	N/C
7	Reserved, do not connect
8	Reserved, do not connect

Electrical characteristics for code outputs on pins 1 and 2 are as described in ICD-GPS-060 revision B, section 3.4.3.3.

Configure BCD codes for output on J7 or J8:

1. 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.
2. The only top-level choices are off (no output) or PTTI output, as shown in the following figure. Select the PTTI output.
3. The second control lists the following available options:
   - BCD Full–1 PPS. This generates the full BCD code along with 1 PPS test signal on pin 3.
   - BCD Full–1 PPM. This generates the full BCD code along with 1 PPM (1 pulse per minute) test signal on pin 3.
   - BCD Abbrev–1 PPS. This generates the abbreviated BCD code (still 50 bits, but only first 24 contain content) along with 1 PPS test signal on pin 3.

– BCD Abbrev–1 PPM. This generates the abbreviated BCD code (still 50 bits, but only first 24 contain content) along with 1 PPM test signal on pin.



J7 output

PTTI Output

BCD Full – 1PPS

Squelch: never

Phase Offset (±ns) : 0

4. Select Apply to complete the configuration.

6.8.12 Provisioning Programmable Pulse Output

The following table lists the Timing I/O modules that can provide a programmable pulse output when installed in 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 S650, then there can be two 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 Telecom
Timing I/O module with fiber input	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

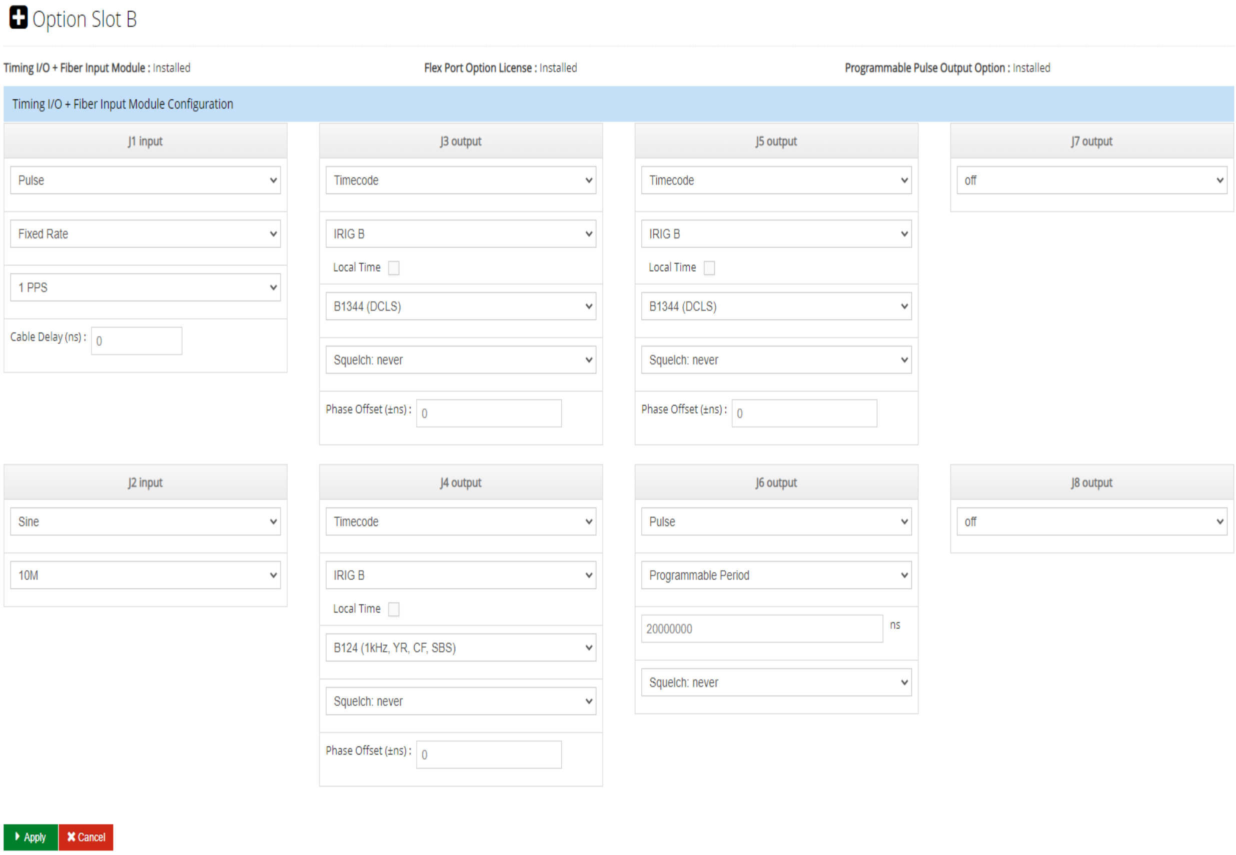
Additional capability is provided to define wildcard digits that allow repeat pulse outputs when the first non-wildcard digit is matched in time.

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. The following figure shows an example, where the module in SLOT A is used and the J7 output is shown to already be set up for the Programmable Pulse capability.
Note: In the region above the J7 configuration, it is shown that the Programmable Pulse Output Option is installed. If it is not installed, this setting is not available. All currently installed options are listed at `Admin > Options`.

Figure 6-32. Option Slot Window—Timing I/O Module with Programmable Pulse License Installed



Option Slot B

Timing I/O + Fiber Input Module : Installed   Flex Port Option License : Installed   Programmable Pulse Output Option : Installed

Timing I/O + Fiber Input Module Configuration

J1 input: Pulse; Fixed Rate; 1 PPS; Cable Delay (ns) : 0

J3 output: Timecode; IRIG B; Local Time □; B1344 (DCLS); Squelch: never; Phase Offset (±ns) : 0

J5 output: Timecode; IRIG B; Local Time □; B1344 (DCLS); Squelch: never; Phase Offset (±ns) : 0

J7 output: off

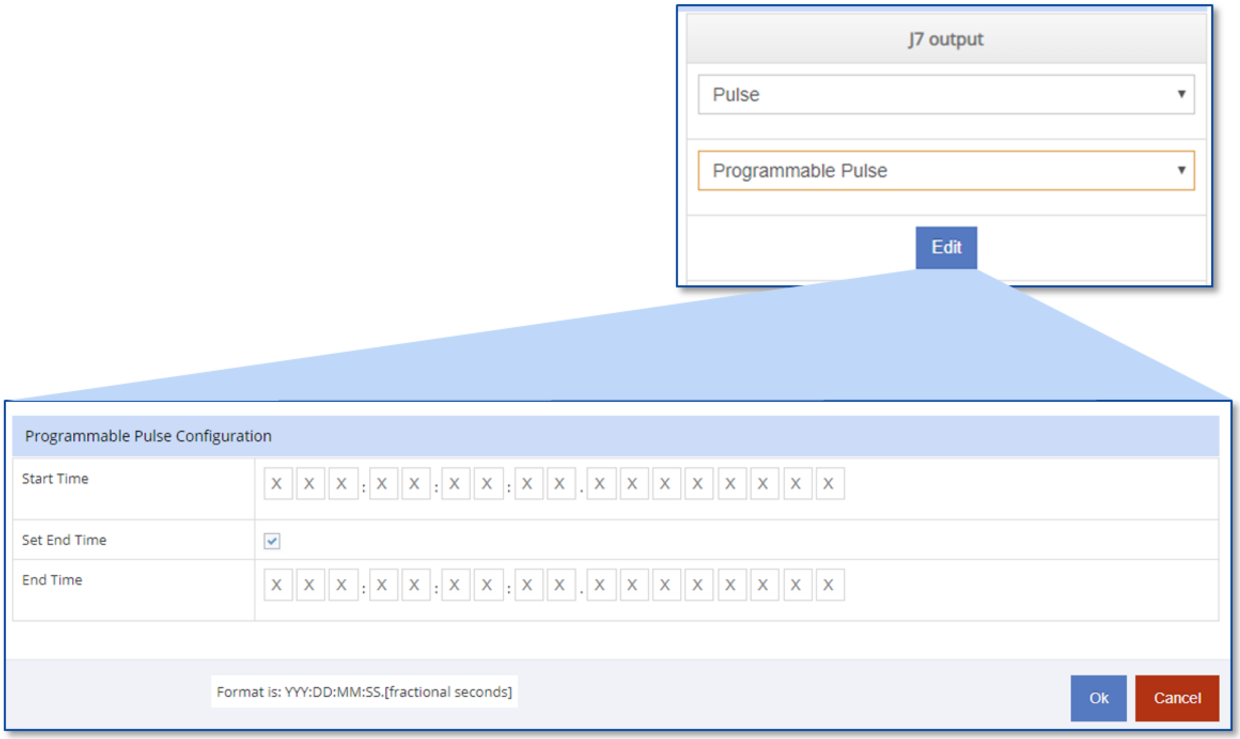
J2 input: Sine; 10M

J4 output: Timecode; IRIG B; Local Time □; B124 (1kHz, YR, CF, SBS); Squelch: never; Phase Offset (±ns) : 0

J6 output: Pulse; Programmable Period; 20000000 ns; Squelch: never

J8 output: off

Figure 6-33. Programmable Pulse Form



J7 output: Pulse; Programmable Pulse

Programmable Pulse Configuration

Start Time: X X X : X X : X X : X X . X X X X X X X X

Set End Time: ☑

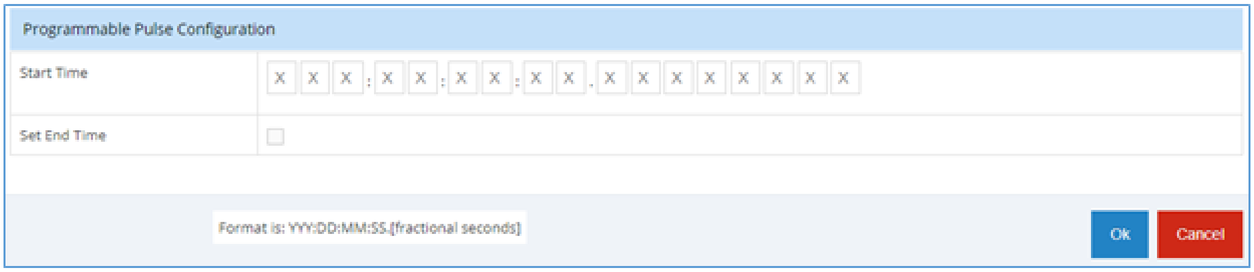
End Time: X X X : X X : X X : X X . X X X X X X X X

Format is: YYY:DD:MM:SS.[fractional seconds]

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 must 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 (for example, 00–23 combined range).

Figure 6-34. Programmable Pulse Configuration



Programmable Pulse Configuration

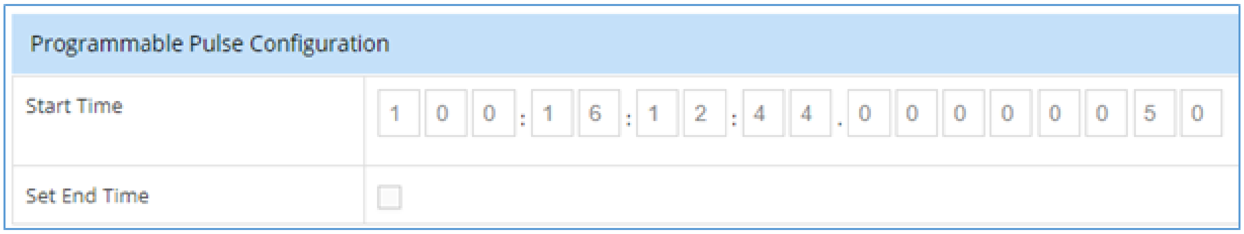
Start Time	X X X : X X : X X : X X . X X X X X X X X
Set End Time	□

Format is: YYY:DD:MM:SS.[fractional seconds]

The simplest usage is to provide numeric entry (no wildcards) for every box. This has the effect of generating only one pulse per year, but it is a helpful way to understand the most basic operation. In other words, the following configuration produces 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, 44thsecond of that minute, 500 nanoseconds after the start of the 44th second

Note: There are eight fractional seconds digits, so the rightmost is tens of nanoseconds. That is why the value shown is 500 ns).

As the end time control is not used in this case, the pulse width is defaulted to the shortest possible, which is 10 ns.



Programmable Pulse Configuration

Start Time	1 0 0 : 1 6 : 1 2 : 4 4 . 0 0 0 0 0 0 5 0
Set End Time	□

As 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 (that is, a number is encountered), there can be no more wildcards.

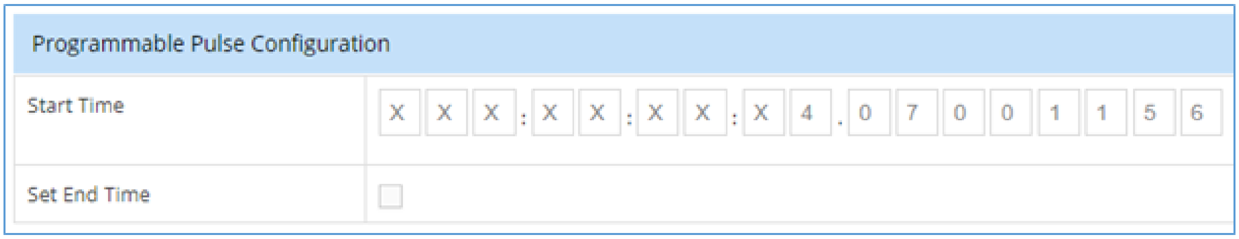
Tip: If you first enter the rightmost wildcard, then all the positions to the left are auto-filled with wildcards.

Following is an example:

- Wildcards are entered for all entries from the left through the tens of seconds digit. The current time for all the wildcard entries never prevents 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. As everything to the left is a wild card, it means that outputs occur sometime in every second that ends in 4. This equals to six different times in every minute: seconds 04, 14, 24, 34, 44, and 54.
- As there are further non-zero digits to the right of the 4, the actual time of the pulse outputs is 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.

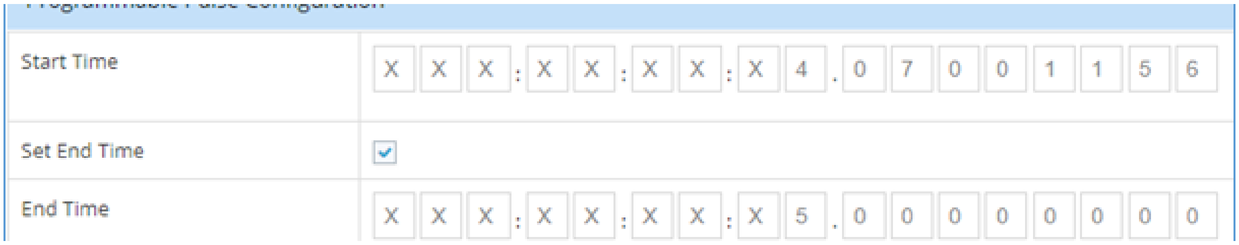


Programmable Pulse Configuration

Start Time	X X X : X X : X X : X 4 . 0 7 0 0 1 1 5 6
Set End Time	□

For all the preceding examples, the pulse width is 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 following figure 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 following example shows that when wildcards are used, both start and stop must share the same wildcard positions, which is enforced by the interface behavior. This example generates pulse widths of about one second, short of that amount by 70.01156 ms, as 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.



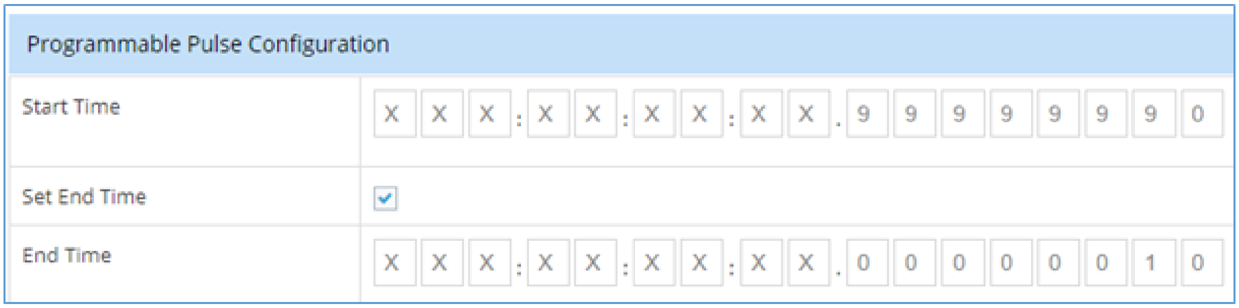
Start Time	X X X : X X : X X : X 4 . 0 7 0 0 1 1 5 6
Set End Time	☑
End Time	X X X : X X : X X : X 5 . 0 0 0 0 0 0 0 0

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 following setup accomplishes this:

- As we are using the wildcard at the 1 second digit, the start time initiates 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.

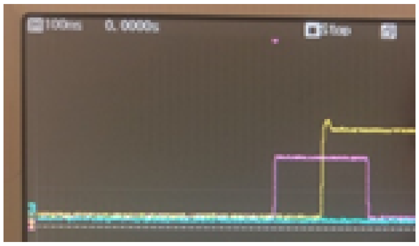
The following figure shows the result on a scope. The yellow waveform is an on-time rising-edge PPS signal. The magenta waveform is the programmed pulse generated by this setup.
Note: The waveform straddles the PPS signal by 100 ns on either side.

This example also shows the behavior when the end time value is a smaller value than the start time, which might seem illogical. The way to think of it is that there is always cause-and-effect between start and end time. If the programmed pulse has not 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, as there has not 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 continues 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.



Programmable Pulse Configuration

Start Time	X X X : X X : X X : X X . 9 9 9 9 9 9 9 0
Set End Time	☑
End Time	X X X : X X : X X : X X . 0 0 0 0 0 0 1 0



To complete any setup, the OK control in lower right is chosen, which returns 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 appears, so that you can save the programmable pulse configuration, if desired.

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 can make time-interval and event timestamp measurements.

6.9.1 Measurement Basics

The time-interval measurement function on S6xx is similar to the measurement on a traditional time-interval stand-alone instrument: measurement of the time-difference between two 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. Following are some of the differences:

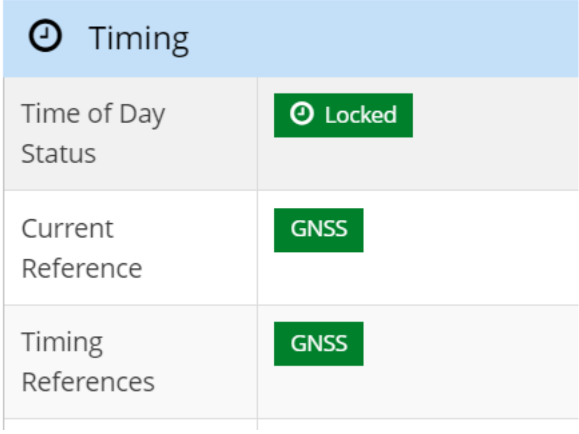
- There is only one input needed: The PPS to be measured. This is connected to the J1 input on the desired module (if there are two modules, then either J1 can be used).
- The J1 input is internally measured against the reference PPS. This reference is the same as the 1 PPS output generated by the S6xx. 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 S6xx.
- Unlike using a time-interval counter, which does not have time awareness, 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 (for example, disconnected or squelched at the source) no measurements are taken during that period but if the signal later returns, then the measurements automatically proceed. The gap in data collection is 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 is positive. If the J1 input PPS occurs before the reference, the result is negative. In general, the “closest reference PPS” is 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 are tagged when they occur. The sustained maximum rate where no events are 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 5.3.3. Admin—Alarm Configuration Window).

Notes: General notes applicable to either of the measurement functions:

- 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 function even if there is no reference into S6xx (for example, S6xx measures even if it is freerunning with no awareness of the current time). While this allows for some special case measurements, users must ensure that the ToD status (see `Dashboard > Timing`) is in Locked state if the objective is to make accurate measurements against a good reference. Following is an optimal display for this use-case:



Timing

Time of Day Status	Locked
Current Reference	GNSS
Timing References	GNSS

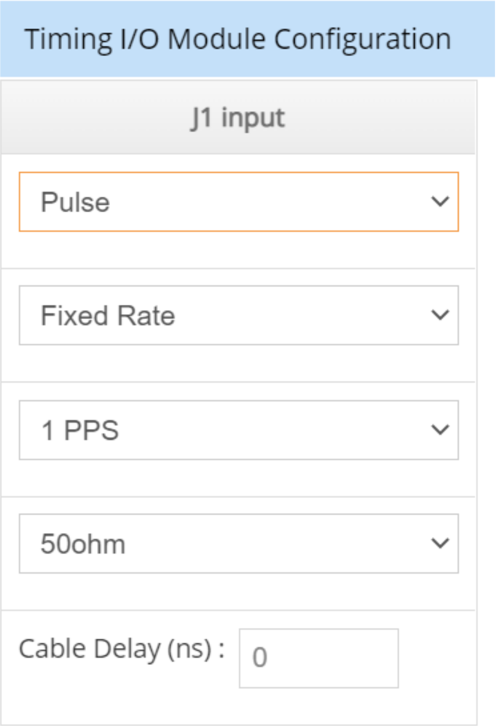
6.9.2 Measurement Setup

1. Connect the signal to be measured to the J1 input that is to be used. 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 three

choices as shown: Pulse, Fixed Rate, and 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 can eliminate transmission time due to cable.

Notes:

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



Timing I/O Module Configuration

J1 input

Pulse

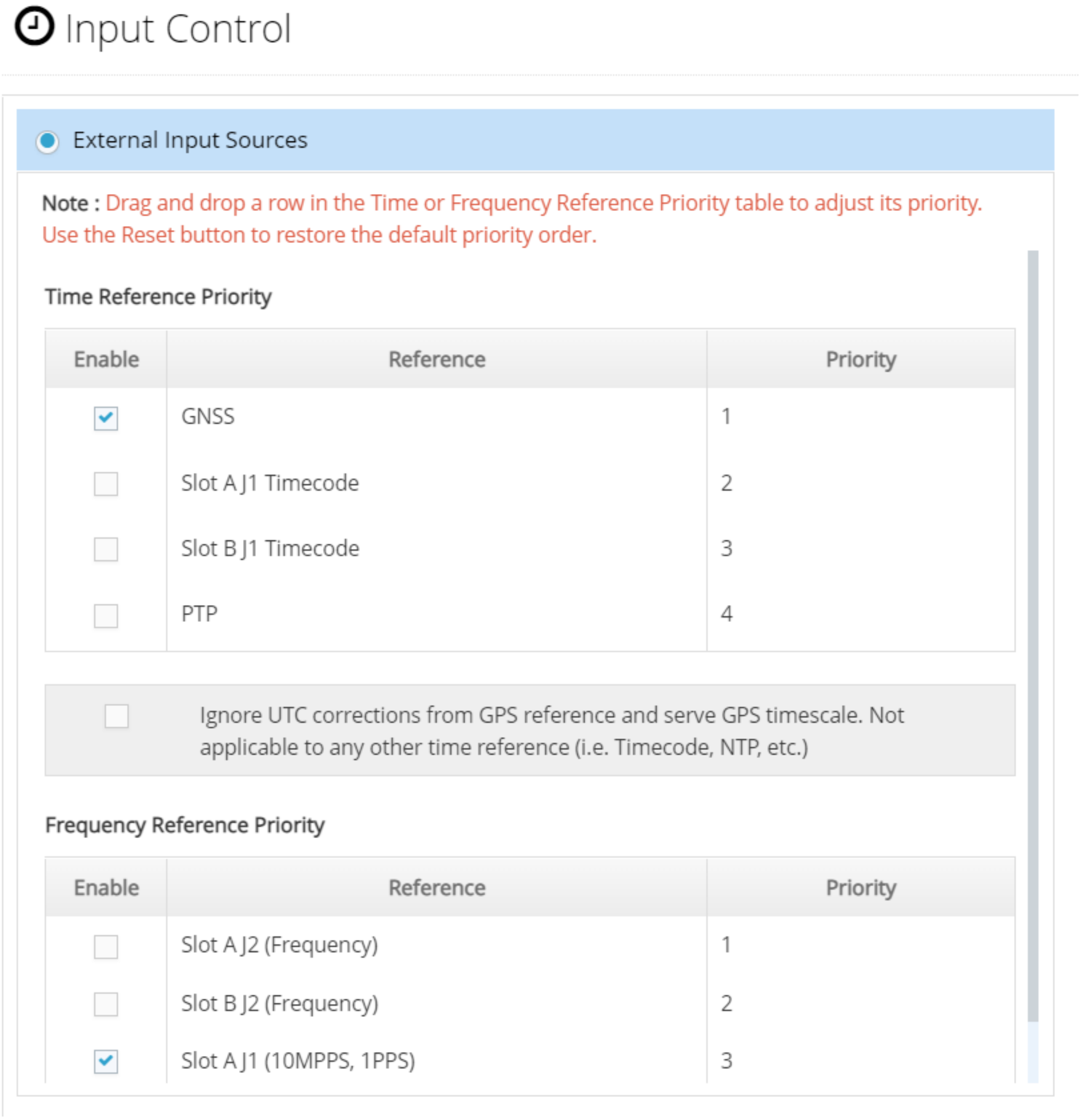
Fixed Rate

1 PPS

50ohm

Cable Delay (ns) : 0

2. As it makes no sense to also allow use of this input also as a sync input reference, the J1 connection must not be enabled on the `Timing > Input Control form`, as shown in the following figure. Disabling J1 as a timing input reference source does not restrict its usage for measurement.



Input Control

● External Input Sources

Note : Drag and drop a row in the Time or Frequency Reference Priority table to adjust its priority. Use the Reset button to restore the default priority order.

Time Reference Priority

Enable	Reference	Priority
☑	GNSS	1
□	Slot A J1 Timecode	2
□	Slot B J1 Timecode	3
□	PTP	4

□ Ignore UTC corrections from GPS reference and serve GPS timescale. Not applicable to any other time reference (i.e. Timecode, NTP, etc.)

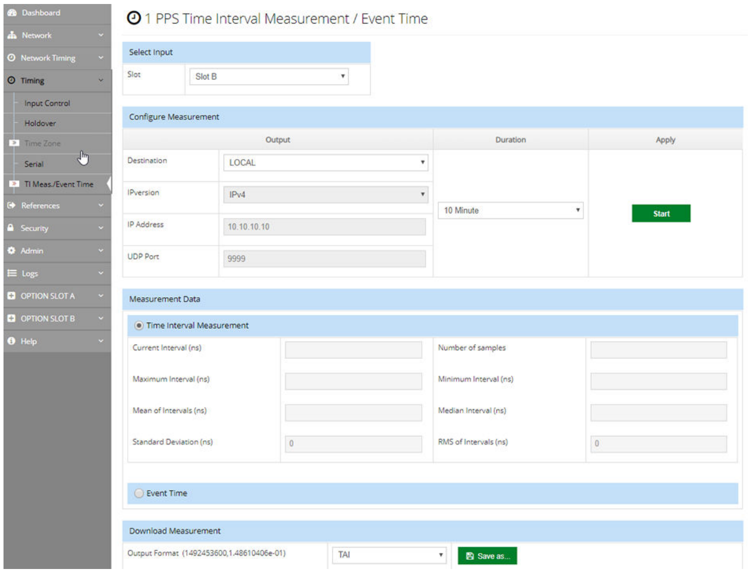
Frequency Reference Priority

Enable	Reference	Priority
□	Slot A J2 (Frequency)	1
□	Slot B J2 (Frequency)	2
☑	Slot A J1 (10MPPS, 1PPS)	3

6.9.3 Making the Measurement

Either type of measurement is controlled on the `Timing > Meas./Event Time` form, as shown in the following figure.

Figure 6-35. Time Interval Measurement/Event Time



1 PPS Time Interval Measurement / Event Time

Select Input

Slot: Slot B

Configure Measurement

Output		Duration	Apply
Destination	LOCAL	10 Minute	Start
IPversion	IPv4		
IP Address	10.10.10.10		
UDP Port	9999		

Measurement Data

● Time Interval Measurement

Current Interval (ns)		Number of samples	
Maximum Interval (ns)		Minimum Interval (ns)	
Mean of Intervals (ns)		Median Interval (ns)	
Standard Deviation (ns)	0	RMS of Intervals (ns)	0

○ Event Time

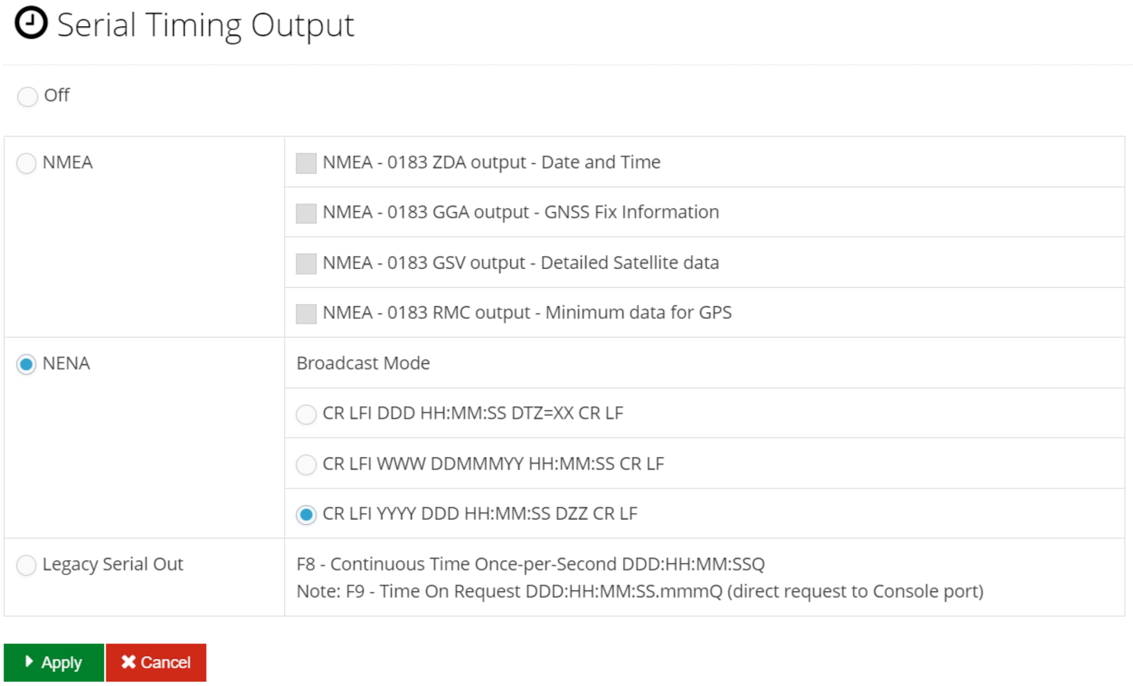
Download Measurement

Output Format (1492453600,1.48610406e-01): TAI

- The Select Input Slot control identifies which slot module J1 connection is used for the measurement. Selection is only possible if S6xx contains two slot modules and both are capable of supporting measurement. If there is only a single module, no choice can be made and the control shows the correct slot. This control is common to time-interval and event timestamping measurements.
- The Configure Measurement section provides three 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 S6xx. Regardless of the 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 and not the 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 continue to be saved, pushing the oldest ones out as needed, so that the contents of the storage (when filled) always be the most recent 86,400 measurements.

    With this setting, none of the other selections in the Output section are relevant (they are greed out).
  - Setting Destination to SERIAL directs the measurement results to the Data/Timing 9-pin serial connection on S6xx. Any terminal program that supports serial connection can be used to collect (and log if desired) the results. As there are other possible uses for this connection, it might be necessary to de-activate other enabled functions currently assigned to it. These other uses are controlled at the `Timing > Serial form`. To use this connection for output of measurements, this form must have setting to OFF, as shown in the following figure.

Figure 6-36. Serial Timing Output Configuration



Serial Timing Output

○ Off

○ NMEA	□ NMEA - 0183 ZDA output - Date and Time
	□ NMEA - 0183 GGA output - GNSS Fix Information
	□ NMEA - 0183 GSV output - Detailed Satellite data
	□ NMEA - 0183 RMC output - Minimum data for GPS
● NENA	Broadcast Mode
	○ CR LFI DDD HH:MM:SS DTZ=XX CR LF
	○ CR LFI WWW DDMMMYY HH:MM:SS CR LF
	● CR LFI YYYY DDD HH:MM:SS DZZ CR LF
○ Legacy Serial Out	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)

- 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 ToD port (on the left side of the form), which is the lower 9-pin connection labeled Data/Timing port on S6xx. Configure these settings to agree with the terminal program settings on the device used to receive the measurements.
  Note: The lower baud rates decrease the number of event time measurements that can be made each second. For example, 9600 baud may limit event time measurements to 25/s instead of 100/s. With the 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 Web GUI). With this setting, the other controls are used to specify the connection that receives the LAN1 output: IP version, IP Address, and UDP port.

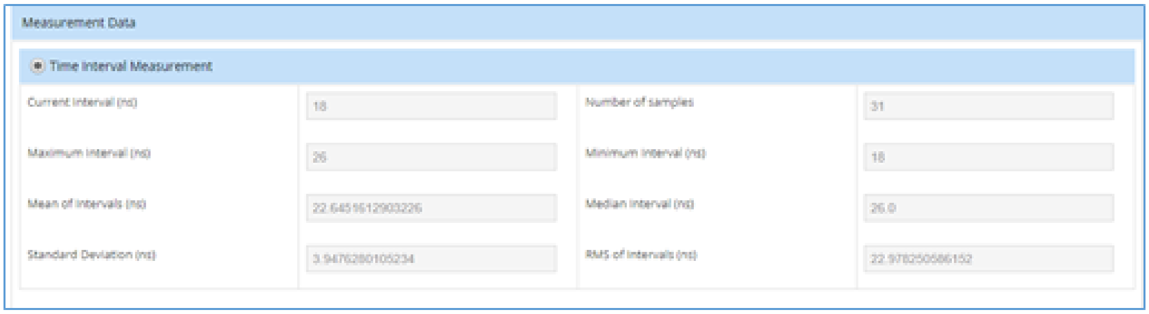
- The Duration section provides control for how long the measurement must run. The control provides a range of bounded choices, all of which open and close the measurement window for the indicated time, initiated by activation of the Start control. The measurement window self-terminates regardless of whether or not any actual measurements have 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 occurs upon its application. Selecting Start begins the measurement and grays out other control settings, as the measurement parameters are “locked in” if the measurement is running. When the measurement is running, the control indicates 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 does 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 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 S6xx system PPS. While the measurement runs, if the measurement Destination is set to LOCAL, the data shown in the following figure 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.



Measurement Data

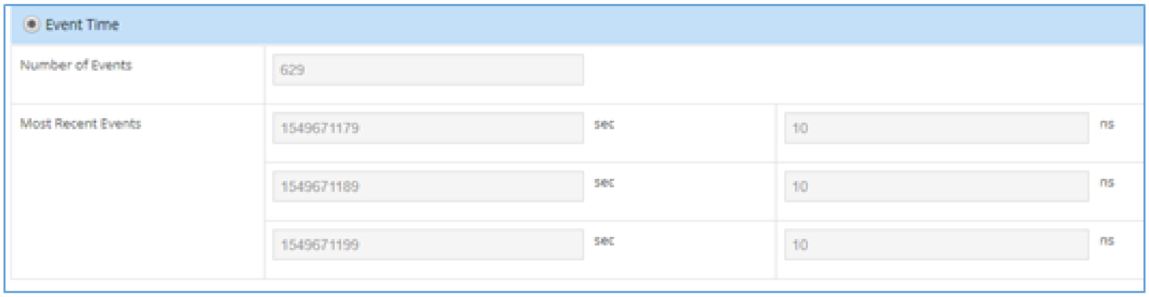
● Time Interval Measurement

Current Interval (ns)	18	Number of samples	31
Maximum Interval (ns)	26	Minimum Interval (ns)	18
Mean of Intervals (ns)	22.6451612903226	Median Interval (ns)	26.0
Standard Deviation (ns)	3.9476280105234	RMS of Intervals (ns)	22.978250586152

– 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 in the following figure is periodically updated. This is a sampling of three recent timestamped events (this display may not always show consecutive events, but the stored data does not miss any events if the sustained input event rate is not greater than 100 events/s).

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 in the following figure, the three events are seen to be precisely 10 seconds apart. The source for these events is 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.



● Event Time

Number of Events	629			
Most Recent Events	1549671179	sec	10	ns
	1549671189	sec	10	ns
	1549671199	sec	10	ns

- 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: The #Start information provides the TAI time of the first measurement in traditional format (it does not 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: The #Start information makes it easy to know in traditional format the TAI time of the first event (it does not 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 SyncServer S6x0. For a list of all alarms, see 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 Acknowledgment) 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 acknowledgment of the alarm, but 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
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 Download button. Enter the desired file name and navigate to the desired location to store the file. 4. Click the **Apply** button.

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

Method	Steps
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 adio 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 must 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 can be MD5, SHA1, SHA224, SHA256, SHA384, or SHA512, with up to a 32-character key. The privacy algorithm can be AES128, AES192, AES192C, AES256, or AES256, with up to a 32-character key.

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.

Notes:

- Changing an SNMP configuration parameter (such as community or SNMPv3 user) causes SNMP to restart and the MIB2 `sysuptime` to restart counting upward.
- To disable SNMPv2c access, delete/blank the SNMP community name(s).

6.12.1 SNMP Status

SyncServer S6x0 supports a proprietary MIB, S650.mib, which provides selected status information for the unit.

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 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 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 must be used to determine which alarm or event was generated. Alarm and Event IDs are listed in 8. System Messages.

Note: SNMP MIB can be downloaded from 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 are compatible with newer versions of firmware, but do 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, SyncServer S6x0 generates v2 traps.

Table 6-32. Provisioning to Generate v2 Traps

Method	Steps
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, SHA1, SHA224, SHA256, SHA384, or SHA512 for auth. 6. Enter privacy phrase, if required. 7. Enter privacy algorithm, if required: AES128, AES192, AES192C, AES256, or AES256. 8. Click the **Save** button.	For SNMPv3 traps, both a user and a trapuser must be configured identically, depending on the SNMP trap manager. In addition, the SNMP manager must use the specified user/trapuser to connect to SyncServer S6x0. This ensures that a SNMPv3 trap is 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 the **Save** button.	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 disables SNMPv2.

6.12.6 Adding and Removing SNMP v3 Users

SNMPv3 provides additional security features that are 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 MD5, SHA1, SHA224, SHA256, SHA384, or SHA512, with a key of up to 32 characters in length. The privacy algorithm is either AES128, AES192, AES192C, AES256, or AES256 with a key of up to 32 characters in length. All keys are uppercase.

Table 6-35. Adding/Removing SNMP v3 Users

Method	Steps
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 authentication: MD5, SHA1, SHA224, SHA256, SHA384, or SHA512. 6. Enter privacy algorithm if required: AES128, AES192, AES192C, AES256, or AES256. 7. Click the **Save** button.
CLI	n/a
Front Panel	n/a

Note: All character except (<), (&), (>), (“), and (') are accepted for SNMP user names, authentication, or privacy keys.

6.13 Provisioning HTTPS Certificate

This method must be used only if the security license is not installed. If the security license is installed, then use the `Security > X.509 SS Cert/CS Req` and `Security > X.509` Mapping pages.

Table 6-36. Provisioning Self Signed HTTPS Certificate

Method	Steps
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 reduces standard NTP operations to a maximum rate of 5000 NTP requests per second. The NTP Reflector timestamping capacity remains unchanged at 360,000 NTP requests per second.

Note: After installing the BlueSky software license, the detectors do not operate until the user starts the desired detector(s) on the Detectors page.

6.14.2 BlueSky Overview

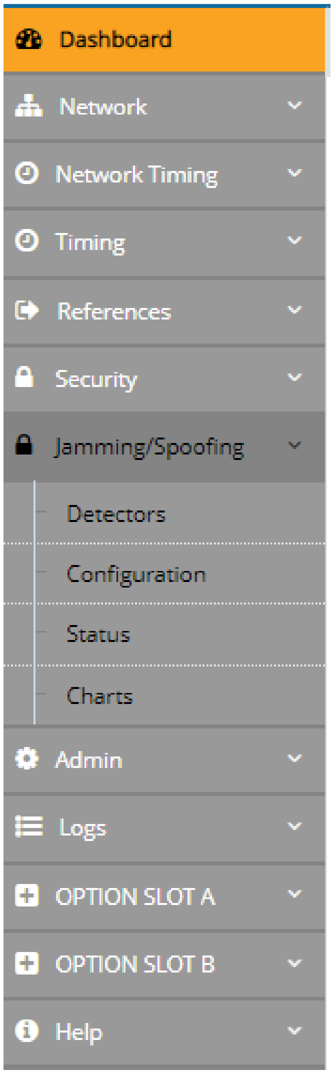
The GNSS BlueSky capability provides an extensive set of detectors that monitor many aspects of GNSS as observed at that specific S6xx installation. General monitoring categories include tracking, spoofing, RF health, and navigation message content. The capability is highly configurable, ranging from 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 and 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 6.14.4.1. Site Survey).

6.14.3 Getting Started

The following figure shows the left panel navigation to access BlueSky capability.

Figure 6-37. BlueSky Navigation—Top Level



Perform the following steps to run GNSS BlueSky capability:

1. Enable process for any detector groups you want to run.
   These are controlled on BlueSky summary form (Figure 6-38) in the **Action** column and are disabled (not running) from factory. Navigate to this form, as shown in the preceding figure. Use the **Action** column to start running any detector group. The settings are retained if the unit is power-cycled.

   Also, consider enabling GNSS Site Survey on summary form to evaluate the GNSS installation. For details, see 6.15.5. Cumulative Site Survey Chart.
2. Enable any alarms and associated behaviors.
   Primary alarm enable/disable controls for BlueSky detectors are on the configuration form (Figure 6-39). Navigate to this form as shown in the preceding figure. 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. For details, see 6.14.8. Alarms and Associated Controls. Other alarm-specific controls are found on `Admin > Alarms form`. Scroll to specific BlueSky alarms and configure as desired.

   These settings are retained if the unit is power-cycled.
3. Monitor results.
   The status form (navigate as shown in the preceding figure, see example at Figure 6-41) provides live updates for all detectors.

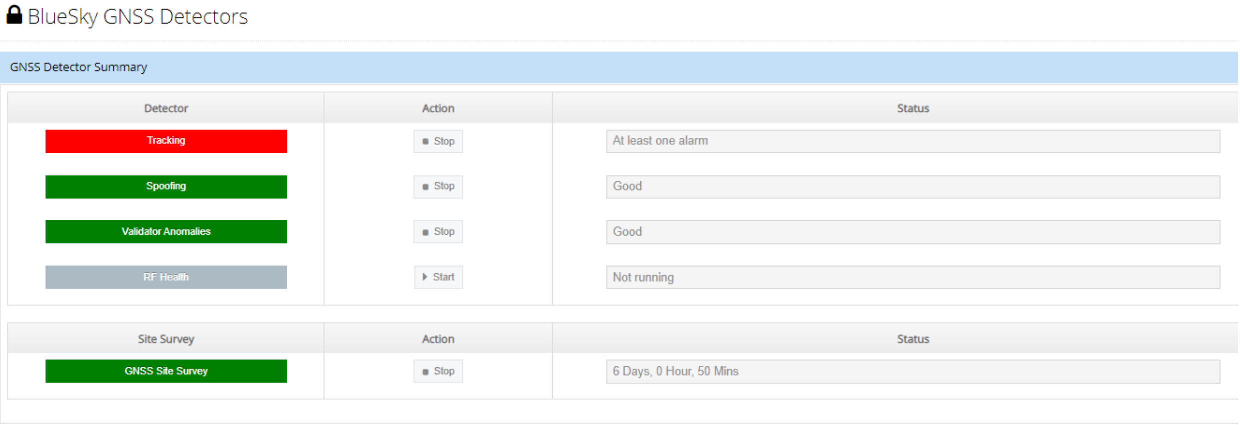
   Many detectors provide charts and download capability. Navigate as shown in the preceding figure and see explanations and examples in 6.15.5. Cumulative Site Survey Chart.

   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 figure shows the BlueSky summary form. This form provides the highest-level status view and control capability. Based on this form, you might choose to drill-down to other forms for greater detail.

Figure 6-38. BlueSky Summary Form



BlueSky GNSS Detectors

GNSS Detector Summary

Detector	Action	Status
Tracking	■ Stop	At least one alarm
Spoofing	■ Stop	Good
Validator Anomalies	■ Stop	Good
RF Health	▶ Start	Not running

Site Survey	Action	Status
GNSS Site Survey	■ Stop	6 Days, 0 Hour, 50 Mins

- 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 is as follows.
  – 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 happens if the control is selected. For example, if the control shows **Start**, then 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**, then it always means that the process is currently running. This does not always mean that it is receiving data, but it will do so every time the data is available. Selecting **Stop** terminates 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 to begin a new data collection process for detectors in that group. This action transitions 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, as the subsequent start clears 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 preceding it, which is why it is given its own sub-section on the form. As 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. For details, see 6.15.5. Cumulative Site Survey Chart.

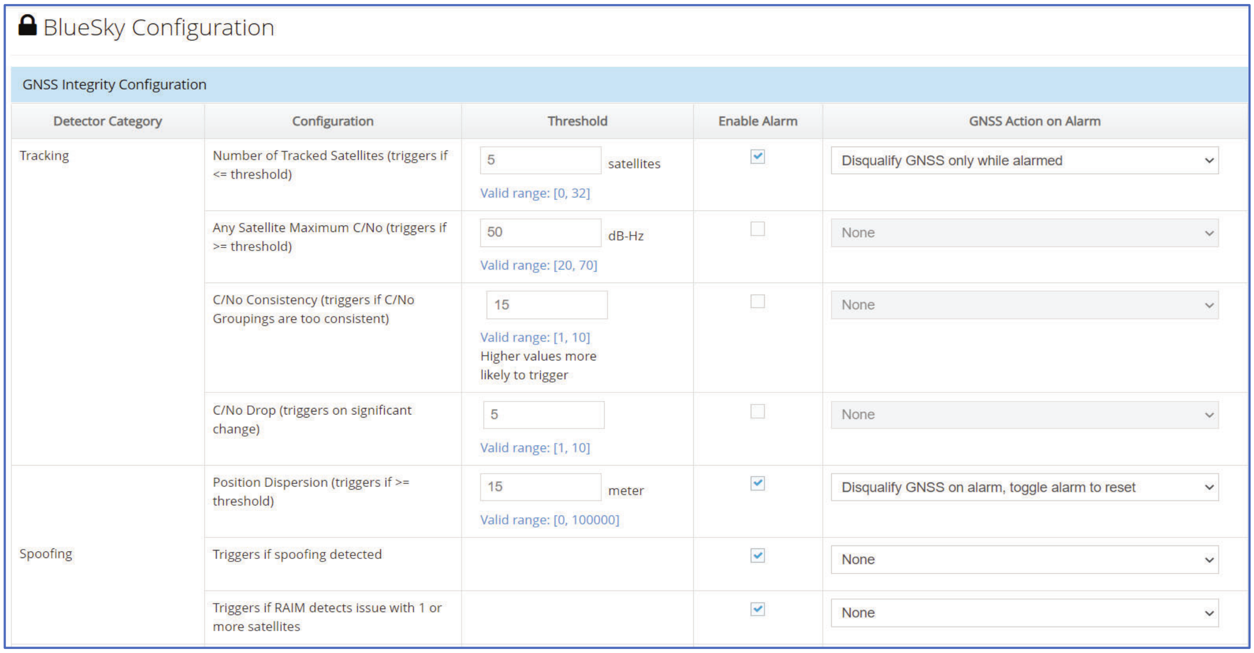
The use of the start/stop action control provides a way to initiate a new accumulation when desired (select stop, then start). Following are the specific functions for each column:

- 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 figure 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).

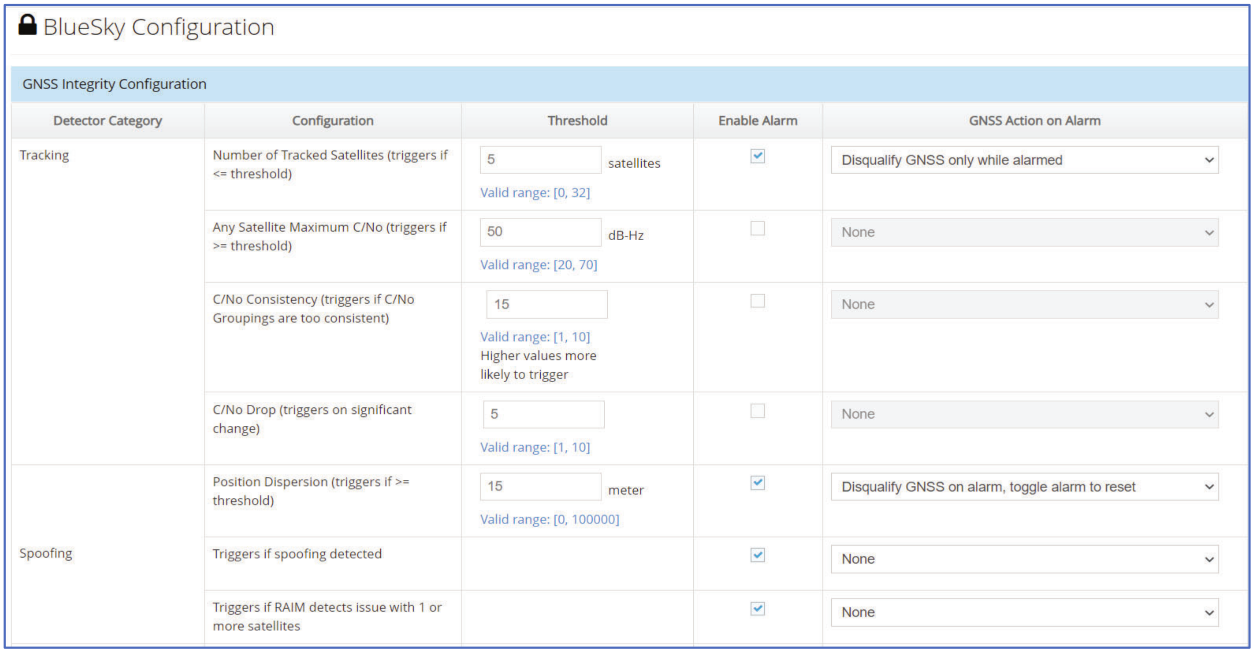
Figure 6-39. BlueSky Configuration Form



BlueSky Configuration

GNSS Integrity Configuration

Detector Category	Configuration	Threshold	Enable Alarm	GNSS Action on Alarm
Tracking	Number of Tracked Satellites (triggers if <= threshold)	5 satellites Valid range: [0, 32]	☑	Disqualify GNSS only while alarmed
	Any Satellite Maximum C/No (triggers if >= threshold)	50 dB-Hz Valid range: [20, 70]	□	None
	C/No Consistency (triggers if C/No Groupings are too consistent)	15 Valid range: [1, 10] Higher values more likely to trigger	□	None
	C/No Drop (triggers on significant change)	5 Valid range: [1, 10]	□	None
	Position Dispersion (triggers if >= threshold)	15 meter Valid range: [0, 100000]	☑	Disqualify GNSS on alarm, toggle alarm to reset
Spoofing	Triggers if spoofing detected		☑	None
	Triggers if RAIM detects issue with 1 or more satellites		☑	None



BlueSky Configuration

GNSS Integrity Configuration

Detector Category	Configuration	Threshold	Enable Alarm	GNSS Action on Alarm
Tracking	Number of Tracked Satellites (triggers if <= threshold)	5 satellites Valid range: [0, 32]	☑	Disqualify GNSS only while alarmed
	Any Satellite Maximum C/No (triggers if >= threshold)	50 dB-Hz Valid range: [20, 70]	☐	None
	C/No Consistency (triggers if C/No Groupings are too consistent)	15 Valid range: [1, 10] Higher values more likely to trigger	☐	None
	C/No Drop (triggers on significant change)	5 Valid range: [1, 10]	☐	None
Spoofing	Position Dispersion (triggers if >= threshold)	15 meter Valid range: [0, 100000]	☑	Disqualify GNSS on alarm, toggle alarm to reset
	Triggers if spoofing detected		☑	None
	Triggers if RAIM detects issue with 1 or more satellites		☑	None

6.14.5.1 Category Column

The **Category** column aggregates groups of detectors using the same categories shown in the summary form (Figure 6-38). As an example of use, if 1 or more of the detectors in the **Tracking** group is in an alarm state, it causes 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 Figure 6-38.

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 Figure 6-41, 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. The **Clear** condition is tracking count exceeds user-set threshold.

Following are the related items:

- Status form (Figure 6-41) provides current total GNSS tracking count. Field highlights red when set condition is met.
- Tracking count chart (Figure 6-45) provides tracking count history as a stacked-bar chart, partitioned by GNSS constellation. Chart also indicates current user-selected threshold.
- **Download** (Figure 6-45) allows download of tracking count history, partitioned by constellation.
- Tracking counts can also be seen on the Dashboard main section and Dashboard of GNSS.

6.14.5.2.2 Satellite Maximum C/No

This detector compares a user-set threshold vs. current GNSS Maximum C/No values from all tracked satellites. As shown in Figure 6-39, a user-entry is provided to set the threshold. The **set** condition occurs when the Maximum C/No value is equal to or greater than the user-set threshold. The **Clear** condition is Maximum C/No value less than user-set threshold.

Following are the related items:

- Status form (Figure 6-41) provides current Maximum C/No value. Field highlights red when set condition is met. Additionally, status form shows individual constellation maximum C/No values.
- Maximum C/No chart (Figure 6-51) provides maximum C/No history. Chart also indicates current user-selected threshold.
- **Download** (Figure 6-51) download provides overall maximum C/No history and individual constellation maximums.

6.14.5.2.3 Satellite C/No Consistency Check

The C/No consistency detector evaluates groupings of GNSS C/No values, looking for patterns that contain highly similar values. The motivation is that it is unusual for normal live sky C/No distributions to be this similar, so detections can be indicators of external signal manipulation.

There are four distinct groups continually evaluated, with each group using C/No values from all tracked satellites in that group as the basis for the evaluation. The groups are GPS, GLONASS, Galileo, and an aggregate group that combines all C/No values from these three constellations. Alarm messages identify the specific group that caused the detector to set/clear.

A sensitivity range control is provided on the configuration form (Figure 6-39) that adjusts the detection threshold for this detector. Higher values (10 is highest) increase the tendency to trigger by allowing detection of less consistent C/No data sets. Lower values (1 is lowest) decrease the tendency to trigger by restricting detection to more highly-consistent data sets.

Current status of this detector is provided on the status form (Figure 6-41). If there is no detection (of any group), then the box indicates "Ok". If any group is currently triggered, then the box indicates "Set". The detector might set and clear quickly, so it is not assured to be observed on the status form. To ensure notification of detection (and clearing), set the alarm checkbox for this detector and use appropriate alarm settings (`Admin->Alarms` form) to be notified as desired. For example, "Send Trap" or "Write Log" can be used to get notification.

6.14.5.2.4 Satellite C/No Drop Monitor

The C/No drop detector evaluates groupings of GNSS C/No values, looking for significant sudden reduction (including loss) of satellite C/No values. The motivation is that it is unusual for normal live sky C/No distributions to suddenly exhibit a high density of C/No drop, so detections may be indicators of external signal manipulation or possibly a marginal installation.

There are 4 distinct groups continually evaluated, with each group using C/No values from all tracked satellites in that group as the basis for the evaluation. The groups are GPS, GLONASS, Galileo, and an aggregate group that combines all C/No values from these 3 constellations. Alarm messages identify the specific group that caused the detector to set/clear.

A sensitivity range control is provided on the configuration form (Figure 6-39) that adjusts the detection threshold for this detector. Higher values (10 is highest) increase the tendency to trigger by allowing detection with datasets containing smaller amounts of C/No drop. Lower values (1 is lowest) decrease the tendency to trigger by restricting detection to datasets with larger amounts of C/No drop.

Current status of this detector is provided on the status form (Figure 6-41). When there is no detection (of any group) the box indicates "Ok". If any group is currently triggered the box indicates "Set". The detector might set and clear quickly, so it is not assured to be observed on the status form. To ensure notification of detection (and clearing), set the alarm checkbox for this detector and use appropriate alarm settings (`Admin->Alarms` form) to be notified as desired. For example, "Send Trap" or "Write Log" can be used to get notification.

6.14.5.3 Detector Details—Spoofing Category

This section describes the 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 and timing anomalies that might be introduced due to use of satellites that exhibit outlier behavior. As shown in Figure 6-39, 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. The **Clear** condition is current position dispersion less than user-set threshold.

Related items:

- Status form (Figure 6-41) provides current position dispersion value. Field highlights red when **set** condition is met.
- Position dispersion chart (Figure 6-49) provides position dispersion history. This chart also indicates current user-selected threshold.
- The **Download** (Figure 6-49) button provides position dispersion history.

6.14.5.3.2 Spoofing

This detector monitors for unusual changes in GNSS signals that might indicate external signal 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, as the only possible results are as shown in Table 6-39 along with the associated detector condition mapping.

6.14.5.3.3 Receiver Autonomous Integrity Monitor

Receiver Autonomous Integrity Monitor (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 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 might be “RAIMed out” (removed from use in solution). Usually, no action is needed with this detection since when it sets it means the outlier satellite(s) has been removed from solution and therefore is not impacting system timing.

There is no user-assignable detection threshold, as the only possible results are listed in the following table along with their detector mapping. Additional RAIM-related content is provided on status form (Figure 6-41).

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 and satellite-to-satellite) and illegal conditions (for example, out of range parameters).

As each rule evaluates to either FAIL (detector condition set) or PASS (detector condition clear), there are no user-configurable detection thresholds.

Notes:

- The Validator detector only evaluates GPS satellites and does not monitor satellite signals from other constellations.
- The BlueSky status form (Figure 6-41) provides current status for every validator anomaly rule. For details, see 6.14.9.8. 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 as GNSS).

6.14.7.1 Continuous Wave Jamming

This detector assesses strength of interfering continuous wave (CW) signals that might be present at the GNSS connection. CW interference closer to GNSS satellite RF center frequencies (not all are same) results in higher jamming values.

The CW jamming detector compares a user-set threshold vs. the current measured jamming percentage. As shown in Figure 6-39, a user-entry is provided to set the threshold. The **set** condition occurs when the current CW jamming percentage ≥ user-set threshold. The **Clear** condition is the current CW jamming percentage less than user-set threshold.

While normal jamming levels are site and installation-dependent, a typical jamming level for an install with no significant issues results in values < 10%. Observation of the history graph of this value might reveal periodic significant changes that can be an indication of periodic external RF events.

Notes:

- Status form (Figure 6-41) provides current CW jamming value. Field highlights red when set condition is met.
- CW Jamming chart (Figure 6-53) provides metric history. This chart also indicates current user-selected threshold.
- The **Download** (Figure 6-53) button provides the CW jamming history.

6.14.7.2 Broadband Interference

This detector responds to both CW and broadband interference. Unlike the CW jamming detector that provides a 0–100 percent measure, this detector provides states as listed in the following table. The **warning** state indicates that jamming is suspected, although there might not be a direct impact on satellite tracking capability. The **critical** state indicates a higher detection level and likely results in inability to use satellites for timing (can result in S6xx in the **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

6.14.7.3 Automatic Gain Control Check

The Automatic Gain Control (AGC) detector monitors the current value associated with the GNSS input. The value is provided as a percentage from 0%–100%. While a typical value is installation-dependent, a good installation should be in the 20%–60% range. Following are few general considerations related to this detector:

- If the signal path from antenna to GNSS input is more attenuated (for example, use of splitters, long cable runs, and so on), then this can increase the AGC value. It is not necessarily a problem if other indications of satellite tracking are good.
- If there is additive noise in the path this could tend to drive down the AGC value. For this case, it is likely that the CW jamming and/or broadband interference values will be elevated.
- Observation of the history graph of this value may reveal periodic significant changes that could be an indication of periodic external RF events

Two detector thresholds are provided. The detector sets if:

- The AGC value is at or above the high threshold, or
- At or below the low threshold.

Following is the list of related items:

- Status form (Figure 6-41) provides current AGC value. Field highlights red when the set condition is met.
- The AGC chart (Figure 6-55) shows AGC history. Chart also indicates the user-selected high and low thresholds.
- The Download button provides the AGC history.

6.14.8 Alarms and Associated Controls

Every detector row shown in Figure 6-39 provides an identical independent set of alarm-related controls. Therefore, while each detector has unique behavior, the control and response of alarms associated with detectors are all the same.

For reference, all alarms associated with the BlueSky functionality are shown in Figure 6-57, Figure 6-58, and Figure 6-59, as presented on the `Admin > Alarms form`. These figures show that the BlueSky alarms are not special alarms but are a foundational part of the generic alarm system for the 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, as shown in Figure 6-39 and details are covered in following sections.

Note:
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 the threshold that might currently exist (in some cases: user settable). The following section describes that an associated alarm is not automatically set because a detector is set.

6.14.8.1 Alarm Enable/Disable

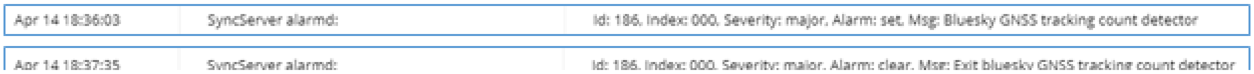
Every detector row in the Configuration form provides an alarm enable/disable checkbox for that detector. This adds a layer of alarm function that does not exist for other S6xx alarms, allowing “per detector” control of which ones can produce alarms. The functionality provided by the checkbox for a given detector is:

- When checked (and applied) the detector actually sets and clears alarms per the detector set/clear descriptions provided in the previous section.
- When unchecked, no actual alarms are produced by this detector. Additionally, if the alarm had been set at time of “uncheck” (and apply), the alarm clears (because it has been user-disabled).

For example, as shown in Figure 6-39, configuration format has the first-row detector (number of tracked satellites) alarm enabled and the second row detector (Max C/No) 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 C/No detector alarm is not.

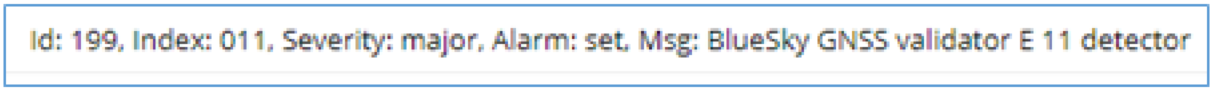
6.14.8.2 Specific Detector Alarms

Every detector has its own alarm, controlled by the enable/disable selection, as covered in previous section. The naming of these alarms can be seen in Figure 6-57, Figure 6-58, and Figure 6-59 taken directly from the generic alarm configuration form at `Admin > Alarms`. The following example shows the set and clear alarm indications for tracking count detector appearing in the message log (`Log > Messages`).



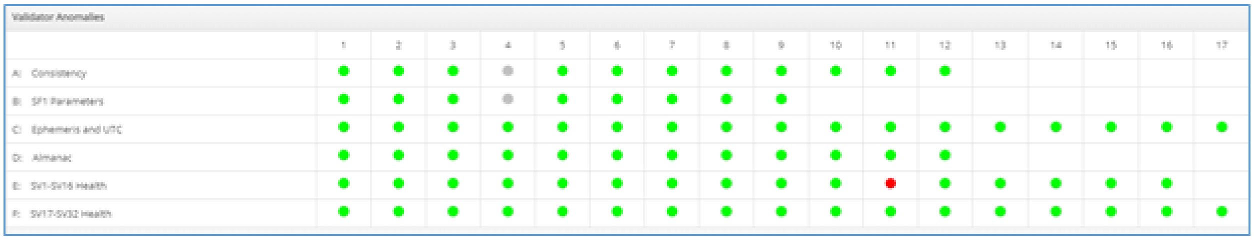
```
Apr 14 18:36:03        SyncServer alarmd:        Id: 186. Index: 000. Severity: major. Alarm: set. Msg: Bluesky GNSS tracking count detector
Apr 14 18:37:35        SyncServer alarmd:        Id: 186. Index: 000. Severity: major. Alarm: clear. Msg: Exit bluesky GNSS tracking count detector
```

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 6-39), each row contains many detectors, all of which are presented on the BlueSky status form (see Figure 6-41). The actual alarm reporting accommodates this by adding column content when identifying validator alarms. For example, the following figure 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 that the correspondence between alarm reporting and status form indication. In this case ,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 (as the E row has alarm enabled).



Validator Anomalies

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
A: Consistency	🟢	🟢	🟢	⚪	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢					
B: SF1 Parameters	🟢	🟢	🟢	⚪	🟢	🟢	🟢	🟢	🟢								
C: Ephemeris and UTC	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
D: Almanac	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢					
E: SV1-SV16 Health	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	
F: SV17-SV32 Health	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢

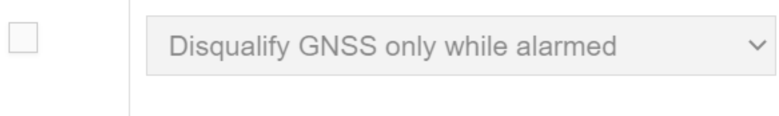
6.14.8.3 Use of Detector Alarms to Control GNSS Qualification Behavior

This section describes behaviors that are common to every BlueSky detector. The following list shows these behaviors at the high level:

- Alarms and behaviors covered here are only possible when the associated detector alarm is enabled (see 6.14.8.1. Alarm Enable/Disable).
- The controls covered here provide the ability to disqualify the use of GNSS as a source of synchronization for S6xx. This is a powerful capability. Therefore, these specific alarms are provided to inform when this becomes a reason for GNSS not being used.

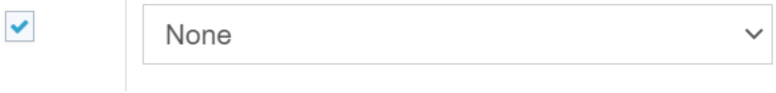
The control method is shown on Figure 6-39. The rightmost column titled **GNSS Action on Alarm** is a drop-down list that provides all of the needed control. Examples of each are shown in the following figures.

- 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 inactive indicating that it is not functional. The following example shows that the **alarm enable** option is not checked, so the advanced control (the subject of this section) is inactive (grayed out) as an indication that it is not functional and not selectable. Several examples are shown in Figure 6-39.



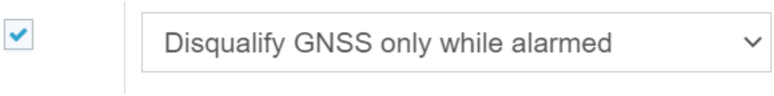
□ Disqualify GNSS only while alarmed

- Alarm enabled, list box is set to **none**. This is also a degenerate case for the advanced GNSS qualification behavior. With this setting the detector produces normal alarms but no GNSS action is taken when alarm is set. Several examples are shown in Figure 6-39.



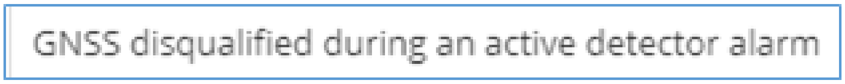
☑ None

- 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 (that is, it is cleared), this detector is not a reason for GNSS disqualification.



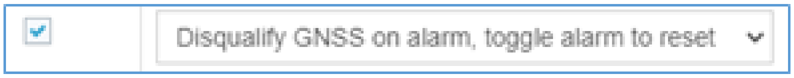
☑ Disqualify GNSS only while alarmed

The alarm associated with this reason for GNSS disqualification is shown and it sets and clears just like any other alarm.



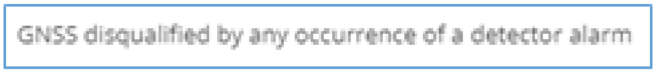
GNSS disqualified during an active detector alarm

- 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 when 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 must 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 re-qualify GNSS on its own. With this setting the user owns that action.



☑ Disqualify GNSS on alarm, toggle alarm to reset

The following figure shows the actual alarm that indicates that GNSS is disqualified due to this setting.



GNSS disqualified by any occurrence of a detector alarm

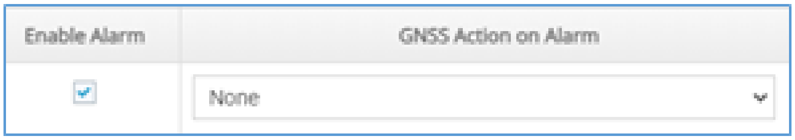
6.14.8.4 GNSS Disqualified Behavior with Multiple Detectors Alarmed

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 6-40 provides an abstract representation used for explanation. The left block is like the alarm portion of configuration form (see Figure 6-39) with the three narrow columns on right representing the enable alarm control and the other two 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 two 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.



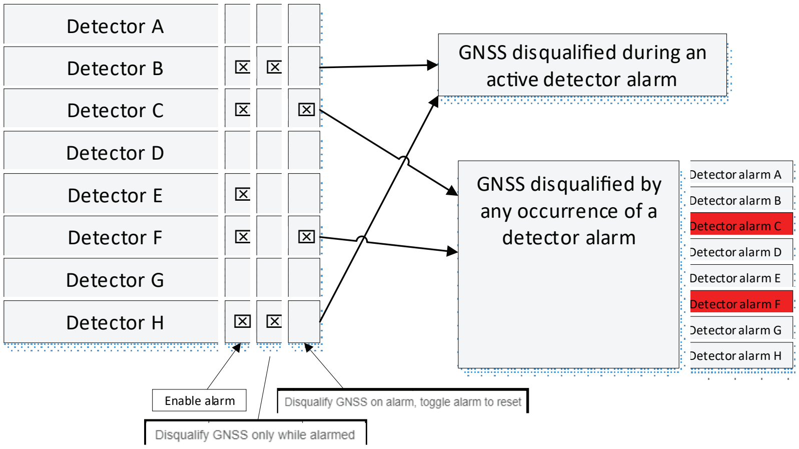
Enable Alarm	GNSS Action on Alarm
☑	None

- Detectors with X in **Enable alarm** and X in **Disqualify GNSS only while alarmed** drive their own detector alarm and also drive the **GNSS disqualified during an active detector** alarm when their detector alarm is set. As 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 the previous section).

  The **GNSS disqualified during an active detector** alarm is set (and results in GNSS being disqualified for use as a sync reference) when **any** detector connected to it is alarmed. This alarm is 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** drives their own detector alarm and ALSO drive the **GNSS disqualified by any occurrence of a detector** alarm when that base detector alarm is set. As 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).

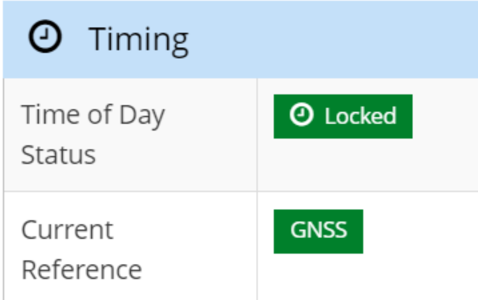
  The **GNSS disqualified by any occurrence of a detector** alarm is set (and result in GNSS being disqualified for use as a sync reference) when **any** detector connected to it becomes alarmed. As covered in the previous section, this alarm does not clear even if the underlying driving detector alarm clears.
  Note: 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 being set. This is needed because even if all the detectors that have caused this alarm to set have themselves become cleared, this alarm remains set. In that situation, you still need to know why this alarm is set; having the alarm report the sourcing detectors provides this information.

Figure 6-40. BlueSky Alarm Releationships



6.14.8.5 Example 1: Multiple Detectors Alarmed with Disqualify GNSS only While Alarmed Setting

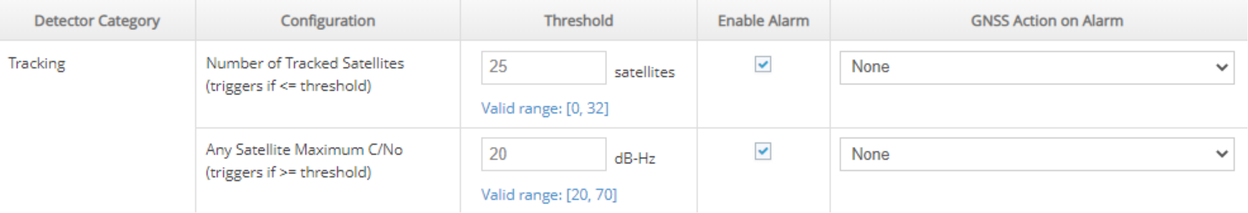
This scenario begins with S6xx locked to GNSS.



Timing

Time of Day Status	Locked
Current Reference	GNSS

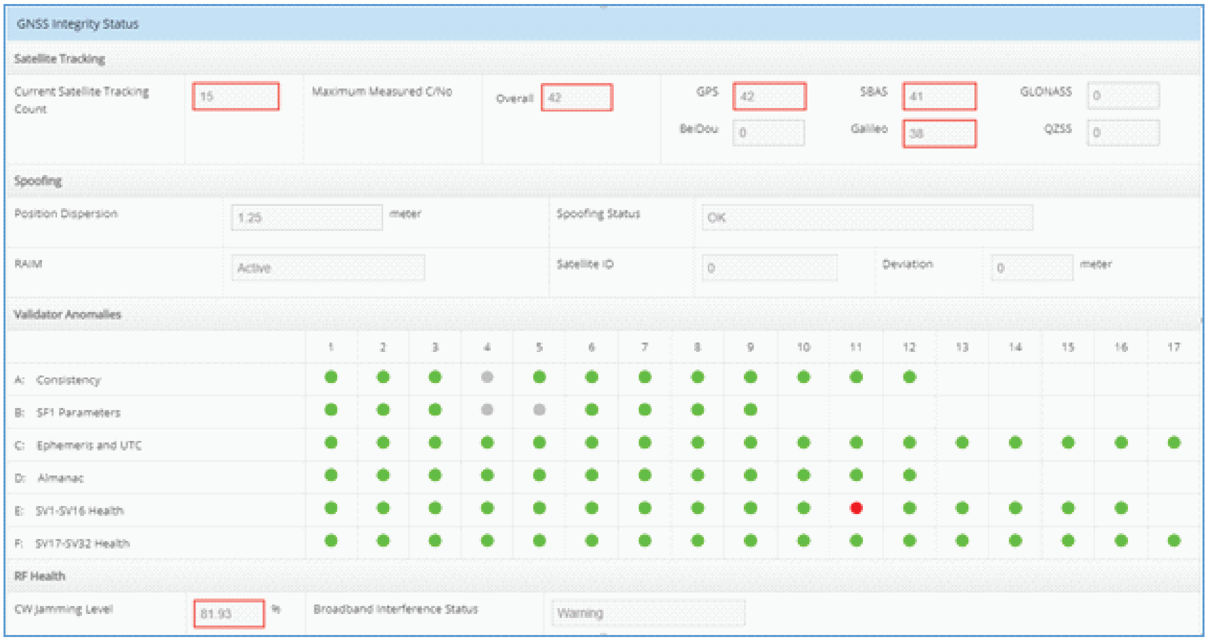
The following example figure shows the detectors that are used, as they are easy to trigger through configuration. To easily cause detectors to set, these thresholds are set to values that trigger the alarm under good operating conditions. Normal use for the detectors is to set the threshold to trigger on conditions of concern.



Detector Category	Configuration	Threshold	Enable Alarm	GNSS Action on Alarm
Tracking	Number of Tracked Satellites (triggers if <= threshold)	25 satellites Valid range: [0, 32]	☑	None
	Any Satellite Maximum C/No (triggers if >= threshold)	20 dB-Hz Valid range: [20, 70]	☑	None

These detectors are outlined in red:

- Tracked satellites detector shows it is set because 15 is less than 25 (configuration setting above)
- Max C/No detector shows it is set because three constellations are each having a maximum value above the threshold set (20).



GNSS Integrity Status

Satellite Tracking

Current Satellite Tracking Count: 15

Maximum Measured C/No: Overall 42; GPS 42; SBAS 41; GLONASS 0; BeiDou 0; Galileo 38; QZSS 0

Spoofing

Position Dispersion: 1.25 meter

Spoofing Status: OK

RAIM: Active

Satellite ID: 0

Deviation: 0 meter

Validator Anomalies

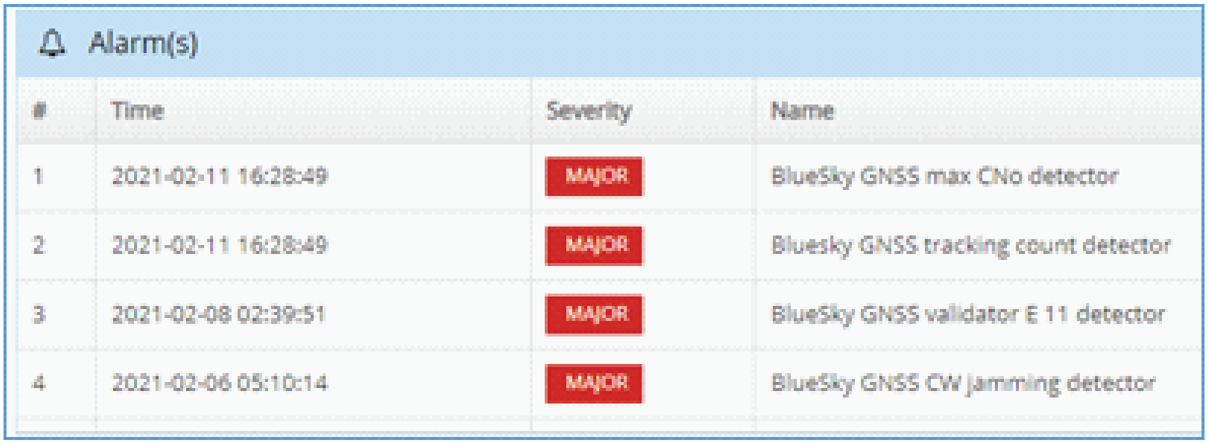
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
A: Consistency	🟢	🟢	🟢	⚪	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢					
B: SF1 Parameters	🟢	🟢	🟢	⚪	⚪	🟢	🟢	🟢	🟢								
C: Ephemeris and UTC	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
D: Almanac	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢					
E: SV1-SV16 Health	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	
F: SV17-SV32 Health	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢

RF Health

CW Jamming Level: 81.93 %

Broadband Interference Status: Warning

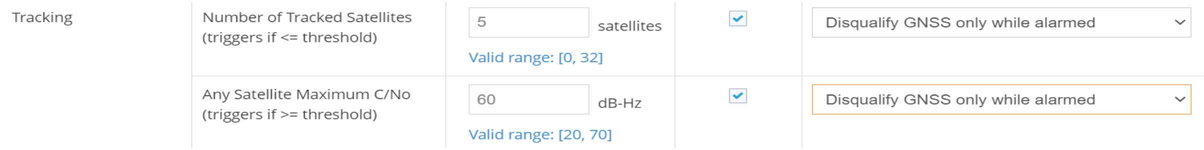
On `Dashboard > Alarms`, the indication that these detectors are actually generating alarms (associated alarm enable is set for each of them) can be seen. Here, they are all set to severity of Major, but that can be controlled on `Admin > Alarms`.



Alarm(s)

#	Time	Severity	Name
1	2021-02-11 16:28:49	MAJOR	BlueSky GNSS max CNo detector
2	2021-02-11 16:28:49	MAJOR	Bluesky GNSS tracking count detector
3	2021-02-08 02:39:51	MAJOR	BlueSky GNSS validator E 11 detector
4	2021-02-06 05:10:14	MAJOR	BlueSky GNSS CW jamming detector

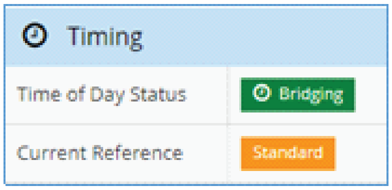
Add the **GNSS Action on Alarm** setting shown in the following figure for only these detectors. Recall that with this setting, if either of these detectors is actually alarmed (the detector must be set and configured with alarm enable for that to occur, as in the current case), then GNSS is disqualified from use as a sync reference. Only if both are not alarmed, then GNSS is allowed to try to qualify.



Tracking	Number of Tracked Satellites (triggers if <= threshold)	5 satellites Valid range: [0, 32]	☑	Disqualify GNSS only while alarmed
	Any Satellite Maximum C/No (triggers if >= threshold)	60 dB-Hz Valid range: [20, 70]	☑	Disqualify GNSS only while alarmed

In normal usage, the preceding 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 to show the incremental functionality of the controls.

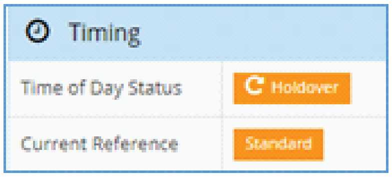
Upon configuring, this S6xx goes into Bridging because GNSS is no longer allowed to qualify.



Timing

Time of Day Status	Bridging
Current Reference	Standard

Later we end up in holdover, which is the normal progression on loss of reference.



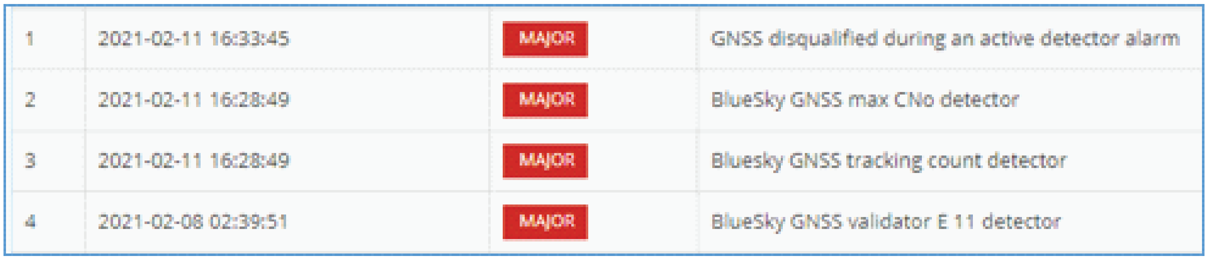
Timing

Time of Day Status	Holdover
Current Reference	Standard

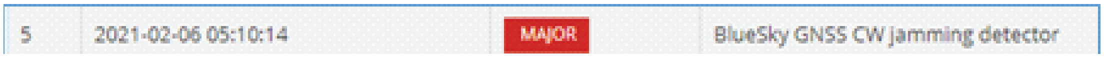
The following figure shows that we have the GNSS disqualified during an active detector alarm additionally set, allowing you to understand why S6xx is now in holdover.

Note: This alarm (unlike the next example) does not explicitly identify the detector alarm(s) that are causing it to be set because one or more currently set detector alarms are the reason. In this case, it is **Max C/No** and **tracking count**. If you are not sure which of these are driving it, 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. They have no impact on GNSS qualification.

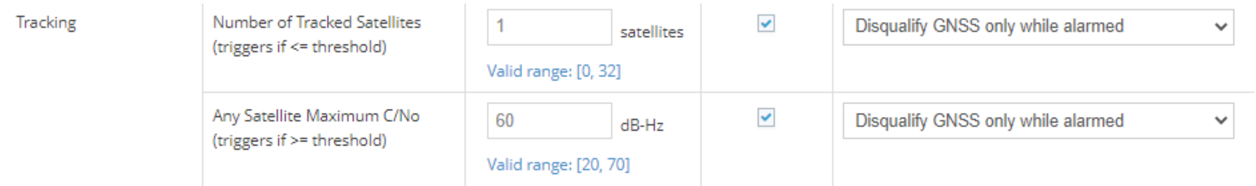


1	2021-02-11 16:33:45	MAJOR	GNSS disqualified during an active detector alarm
2	2021-02-11 16:28:49	MAJOR	BlueSky GNSS max CNo detector
3	2021-02-11 16:28:49	MAJOR	Bluesky GNSS tracking count detector
4	2021-02-08 02:39:51	MAJOR	BlueSky GNSS validator E 11 detector



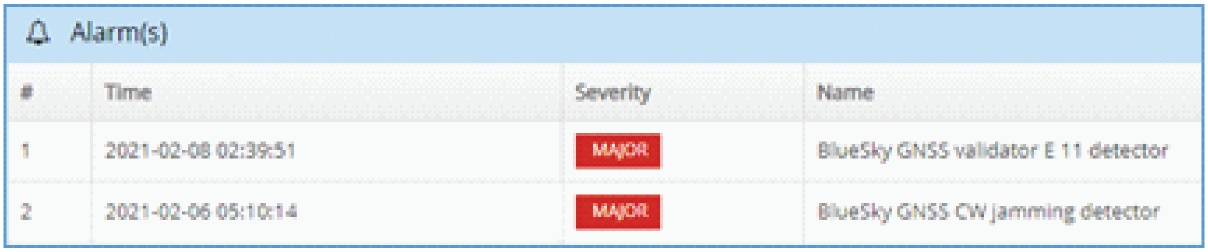
5	2021-02-06 05:10:14	MAJOR	BlueSky GNSS CW jamming detector

The thresholds for these detectors are changed so that the detector conditions are cleared. In real usage, this represents the underlying condition changing—it is not the normal use-case that the user changes the thresholds to make the alarm go away.



Tracking	Number of Tracked Satellites (triggers if <= threshold)	1 satellites Valid range: [0, 32]	☑	Disqualify GNSS only while alarmed
	Any Satellite Maximum C/No (triggers if >= threshold)	60 dB-Hz Valid range: [20, 70]	☑	Disqualify GNSS only while alarmed

In reaction to the preceding change, the remaining alarms are only for the other detectors. As both detectors associated with GNSS disqualification have cleared, the GNSS summary alarm has also gone away. S6xx proceeds to re-lock to GNSS, as the reason for not allowing GNSS for sync has been removed.

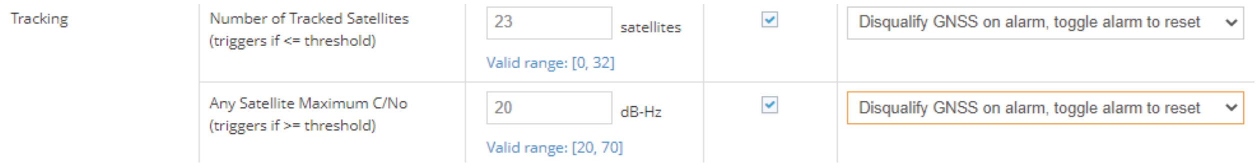


Alarm(s)

#	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

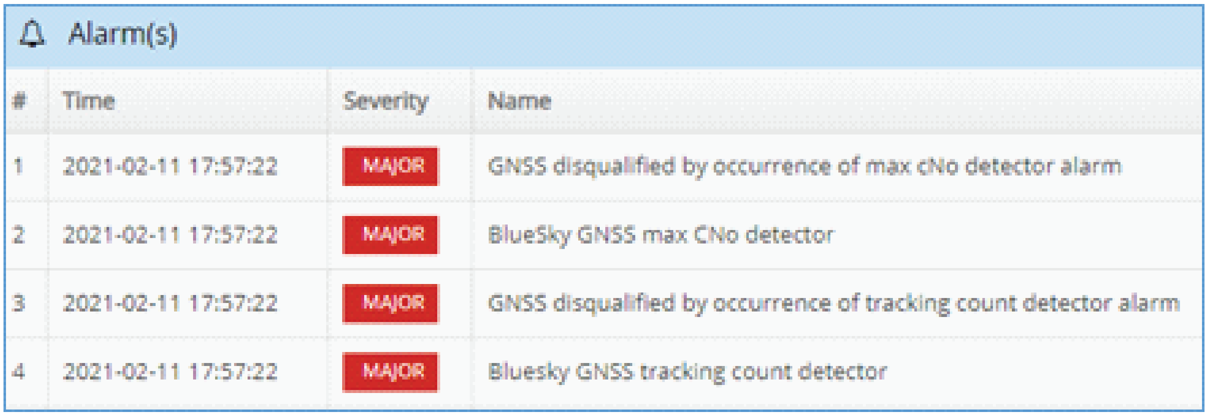
6.14.8.6 Example 2: Multiple Detectors Alarmed with Disqualify GNSS on Alarm, Toggle Alarm to Reset Setting

This is similar to the previous example, except now the other GNSS disqualification setting is used, as shown in the following figure. Once again, these detectors are set to values where both detector conditions will be set.



Tracking	Number of Tracked Satellites (triggers if <= threshold)	23 satellites Valid range: [0, 32]	☑	Disqualify GNSS on alarm, toggle alarm to reset
	Any Satellite Maximum C/No (triggers if >= threshold)	20 dB-Hz Valid range: [20, 70]	☑	Disqualify GNSS on alarm, toggle alarm to reset

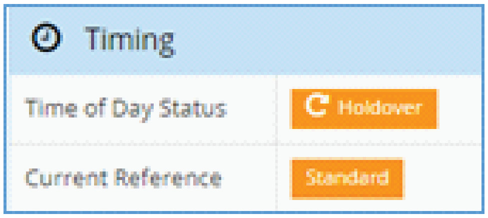
The following figure shows the resulting `Dashboard > Alarms`. Along with the individual detector alarms, each one has caused an independent disqualification alarm. They are both of the form: GNSS disqualified by occurrence, but each one explicitly names the specific detector that is causing it. This is needed because 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

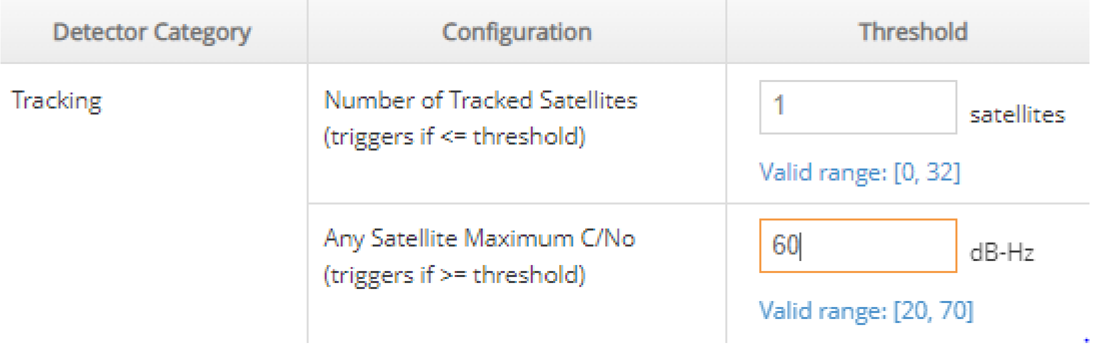
The following figure shows that the GNSS disqualification alarms cause S6xx to end up in holdover, as expected:



Timing

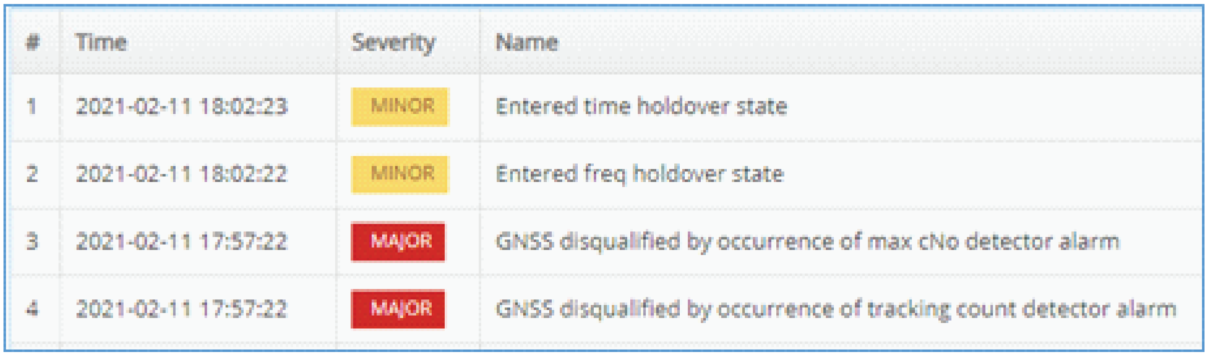
Time of Day Status	Holdover
Current Reference	Standard

Next, change thresholds so that the underlying detector conditions are cleared. The base detector alarms are also cleared.



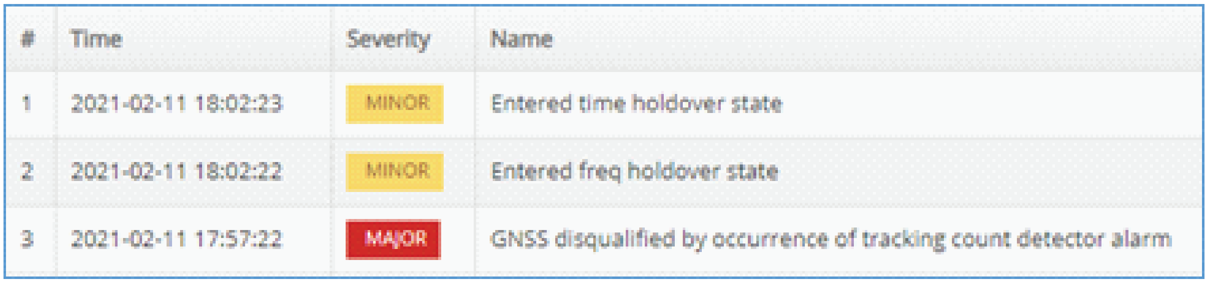
Detector Category	Configuration	Threshold
Tracking	Number of Tracked Satellites (triggers if <= threshold)	1 satellites Valid range: [0, 32]
	Any Satellite Maximum C/No (triggers if >= threshold)	60 dB-Hz Valid range: [20, 70]

In response, the base detector alarms are gone but the GNSS disqualification alarms remain as they must. These alarms do not clear unless the user toggles the base alarm OFF, and then ON. As these alarms 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 must have their alarms toggled.



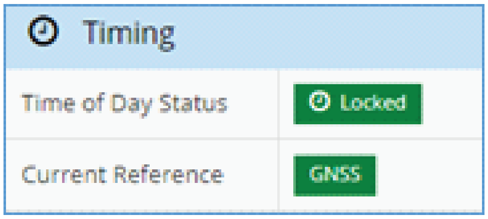
#	Time	Severity	Name
1	2021-02-11 18:02:23	MINOR	Entered time holdover state
2	2021-02-11 18:02:22	MINOR	Entered freq holdover state
3	2021-02-11 17:57:22	MAJOR	GNSS disqualified by occurrence of max cNo detector alarm
4	2021-02-11 17:57:22	MAJOR	GNSS disqualified by occurrence of tracking count detector alarm

Going to the configuration form, the alarm for **Max C/No** 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. It does not work if the underlying detector condition happens to still be set. As this action is only taken for Max C/No 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 preceding alarm also. This eventually leads to re-lock of GNSS, as there are no remaining GNSS disqualification alarms.



Timing

Time of Day Status	Locked
Current Reference	GNSS

6.14.8.7 Special Case Alarm Behavior

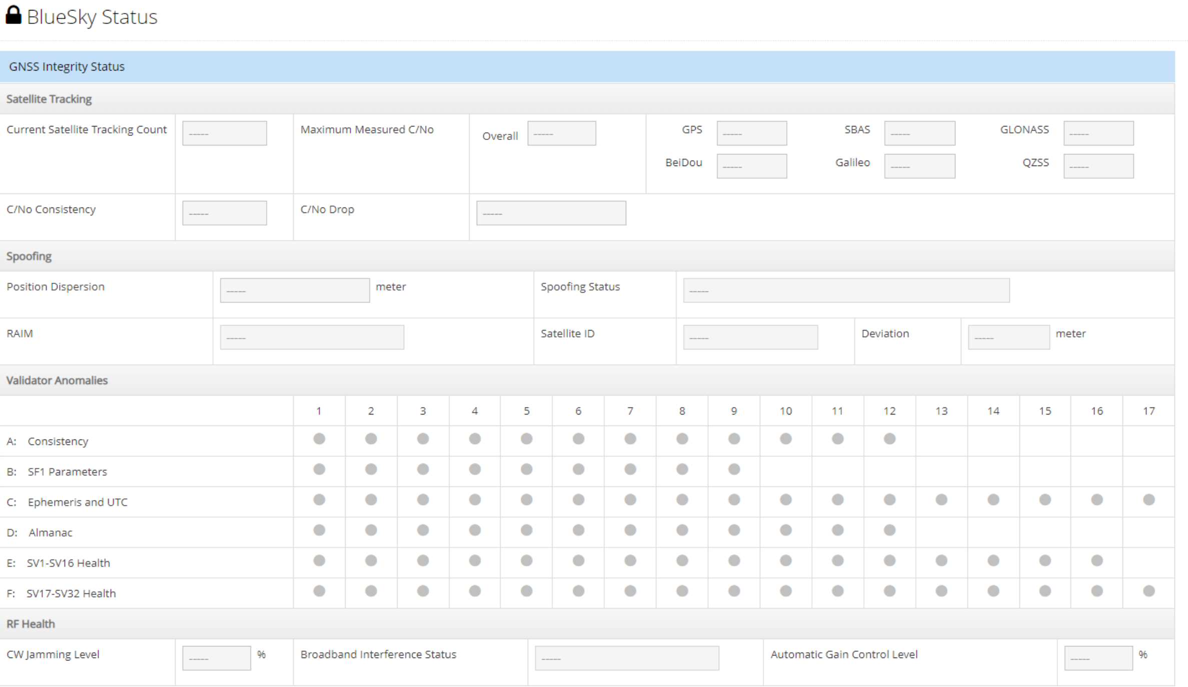
Athough the BlueSky alarms are fundamentally generic S6xx alarms, the following alarm-related behaviors are unique to these alarms due to their added unique controls:

- 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 6.14.8.3. Use of Detector Alarms to Control GNSS Qualification Behavior) is 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 is 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 6-41 shows the status form which provides live updates (most recent status) for all detectors. Following are the common characteristics of the form:

- All status results are lost if unit is rebooted/power-cycled. However, many of the charted results (see 6.15. Charts) can be saved to external storage.
- The four 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 in Figure 6-38, 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 (approximately five 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 6.14.4. Summary Form), the results in that group are appropriately indicated as unavailable. The following figure shows what status form looks like with all detector groups not running.



BlueSky Status

GNSS Integrity Status

Satellite Tracking

Current Satellite Tracking Count	------	Maximum Measured C/No	Overall	------	GPS	------	SBAS	------	GLONASS	------
					BeiDou	------	Galileo	------	QZSS	------
C/No Consistency	------	C/No Drop	------							

Spoofing

Position Dispersion	------ meter	Spoofing Status	------			
RAIM	------	Satellite ID	------	Deviation	------	meter

Validator Anomalies

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
A: Consistency	●	●	●	●	●	●	●	●	●	●	●	●					
B: SF1 Parameters	●	●	●	●	●	●	●	●	●								
C: Ephemeris and UTC	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
D: Almanac	●	●	●	●	●	●	●	●	●	●	●	●					
E: SV1-SV16 Health	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
F: SV17-SV32 Health	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

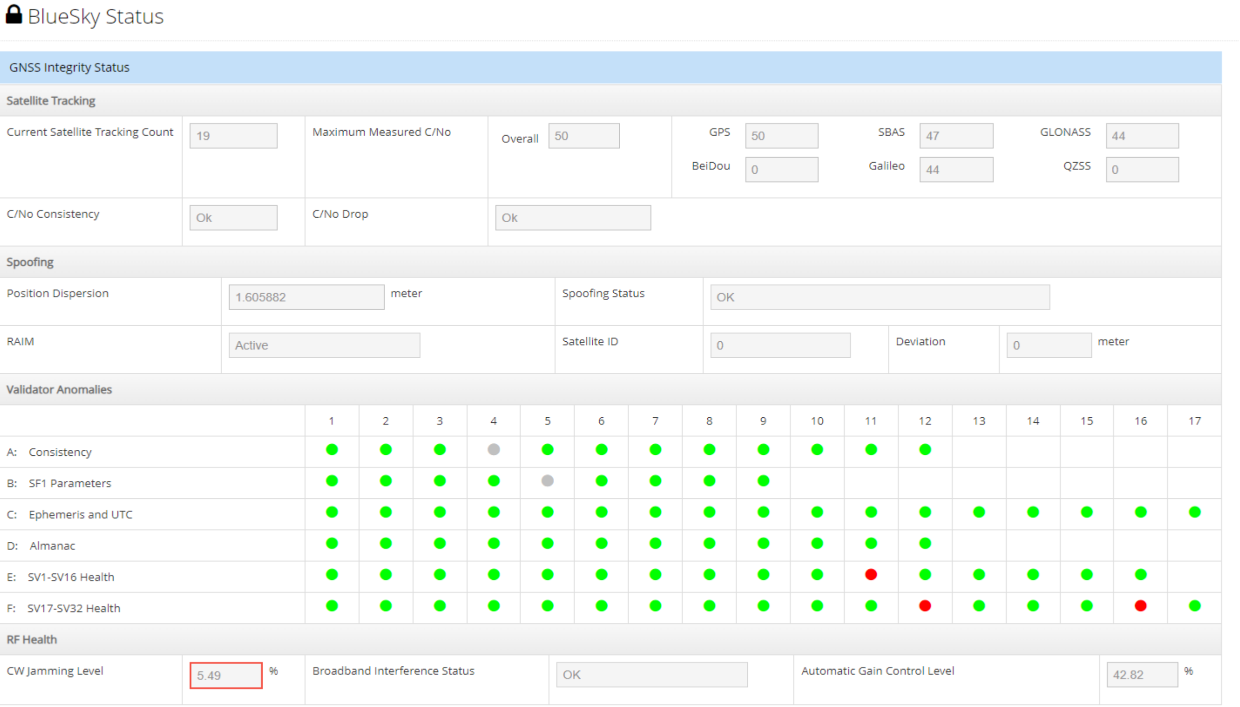
RF Health

CW Jamming Level	------ %	Broadband Interference Status	------	Automatic Gain Control Level	------ %

- Considering 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 is indicated on the status form, regardless of whether it is configured to generate alarms. The is the one place to always see detector **condition**. If a detector that is set propagates information beyond this form, depends upon the setting of the associated alarm enable/disable control (see Figure 6-39). When alarm is enabled, then the set condition drives all alarm-related behaviors. When the alarm is not enabled, the set condition becomes information-only content highlighted on the status form.

The following example figure shows the detectors that are currently set (does not necessarily mean alarmed). For the Validator Anomalies group, this condition is shown with a red dot and for all other detectors the value is outlined in red.

Figure 6-41. Example—BlueSky Status Form



BlueSky Status

GNSS Integrity Status

Satellite Tracking

Current Satellite Tracking Count	19	Maximum Measured C/No	Overall	50	GPS	50	SBAS	47	GLONASS	44			
					BeiDou	0	Galileo	44	QZSS	0			
C/No Consistency	Ok	C/No Drop	Ok										

Spoofing

Position Dispersion	1.605882 meter	Spoofing Status	OK			
RAIM	Active	Satellite ID	0	Deviation	0	meter

Validator Anomalies

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
A: Consistency	🟢	🟢	🟢	⚪	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢					
B: SF1 Parameters	🟢	🟢	🟢	🟢	⚪	🟢	🟢	🟢	🟢								
C: Ephemeris and UTC	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢
D: Almanac	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢					
E: SV1-SV16 Health	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	
F: SV17-SV32 Health	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🔴	🟢

RF Health

CW Jamming Level	5.49 %	Broadband Interference Status	OK	Automatic Gain Control Level	42.82 %

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 6-39) it is outlined in red.

Related items:

- Tracking count threshold can be set on configuration form (Figure 6-39).
- Tracking count chart (Figure 6-45) provides tracking count history as a stacked-bar chart, partitioned by GNSS constellation. This chart also indicates current user-selected threshold.
- **Save as** (Figure 6-45) allows download of tracking count history, partitioned by constellation.
- Tracking counts can also be seen on dashboard main section and `Dashboard -> GNSS`.

6.14.9.2 Satellite Maximum C/No Status

This detector shows the current overall highest C/No (Carrier-to-Noise Ratio) of all currently tracked satellites. When the value is equal to or greater than threshold configuration (see Figure 6-39), it is outlined in red.

Additional status showing C/No maximums for individual GNSS constellations is also provided.

Related items:

- C/No maximum threshold can be set on configuration form (Figure 6-39).
- Maximum C/No chart (Figure 6-51) provides maximum C/No history. Chart also indicates current user-selected threshold.
- Download (Figure 6-51) allows download of C/No maximum history, including partitions by constellation.

- Current C/No can also be seen on `Dashboard > GNSS` and the Current Sky View chart by hovering mouse over any satellite.

6.14.9.3 C/No Consistency Status

This detector looks for C/No values that are too consistent. Normally, live sky signals have significant variation, but a simulator-based spoofing attack might transmit signals with the same or very similar C/No levels. If the detector is set, the status field is outlined in red.

The status displays "Ok" if the detector is clear. The status displays "Set" if the detector is set. For more details about behavior of this detector, see 6.14.5.2.3. Satellite C/No Consistency Check.

6.14.9.4 C/No Drop Status

This detector monitors C/No signals for a drop-in level within a certain time window. The algorithm looks at the ratio of number of satellite signals that dropped compared to the total number of satellite signals present over the time window.

If the detector is set, then the status field is outlined in red.

The status displays "Ok" if the detector is clear. The status displays "Set" if the detector is set. For more details regarding behavior of this detector, see 6.14.5.2.4. Satellite C/No Drop Monitor.

6.14.9.5 Position Dispersion Status

This detector shows the current position dispersion value. This metric is used to detect erroneous position entries and timing anomalies that might be introduced due to tracking and use of satellites that exhibit outlier behavior. When the value is equal to or greater than user-set threshold (see Figure 6-39), it is outlined in red.

Following are the related items:

- Position dispersion threshold can be set on configuration form (Figure 6-39).
- Position dispersion chart (Figure 6-49) provides position dispersion history. Chart also indicates current user-selected threshold.
- **Download** (Figure 6-49) download provides position dispersion history.

6.14.9.6 Spoofing Status

Current status for the spoofing detector is next to title in the Spoofing group labeled as **Spoofing Status**. This detector monitors for unusual changes in GNSS signals that can 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 following table lists the possible status responses and relationship to detector set/clear. If the detector is set, then the status field is outlined in red.

Table 6-39. Possible Spoofing Detector Responses

Reported on Status Form	Detector Condition
Unknown	Clear
OK	Clear
Spoofing indicated	Set

6.14.9.7 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

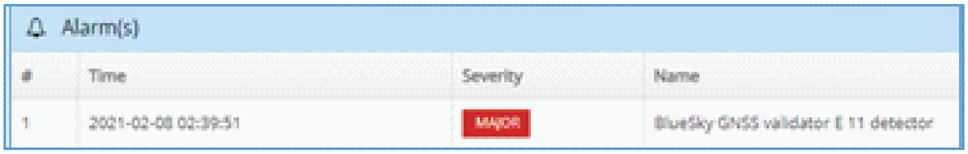
- The Satellite ID field provides the status used to set/clear this detector, as shown in Table 6-40. There are no user-definable detection thresholds. If there is more than one satellite being RAIMed, the ID indicates the one with the greatest bias. When the detector is set, this field is outlined in red.

6.14.9.8 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 6-41 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 6-41). Those controls apply to all of the rules (detectors) in that row. Key points:

- Each detector can produce 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.



Alarm(s)

#	Time	Severity	Name
1	2021-02-08 02:39:51	MAJOR	BlueSky GNSS validator E 11 detector

- The alarm and GNSS action control level for each detector is for the entire row associated with that detector. For this example, as E11 is generating an alarm, any detector in row E is capable of generating an alarm. Therefore, if the E5 and E7 detectors were also set then we would have 3 distinct alarms currently active.
- For the GNSS-action behavior (for more information, see 6.14.8.3. 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.

6.14.9.8.1 LED Behavior

The status shown for each rule has the following meanings:

- **Green Dot**: the most recent update of this rule found NO rule violation from any tracked GPS satellite. Also, there have been tracked GPS satellites within the timeout period (otherwise, this dot will 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 will be gray).
- **Gray Dot**: This rule has either:
  - Not ever run because the validator anomaly process (see Figure 6-38) was started, or
  - 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.

6.14.9.8.2 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.

6.14.9.9 Automatic Gain Control Status

This detector shows the current AGC value. When the value is equal to or outside the configured high and low thresholds, it is outlined in red.

Following is the list of related items:

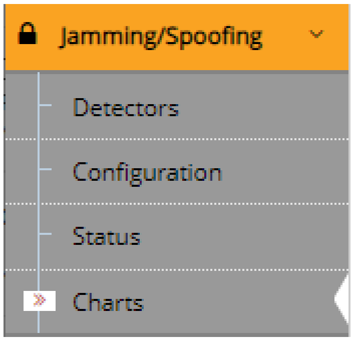
- AGC thresholds can be set on configuration form (Figure 6-39).
- AGC chart (Figure 6-55) provides AGC history. This chart also indicates current user-selected thresholds.
- **Download** (Figure 6-55) option allows download of tracking count history that is partitioned by constellation.

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 through the following navigation:



Once there, the following properties apply (see Figure 6-42 for description):

- A drop-down list box provides control of which chart can be viewed. Changing the selection directly brings up the selected chart.
- If data associated with the viewed chart can also be downloaded to external storage, a Download control is provided at bottom of form.
- For charts that support the Download control, 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

Following are the five charts that have the x-axis as time:

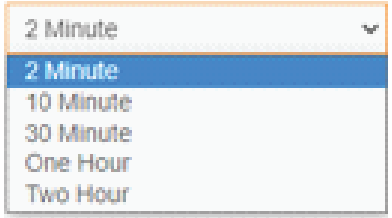
- Tracked Satellites
- Position Dispersion
- Maximum C/No
- CW Jamming
- Automatic Gain Control

Although 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 two 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 minutes) x (21600) = 43200 minutes = 30 days before it fills. Upon filling, all databases drop oldest data to incorporate newest data.
- All charts have user-configurable thresholds (see Figure 6-42) 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

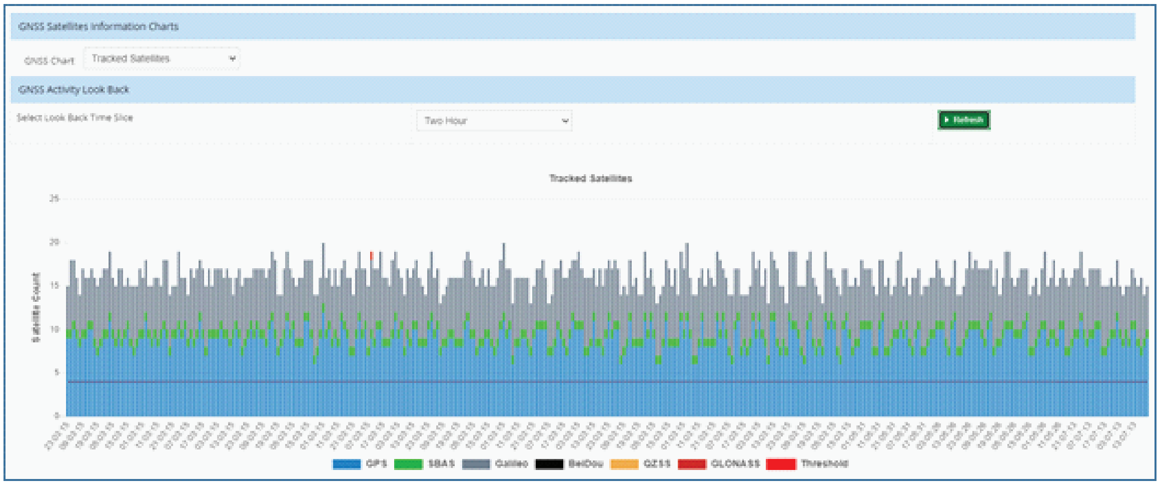
As these charts are supported by such large amounts of underlying data, zoom controls are provided with similar behavior on all of them. Figure 6-45 and Figure 6-42 are used here to help explain, both of which show tracked satellites charts but with the extreme ranges of zoom capability. The zoom control 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 following choices.



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 shows 5x more range than 2-minute interval, but only one out of every five samples are shown to accomplish this. The largest setting (2 hour) shows the entire 30 days of database range although this 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 cannot be shown for that zoom choice, the older data is not shown.

Figure 6-42. Example of Maximum X-Axis Time Range—Zoom Set to 2 Hours per Plotted Value



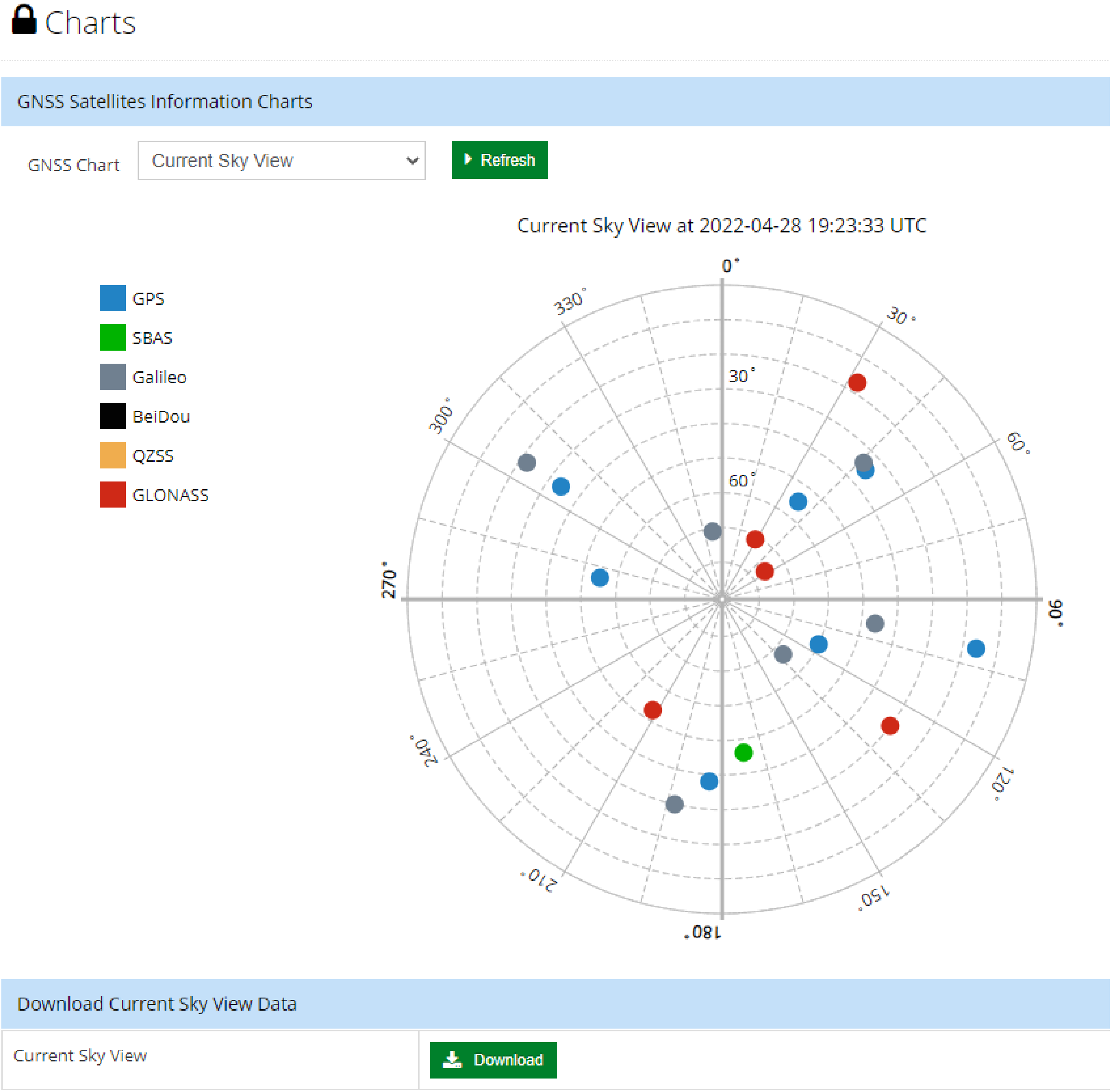
GNSS Chart: Tracked Satellites

Select Look Back Time Slice: Two Hour

6.15.3 Current Sky View Chart

The following figure shows an example.

Figure 6-43. Sky View Chart



Charts

GNSS Satellites Information Charts

GNSS Chart: Current Sky View

Download Current Sky View Data

Current Sky View

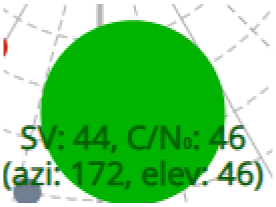
The polar plot provides a sky view of all satellites (colored dots) currently tracked by this S6xx unit.

- Distance from center is the elevation (in degrees) from horizon. Outer edge of circle is 0 degrees (that is, 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: The outer edge of circle has azimuth labels.

Constellations are color-coded per the legend at left of the chart. The example shows that GPS, SBAS, and Galileo are being tracked.

This chart does not self-update. To refresh the chart, select **Refresh**/**Exit and Return** or refresh the browser. The actual sampling rate for the chart is approximately every five minutes. Therefore, if the chart is refreshed, it does not mean that the new data will necessarily result from it.

Hovering the mouse over any satellite brings up detail on that satellites elevation, azimuth and Satellite Vehicle (SV) number and C/No. The following example shows that the satellite “bubble” enlarges and continues to match its original color. It also provides satellite vehicle number, C/No (of tracking), and details about the sky location.



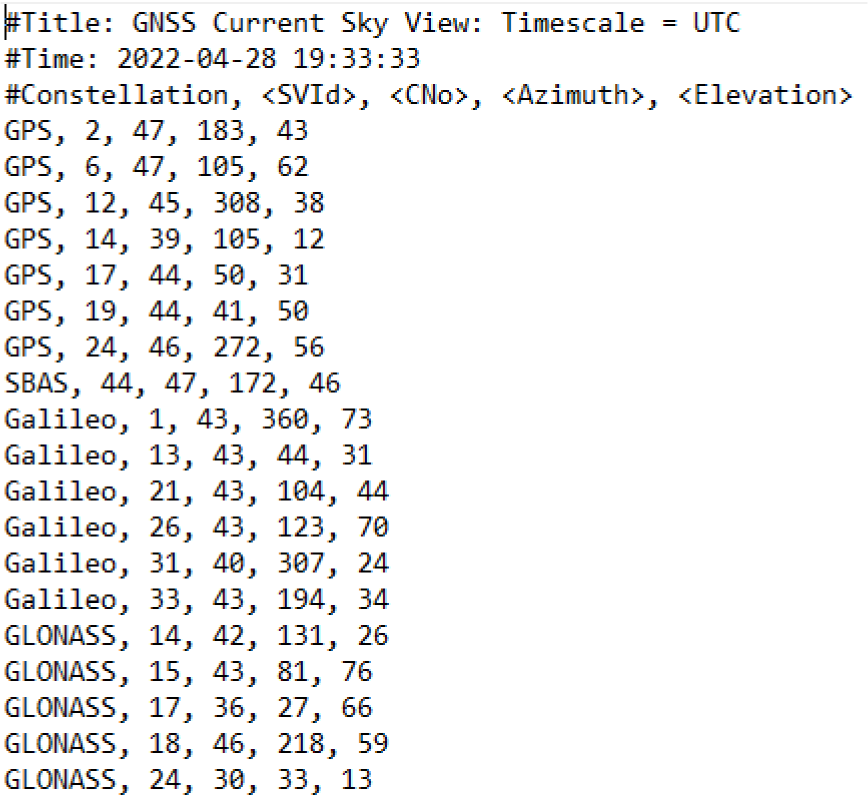
6.15.3.1 Sky View Download Format

The content of viewed chart can be externally saved using the **Download** control at bottom of the form. The format is nearly self-explanatory (see the following example). Following are the details:

- The three rows starting with # are informational
  - The first row provides a title for chart and identifies time information is UTC.
    Note: This is only true if S6xx has UTC time.
  - The second row provides the UTC time at which this data is collected.
  - The third row is a legend for the represented data. These are the same items that are identified in the chart detail description.
- The remainder is the data itself:
  - The first column names the associated constellation.
  - All the data is comma-separated.

The saved file is named: SyncServer_GNSS_Skyview.txt.

Figure 6-44. Example Sky View Download…

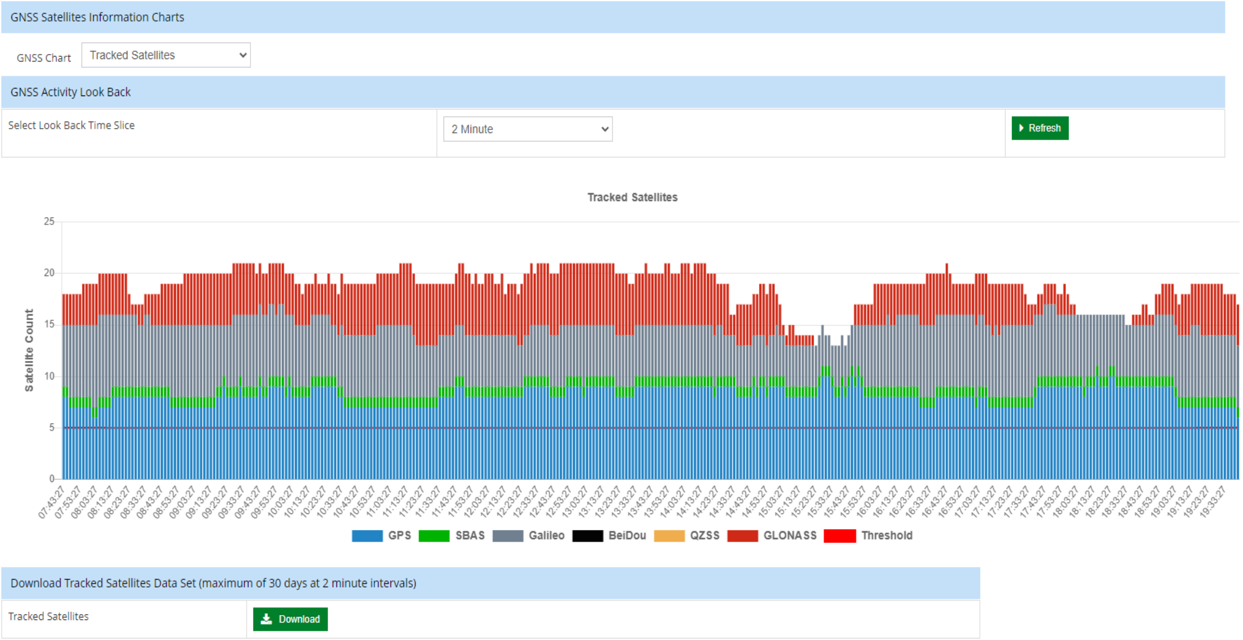


```
#Title: GNSS Current Sky View: Timescale = UTC
#Time: 2022-04-28 19:33:33
#Constellation, <SVId>, <CNo>, <Azimuth>, <Elevation>
GPS, 2, 47, 183, 43
GPS, 6, 47, 105, 62
GPS, 12, 45, 308, 38
GPS, 14, 39, 105, 12
GPS, 17, 44, 50, 31
GPS, 19, 44, 41, 50
GPS, 24, 46, 272, 56
SBAS, 44, 47, 172, 46
Galileo, 1, 43, 360, 73
Galileo, 13, 43, 44, 31
Galileo, 21, 43, 104, 44
Galileo, 26, 43, 123, 70
Galileo, 31, 40, 307, 24
Galileo, 33, 43, 194, 34
GLONASS, 14, 42, 131, 26
GLONASS, 15, 43, 81, 76
GLONASS, 17, 36, 27, 66
GLONASS, 18, 46, 218, 59
GLONASS, 24, 30, 33, 13
```

6.15.4 Tracked Satellites Chart

The following figure shows an example. The plot is a timeline (with **NOW** at current time) of history of tracked satellites. As with all plots that distinguish satellite constellations, they are color coded consistently, as per the legend shown in the following data.

Figure 6-45. Tracked Satellites Chart—2 Minute Interval per Data Value



GNSS Satellites Information Charts

GNSS Chart: Tracked Satellites

GNSS Activity Look Back

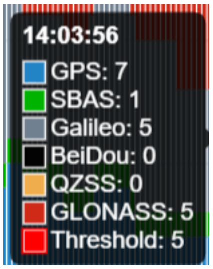
Select Look Back Time Slice: 2 Minute

Download Tracked Satellites Data Set (maximum of 30 days at 2 minute intervals)

Tracked Satellites

Each data column is a stacked bar that distinguishes all the constellations that are tracked at that time. More details for a given stacked bar can be seen by hovering the mouse over any portion of the chart. The top shows the x-axis time for the results.

Figure 6-46. Example



14:03:56

GPS: 7

SBAS: 1

Galileo: 5

BeiDou: 0

QZSS: 0

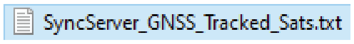
GLONASS: 5

Threshold: 5

This chart shares common behavioral attributes with all other "vs. time" charts. For more details, see 6.15.2. Common Attributes of Vs. Time Charts.

6.15.4.1 Tracked Satellites Download Format

Figure 6-45 shows that the tracked satellites data can be saved to external storage. The saved file is given a relevant name:



SyncServer_GNSS_Tracked_Sats.txt

Following is the first portion of the formatted output. The rows beginning with "#" are comments useful for chart labeling and/or description of the data meaning.

Notes:

- The sample points are two minutes apart (see 6.15.2. Common Attributes of Vs. Time Charts)
- Individual constellation tracking counts are provided with each sample
- A complete database results in 31,200 data rows

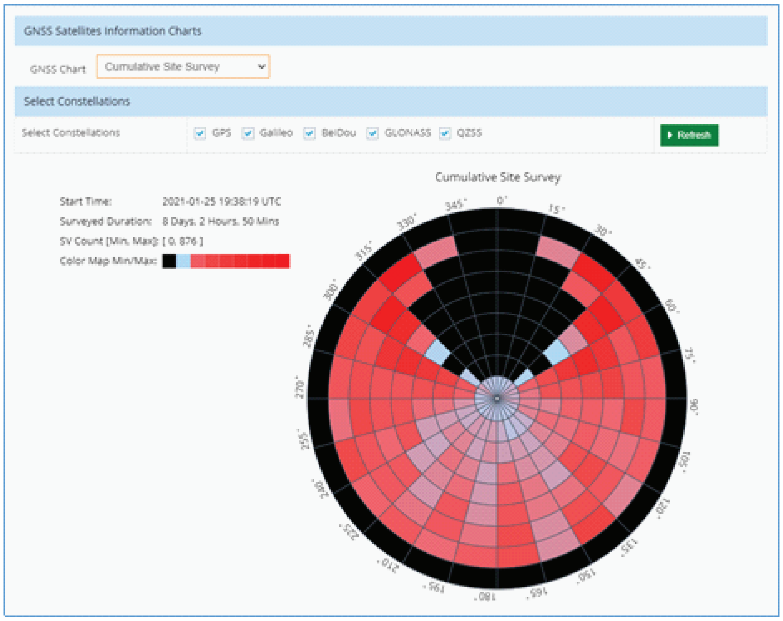
```
#Title: GNSS Tracked Satellites: Timescale = UTC
#UTC, <GPS tracked>, <SBAS tracked>, <Galileo tracked>, <BeiDou tracked>, <QZSS
```

```
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

As shown in the following figure, the primary purpose of this chart is to provide a large-sample assessment of how well the antenna placement is supporting actual tracking of satellites. The simple concept is to 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.

Figure 6-47. Cumulative Site Survey Chart (No Constellation Filter)



GNSS Satellites Information Charts

GNSS Chart: Cumulative Site Survey

Select Constellations

Select Constellations: ☑ GPS ☑ Galileo ☑ BeiDou ☑ GLONASS ☑ QZSS

Start Time: 2021-01-25 19:38:19 UTC
Surveyed Duration: 8 Days, 2 Hours, 50 Mins
SV Count [Min, Max]: [0, 876]
Color Map Min/Max: ■🟦🟥

There is only one other high-level control associated with this chart: start/stop of the accumulation process on the Detector summary form (Figure 6-38). 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.

Following are the fundamentals of the chart:

- 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 (that is, 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: 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. It allows detailed status for the selected grid to be observed.
- The update rate is about every five minutes, that is, approximately every five 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 (that is, while observing the chart, it does 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.

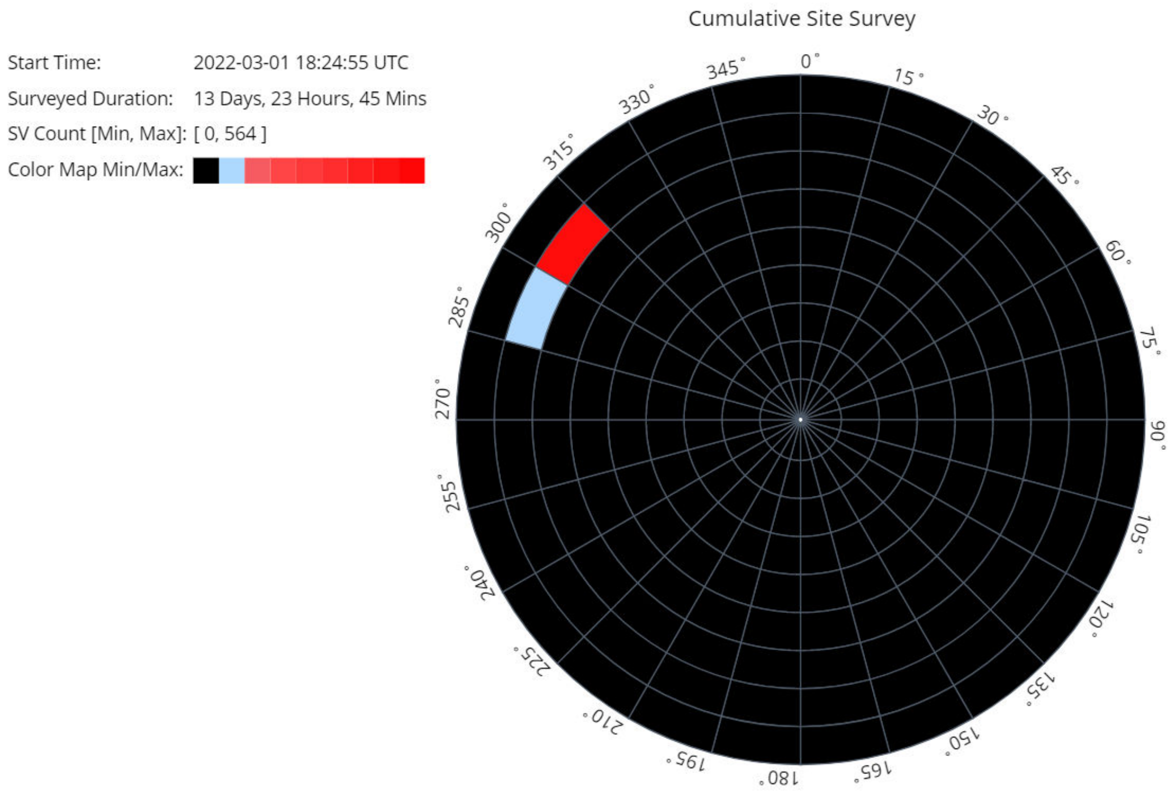
The chart can be useful for:

- 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.
- 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.
  Note: If a constellation is not configured (`References > GNSS` Config), then it has zero occurrences even if it is 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 and the underlying accumulation always accumulates all constellation data. The following figure shows how the chart in Figure 6-47 looks if it is restricted to only GLONASS satellites. As with all chart controls, the filter selection is not “remembered” if you exit this form and return later. It always enters with all constellations included.

Figure 6-48. Site Survey Chart with Filter Set to Only Display GLONASS



Start Time: 2022-03-01 18:24:55 UTC
Surveyed Duration: 13 Days, 23 Hours, 45 Mins
SV Count [Min, Max]: [0, 564]
Color Map Min/Max: ⬛🟦🟥🟥🟥🟥🟥🟥🟥

6.15.5.2 Left-Side Chart Information

The following list provides descriptions for the upper-left content of Cumulative Site Survey chart (Figure 6-47).

- **Start Time**: This field is set when the current cumulative site survey session is started.
- **Surveyed Duration**: This field shows how long the current survey has been running.
- **SV Count (Minimum, Maximum)**: This field shows the minimum and maximum accumulation of SV in all bins (there are 216 bins, that is, nine elevation zones x 24 azimuths = 216). In the example of Figure 6-47, 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 (Minimum, Maximum)**: This is the color legend for the graph:
  - No hits: Black
  - Very few hits: Light blue
  - Rest: Increasing intensity of reddish hues with maximum grid(s) as red

6.15.5.3 Chart Information

Color-coding in the example (Figure 6-47) shows the following:

- A large area to the north never tracks any satellites. This is due to its geographical location, and is not an installation issue.
- The 0 degree–10 degrees elevation black ring is due to the elevation mask being set to 10 degrees.

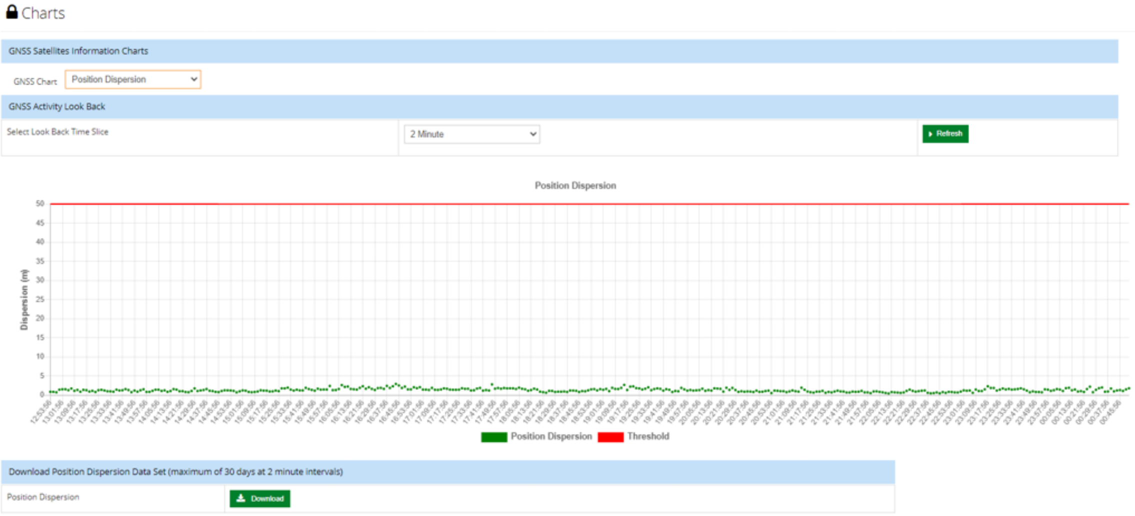
Details about each bin in the chart can be obtained by hovering over that bin via mouse. The grid that is referenced by the detailed data being shown is identified by the purple grid toward the bottom center portion of the chart (where the mouse was pointing when this chart was captured). As the mouse is moved, the associated grid shows this color along with the detail nearby. Following is a review of these details:

- **Top Row**: Identifies the location of the 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 is 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, the GPS updates this grid about nine 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 6.15.5.1. Select Constellations Row), the constellations that are not included by the filter show "-----".

6.15.6 Position Dispersion Chart

The following figure shows an example of the Position Dispersion chart. The plot has a timeline (x-axis, with **NOW** at far right) showing history of position dispersion (y-axis) values.

Figure 6-49. Position Dispersion Chart



Charts

GNSS Satellites Information Charts

GNSS Chart: Position Dispersion

GNSS Activity Look Back

Select Look Back Time Slice: 2 Minute

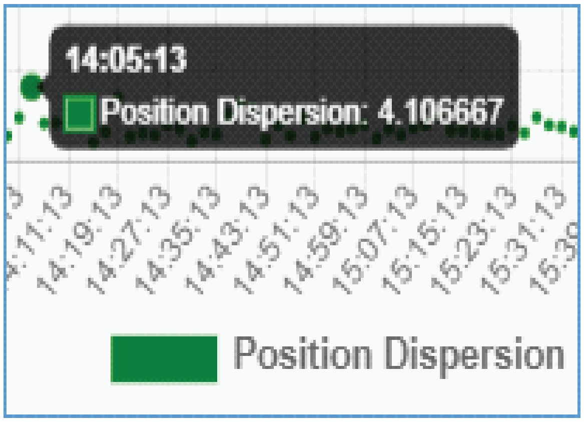
Download Position Dispersion Data Set (maximum of 30 days at 2 minute intervals)

Position Dispersion

Detail for any plotted dispersion result can be seen by hovering the mouse over appropriate portion of the chart, as shown in the following figure.

Note: The **cartoon** box points at and enhances the size of the data value being identified.

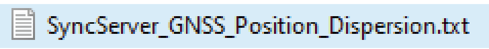
Figure 6-50. Example



This chart shares common behavioral attributes with all other Vs. Time charts. For more information, see 6.15.2. Common Attributes of Vs. Time Charts.

6.15.6.1 Position Dispersion Download Format

Figure 6-49 shows that the position dispersion data can be saved to external storage. The saved file is given a relevant name:

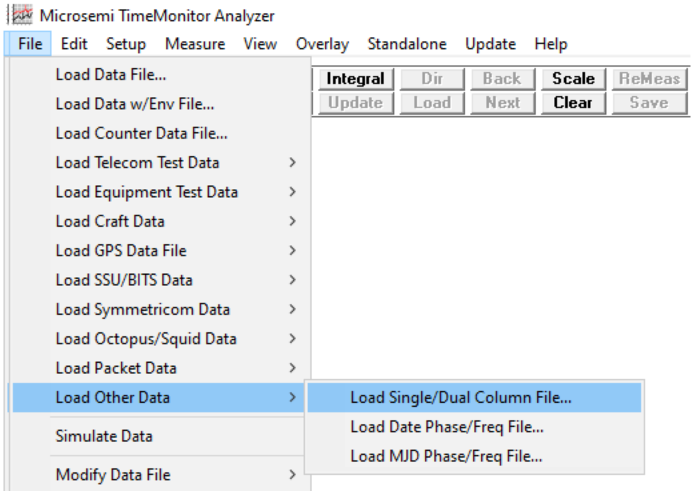

SyncServer_GNSS_Position_Dispersion.txt

Following is the first portion of formatted output. The rows beginning with “#” are comments useful for chart labeling and/or description of the data meaning.

- The sample points are two minutes apart
- The right-hand column is the dispersion value for the indicated time
- A full database results 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
```

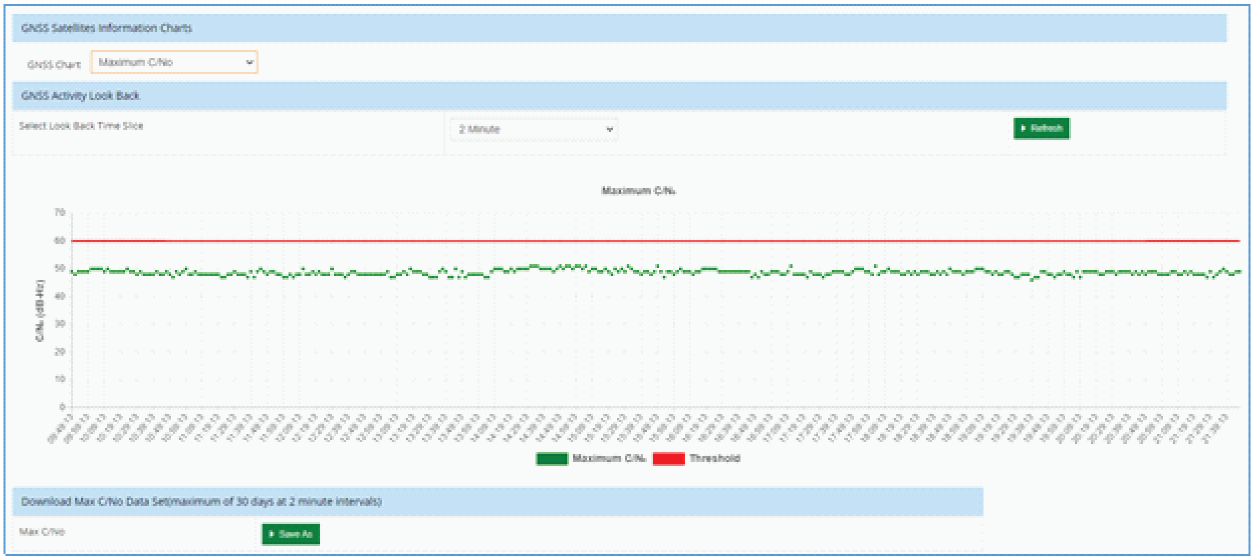
Microchip TimeMonitor Analyzer supports this format. Use the following selection:



6.15.7 Maximum C/No Chart

The following figure shows an example of Maximum C/No chart. The plot has a timeline (x-axis, with **NOW** at far right) showing history of maximum C/No (y-axis) values.

Figure 6-51. Maximum C/No Chart



GNSS Satellites Information Charts

GNSS Chart: Maximum C/No

GNSS Activity Look Back

Select Look Back Time Slice: 2 Minute

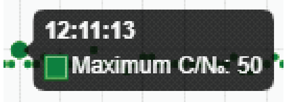
Download Max C/No Data Set(maximum of 30 days at 2 minute intervals)

Max C/No

Detail for any plotted maximum C/No result is seen by hovering the mouse over appropriate portion of the chart (example shown in Figure 6-52).

Note: The **cartoon** box points at and enhances the size of the data value being identified.

Figure 6-52. Example Mouse Hover



This chart shares common behavioral attributes with all other Vs. Time charts. For more information, see 6.15.2. Common Attributes of Vs. Time Charts.

6.15.7.1 Maximum C/No Download Format

Figure 6-51 shows that maximum C/No data can be saved to external storage. The saved file is given a relevant name: SyncServer_GNSS_Max_CNo.txt.

Following is the first portion of formatted output. The rows beginning with “#” are comments useful for chart labeling and/or description of the data meaning.

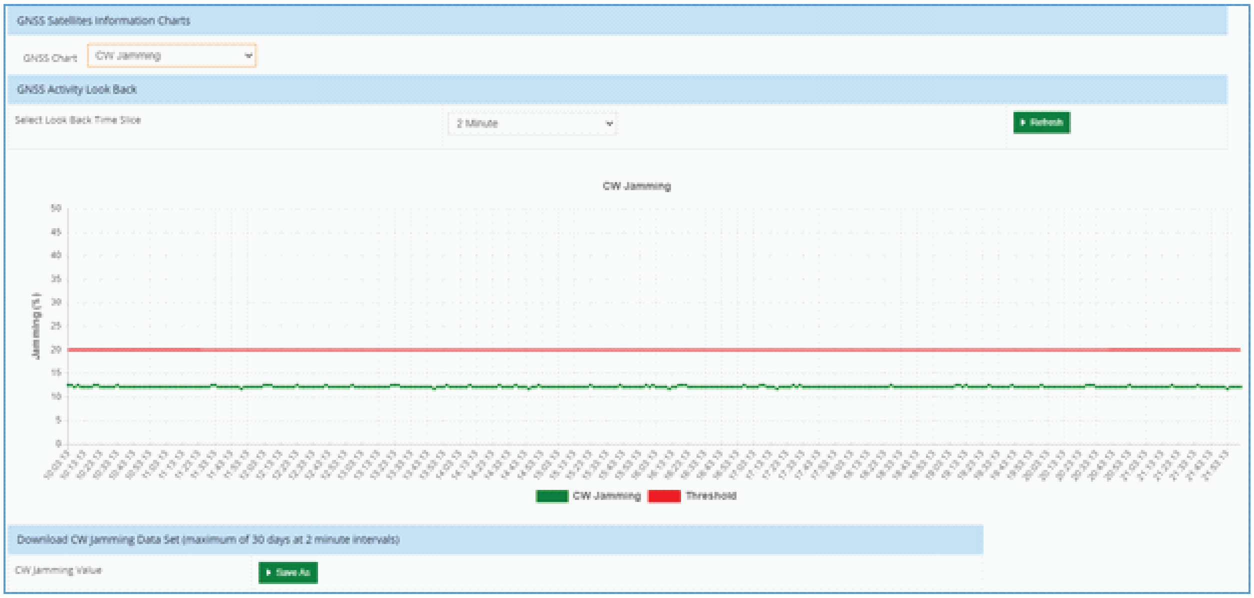
- The sample points are two minutes apart
- The left-most data column is the maximum C/No for all constellations from that sample. The remaining columns are the maximum C/No for all satellites from that specific constellation.
- A full database results in 31,200 data rows

```
#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

The following figure shows an example of the CW Jamming chart. The plot has a timeline (x-axis, with **NOW** at far right) shows history of CW Jamming (y-axis) values.

Figure 6-53. CW Jamming Chart



GNSS Satellites Information Charts

GNSS Chart: CW Jamming

GNSS Activity Look Back

Select Look Back Time Slice: 2 Minute

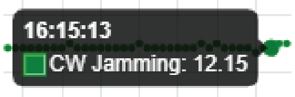
Download CW Jamming Data Set (maximum of 30 days at 2 minute intervals)

CW Jamming Value

Detail for any plotted CW Jamming result is seen by hovering the mouse over appropriate portion of the chart, as shown in the following figure.

Note: The **cartoon** box points at and enhances the size of the data value being identified.

Figure 6-54. Example mouse hover



This chart shares common behavioral attributes with all other Vs. Time charts. For more information, see 6.15.2. Common Attributes of Vs. Time Charts.

6.15.8.1 CW Jamming Download Format

Figure 6-53 shows that CW Jamming data can be saved to external storage. The saved file is given a relevant name:

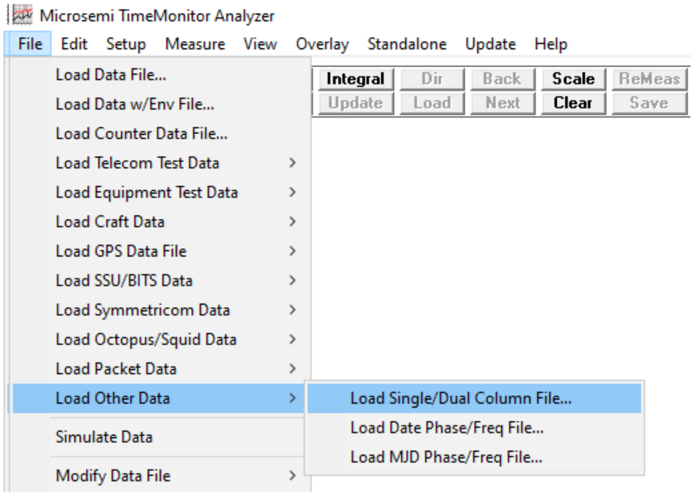
SyncServer_GNSS_CW_Jamming.txt

Following is the first portion of formatted output. The rows beginning with “#” are comments useful for chart labeling and/or description of the data meaning.

- The sample points are two minutes apart
- The right-hand column is the CW jamming value for the indicated time
- A full database results 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
```

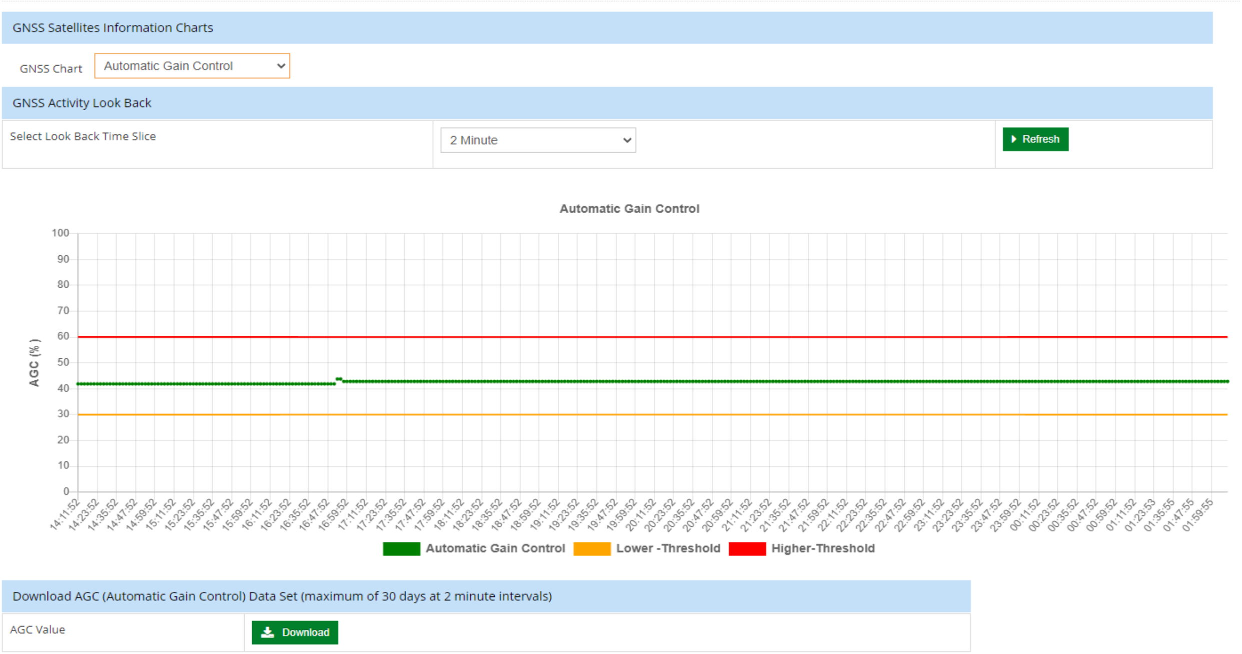
Microchip TimeMonitor Analyzer supports this format. Use the following selection:



6.15.9 Automatic Gain Control Chart

The following figure shows an example of the Automatic Gain Control chart. The plot has a timeline (x-axis, with **NOW** at far right) shows history of Automatic Gain Control (y-axis) values.

Figure 6-55. Automatic Gain Control Chart



GNSS Satellites Information Charts

GNSS Chart: Automatic Gain Control

GNSS Activity Look Back

Select Look Back Time Slice: 2 Minute

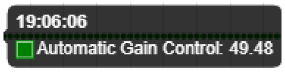
Download AGC (Automatic Gain Control) Data Set (maximum of 30 days at 2 minute intervals)

AGC Value

Detail for any plotted Automatic Gain Control result is seen by hovering the mouse over appropriate portion of the chart, as shown in the following figure.

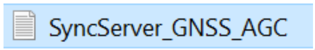
Note: The **cartoon** box points at and enhances the size of the data value being identified.

Figure 6-56. Example mouse hover



This chart shares common behavioral attributes with all other Vs. Time charts. For more information, see 6.15.2. Common Attributes of Vs. Time Charts.

6.15.9.1 Automatic Gain Control Download Format

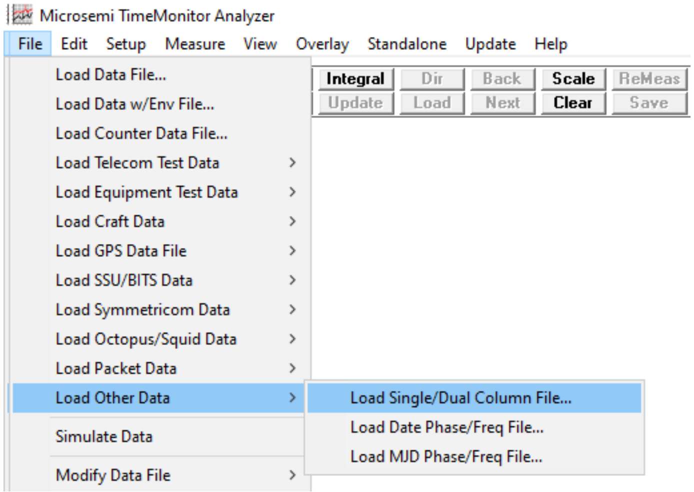
Figure 6-55 shows that the Automatic Gain Control data can be saved to external storage. The saved file is given a relevant name:  SyncServer_GNSS_AGC.

Following is the first portion of formatted output. The rows beginning with “#” are comments useful for chart labeling and/or description of the data meaning.

- The sample points are two minutes apart
- The right-hand column is the CW jamming value for the indicated time
- A full database results in 31,200 data rows

```
#Title: Automatic Gain Control (AGC): Timescale = UTC
#UTC, <AGC>
2022-02-22,16:36:06, 48.529999
2022-02-22,16:38:06, 48.529999
2022-02-22,16:40:06, 48.529999
2022-02-22,16:42:06, 48.529999
2022-02-22,16:44:06, 48.529999
2022-02-22,16:46:06, 48.529999
2022-02-22,16:48:06, 48.529999
2022-02-22,16:50:06, 48.529999
```

Microchip TimeMonitor Analyzer supports this format. Use the following selection:

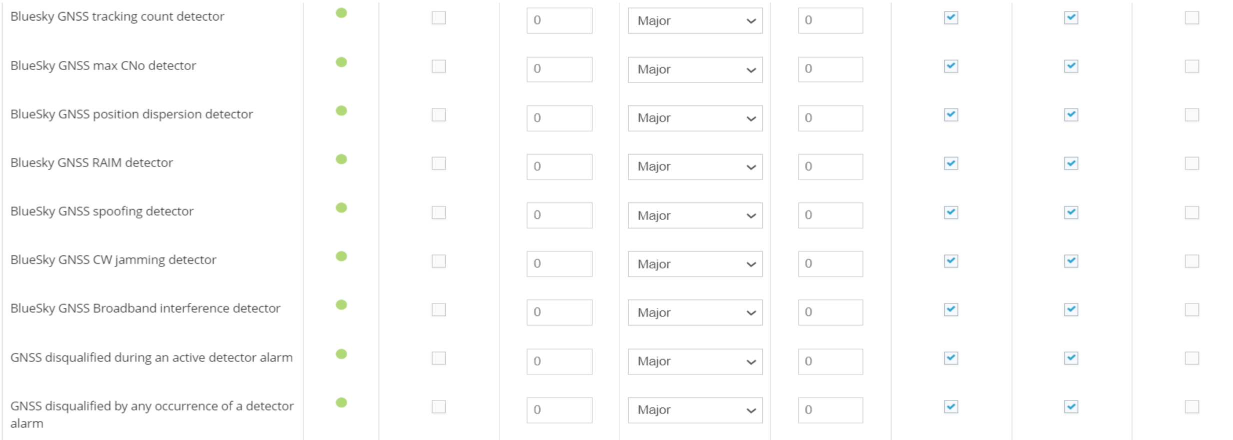


6.16 BlueSky Alarms

This section describes the alarms that are directly associated with BlueSky capabilities. The following figures show all the BlueSky alarms. These figures are directly taken from the `Admin > Alarms` form. This makes the crucial 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.

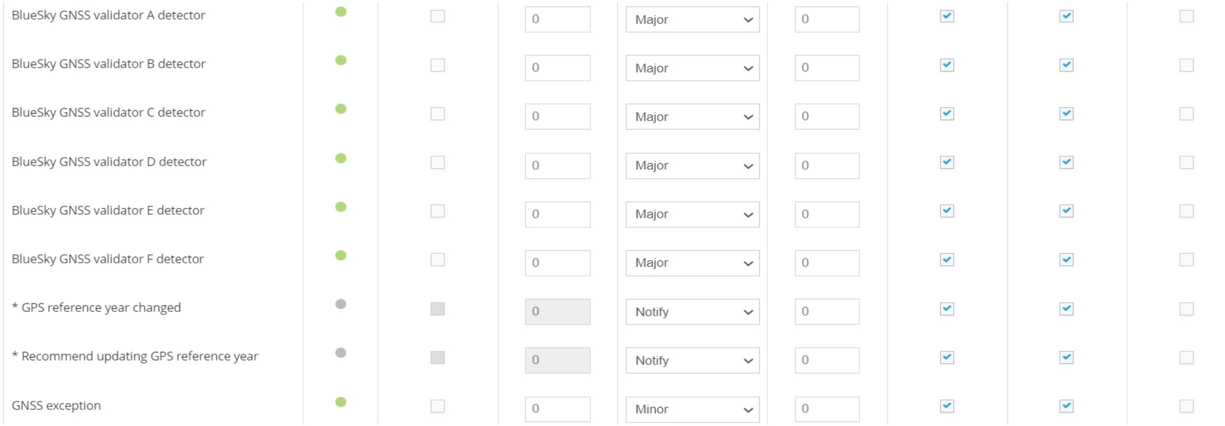
For more information about BlueSky-unique controls associated with these alarms, see 6.14.8. Alarms and Associated Controls.

Figure 6-57. BlueSky Alarms—Part 1



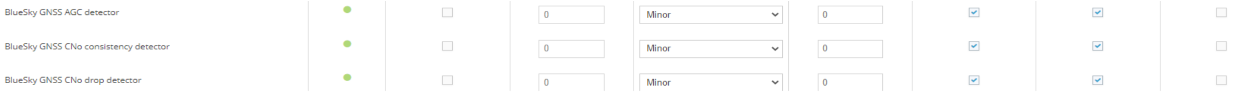
Bluesky GNSS tracking count detector	●	☐	0	Major	0	☑	☑	☐
BlueSky GNSS max CNo detector	●	☐	0	Major	0	☑	☑	☐
BlueSky GNSS position dispersion detector	●	☐	0	Major	0	☑	☑	☐
Bluesky GNSS RAIM detector	●	☐	0	Major	0	☑	☑	☐
BlueSky GNSS spoofing detector	●	☐	0	Major	0	☑	☑	☐
BlueSky GNSS CW jamming detector	●	☐	0	Major	0	☑	☑	☐
BlueSky GNSS Broadband interference detector	●	☐	0	Major	0	☑	☑	☐
GNSS disqualified during an active detector alarm	●	☐	0	Major	0	☑	☑	☐
GNSS disqualified by any occurrence of a detector alarm	●	☐	0	Major	0	☑	☑	☐

Figure 6-58. BlueSky Alarms—Part 2



BlueSky GNSS validator A detector	●	☐	0	Major	0	☑	☑	☐
BlueSky GNSS validator B detector	●	☐	0	Major	0	☑	☑	☐
BlueSky GNSS validator C detector	●	☐	0	Major	0	☑	☑	☐
BlueSky GNSS validator D detector	●	☐	0	Major	0	☑	☑	☐
BlueSky GNSS validator E detector	●	☐	0	Major	0	☑	☑	☐
BlueSky GNSS validator F detector	●	☐	0	Major	0	☑	☑	☐
* GPS reference year changed	●	☐	0	Notify	0	☑	☑	☐
* Recommend updating GPS reference year	●	☐	0	Notify	0	☑	☑	☐
GNSS exception	●	☐	0	Minor	0	☑	☑	☐

Figure 6-59. BlueSky Alarms—Part 3



BlueSky GNSS AGC detector	●	☐	0	Minor	0	☑	☑	☐
BlueSky GNSS CNo consistency detector	●	☐	0	Minor	0	☑	☑	☐
BlueSky GNSS CNo drop detector	●	☐	0	Minor	0	☑	☑	☐

7. Maintenance and Troubleshooting

This section describes maintenance, safety, troubleshooting, repairing, and part number details of the SyncServer device.

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 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 be very helpful in troubleshooting SyncServer S6x0. Use the Alarms page of the Web GUI to view system messages or use SNMP trap messages.

Note: 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 reports an event in the event log (add the actual event here), and the system reboots.

7.4.1 Diagnosing SyncServer S6x0—Reading LED Conditions

The following table lists functions of the LED indicators on the front panel of the unit and the 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	NETWORK	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 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 SyncServer S6x0

SyncServer S6x0 cannot be repaired in the field. There are no field-serviceable fuses in 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 SyncServer S6x0’s web interface and software available from Microchip. When 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. See the following section 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 resets 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 prior to putting the shelf into service.

⚠ CAUTION

To avoid a possible service call, do not issue a command to SyncServer S6x0 during an upgrade and do not remove power from SyncServer S6x0 during an upgrade. Doing so can corrupt the flash memory, disabling SyncServer S6x0.

7.6.1 SyncServer S6x0 Upgrade

The upgrade process is simple, but there is Loss of Service (LOS) at reboot. The upgrade takes approximately seven minutes to complete. The upgrade process requires an authorization file to proceed. This file verifies that the SyncServer unit is authorized to upgrade the selected upgrade file.

SyncServer 6x0 does not contain a battery-backed real-time clock. Therefore, it always boots up with a default value for the system time. This time is 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 is used for the first log entries when booting up the unit. The time changes 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

Notes:

- 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.
- If “upgrading” from revision 2.0 or higher to an older revision, then the system sets configuration to factory default values.
- Configuration changes made after the upgrade but before the reboot will not be available after the reboot.
- 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 uploads are very slow and might 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

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

Item	Part Number
S650 Quickship Models	
SyncServer S650+Timing I/O Module	090-15200-651
SyncServer S650+Timing I/O Module + Rubidium	090-15200-652
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 Server 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
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 Server 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

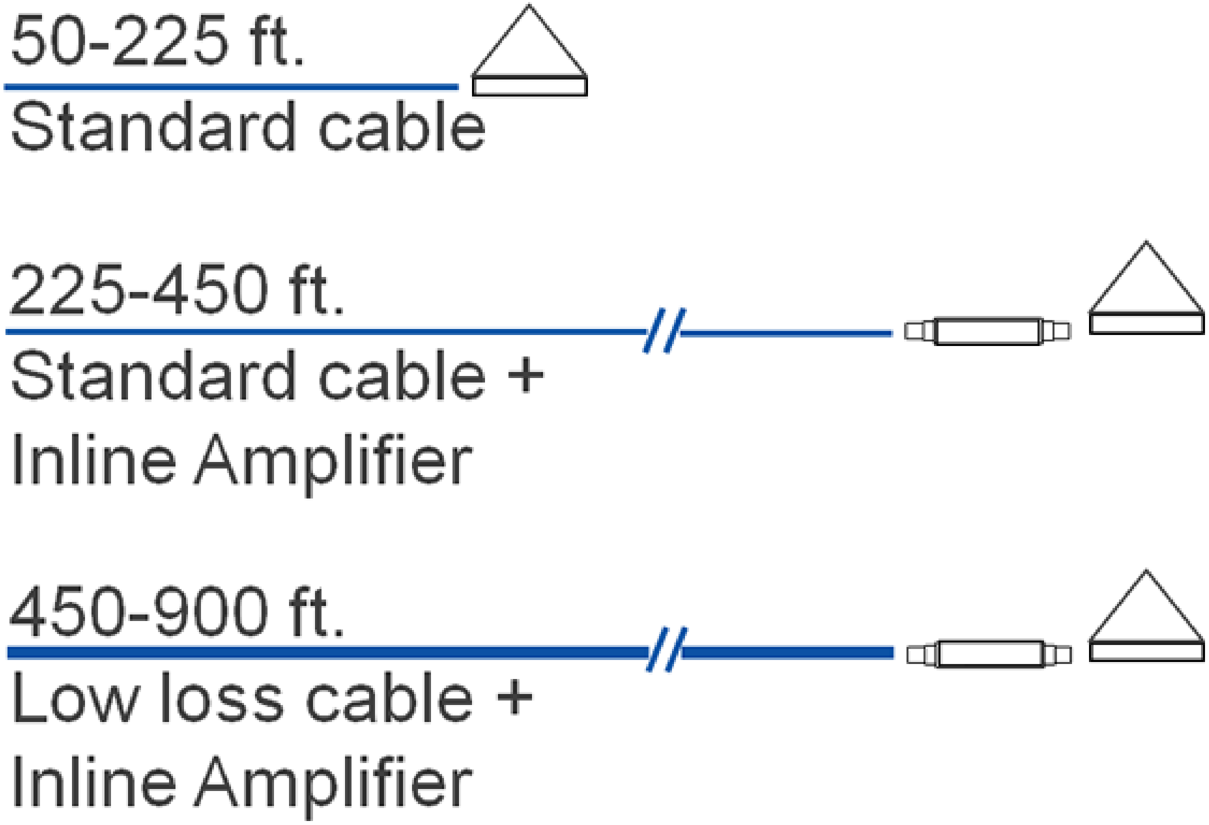
Antenna cables and accessories enable versatile solutions that are easy to achieve. Inline GNSS amplifiers installed at the antenna are an easy way to extend cable that runs from 225 feet to up to 900 feet, depending on cable type. Lightning arrestors provide valuable electrical protection to SyncServer. antenna cable splitters leverage a single antenna and cable for up to four GNSS receivers.

Ordering antenna components is a simple task. It is important to have a general idea of the total required cable length between SyncServer and the mounting location of the antenna. Any extra cable can be coiled to the side.

Table 7-7 lists the available and pre-configured kits that include cable, antenna, and related mounting accessories. These kits vary by total cable length, and are based on whether a lightning arrestor is required or not. For long cable runs (> 225 feet), the components are assembled individually. For more information, see the following figure.

To assist and simplify configuration, Microchip has an Excel-based antenna configurator that helps you to determine the exact part numbers they need for the desired cable length and accessories. For more information about the configuration, see the Microchip website.

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 feet cable to connect to the next accessory (inline amplifier or antenna).

Notes:

- Lightning Arrest Kit includes 25 feet cable. Total length includes the additional cable that is part of the Lightning arrestor, if selected.
- To receive GLONASS or BeiDou signals, the antenna system must be made of GLONASS and/or BeiDou compatible components.

Table 7-7. GNSS Antenna Kits and Accessories

Antenna Kit	Part Number
Kit: Total length: 50 feet Cable: 50 feet; antenna kit (093-15202-001)	990-15202-050
Kit: Total length: 75 feet Cable: 50 feet; lightning arrestor (112-43400-00-3) Cable: 25 feet; antenna kit (093-15202-001)	990-15202-075

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

Antenna Kit	Part Number
Kit: Total length: 100 ft, Cable: 100 ft; antenna kit (093-15202-001)	990-15202-100
Kit: Total length: 125 feet Cable: 100 feet; lightning arrestor (112-43400-00-3) Cable: 25 feet; antenna kit (093-15202-001)	990-15202-125
Kit: Total length: 150 feet Cable: 150 feet; antenna kit (093-15202-001)	990-15202-150
Kit: Total length: 175 feet Cable: 150 feet; lightning arrestor (112-43400-00-3) Cable: 25 feet; antenna kit (093-15202-001)	990-15202-175
Kit: Total length: 200 feet Cable: 200 feet; antenna kit (093-15202-001)	990-15202-200
Kit: Total length: 225 ft, Cable: 200 feet; lightning arrestor (112-43400-00-3) Cable: 25 feet; antenna kit (093-15202-001)	990-15202-225
250 feet antenna cable	060-15202-250
350 feet antenna cable	060-15202-350
450 feet antenna cable	060-15202-450
500 feet low loss antenna cable	060-15202-500
750 ft. low loss antenna cable	060-15202-750
900 feet 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
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

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

Antenna Kit	Part Number
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/Galileo/GLONASS/BeiDou 1:4 splitter with two (2) x 3 feet 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, 40 dB GNSS antenna, N connector. Standard cable is LMR-240 or equivalent. Low loss cable is LMR-400 or equivalent.

7.8 Returning SyncServer S6x0

You must return the equipment to Microchip only after you have exhausted the troubleshooting procedures described in the preceding sections, or if Microchip FTS Services and Support has advised you to return the unit.

Note: 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 must be protected with connector covers and the equipment must be wrapped in plastic before packaging. Ensure that the display and connectivity panels are protected when packaged.

7.8.2 Equipment Return Procedure

Perform the following steps to return the 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 (RMA) before returning the product for service. You can request an RMA at Microchip Timing & Synchronization Systems Support page. 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 on)
4. Ship the product to Microchip, transportation prepaid and insured, with the 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 TLS/SSL Cipher Suites

The following TLS/SSL cipher suites are current as per firmware release 5.0. The list might change with subsequent firmware releases.

Ciphers used with cipher suite configuration of SSL_HIGH_ENCRYPTION:

- TLSv1.3 128 bits TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253
- TLSv1.3 256 bits TLS_AES_256_GCM_SHA384 Curve 25519 DHE 253
- TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253

Ciphers used with cipher suite configuration of SSL_HIGH_AND_MEDIUM_ENCRYPTION:

- TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384Curve 25519 DHE 253
- TLSv1.2 256 bits DHE-RSA-AES256-GCM-SHA384 DHE 2048 bits
- TLSv1.2 256 bits ECDHE-RSA-CHACHA20-POLY1305 Curve 25519 DHE 253
- TLSv1.2 256 bits DHE-RSA-CHACHA20-POLY1305 DHE 2048 bits
- TLSv1.2 256 bits DHE-RSA-AES256-CCM8 DHE 2048 bits
- TLSv1.2 256 bits DHE-RSA-AES256-CCM DHE 2048 bits
- TLSv1.2 256 bits ECDHE-ARIA256-GCM-SHA384 Curve 25519 DHE 253
- TLSv1.2 256 bits DHE-RSA-ARIA256-GCM-SHA384 DHE 2048 bits
- TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256Curve 25519 DHE 253
- TLSv1.2 128 bits DHE-RSA-AES128-GCM-SHA256 DHE 2048 bits
- TLSv1.2 128 bits DHE-RSA-AES128-CCM8 DHE 2048 bits
- TLSv1.2 128 bits DHE-RSA-AES128-CCM DHE 2048 bits
- TLSv1.2 128 bits ECDHE-ARIA128-GCM-SHA256 Curve 25519 DHE 253
- TLSv1.2 128 bits DHE-RSA-ARIA128-GCM-SHA256 DHE 2048 bits
- TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve 25519 DHE 253
- TLSv1.2 256 bits DHE-RSA-AES256-SHA256 DHE 2048 bits
- TLSv1.2 256 bits ECDHE-RSA-CAMELLIA256-SHA384 Curve 25519 DHE 253
- TLSv1.2 256 bits DHE-RSA-CAMELLIA256-SHA256 DHE 2048 bits
- TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve 25519 DHE 253
- TLSv1.2 128 bits DHE-RSA-AES128-SHA256 DHE 2048 bits
- TLSv1.2 128 bits ECDHE-RSA-CAMELLIA128-SHA256 Curve 25519 DHE 253
- TLSv1.2 128 bits DHE-RSA-CAMELLIA128-SHA256 DHE 2048 bits
- TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve 25519 DHE 253
- TLSv1.2 256 bits DHE-RSA-AES256-SHA DHE 2048 bits
- TLSv1.2 256 bits DHE-RSA-CAMELLIA256-SHA DHE 2048 bits
- TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve 25519 DHE 253
- 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
- TLSv1.2 256 bits AES256-GCM-SHA384
- TLSv1.2 256 bits AES256-CCM8
- TLSv1.2 256 bits AES256-CCM
- TLSv1.2 256 bits ARIA256-GCM-SHA384
- TLSv1.2 128 bits AES128-GCM-SHA256
- TLSv1.2 128 bits AES128-CCM8
- TLSv1.2 128 bits AES128-CCM
- TLSv1.2 128 bits ARIA128-GCM-SHA256
- TLSv1.2 256 bits AES256-SHA256
- TLSv1.2 256 bits CAMELLIA256-SHA256
- TLSv1.2 128 bits AES128-SHA256
- TLSv1.2 128 bits CAMELLIA128-SHA256
- TLSv1.2 256 bits AES256-SHA
- TLSv1.2 256 bits CAMELLIA256-SHA
- TLSv1.2 128 bits AES128-SHA
- TLSv1.2 128 bits SEED-SHA
- TLSv1.2 128 bits CAMELLIA128-SHA

7.10 SSH Cipher Information

The following SSH cipher information is current as per firmware release 5.0. The list might change with subsequent firmware releases.

- Key Exchange Algorithms:
  - (kex) curve25519-sha256@libssh.org
  - (kex) diffie-hellman-group16-sha512
  - (kex) diffie-hellman-group18-sha512
  - (kex) diffie-hellman-group14-sha256
- Host-Key Algorithms:
  - (key) rsa-sha2-512
  - (key) rsa-sha2-256
  - (key) ssh-rsa
- Encryption Algorithms (Ciphers):
  - (enc) chacha20-poly1305@openssh.com
  - (enc) aes128-ctr
  - (enc) aes192-ctr
  - (enc) aes256-ctr
  - (enc) aes128-gcm@openssh.com
  - (enc) aes256-gcm@openssh.com
- Message Authentication Code Algorithms:
  - (mac) umac-128-etm@openssh.com
  - (mac) hmac-sha2-256-etm@openssh.com
  - (mac) hmac-sha2-512-etm@openssh.com

7.11 User Guide Updates

When this manual is updated, the updated version is 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 must register with Microchip for a username and password. If you are currently registered, login and download the manual update.

For technical support details, see 16. Technical Support.

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
- 10 security/Authorization messages
- 20 SyncServer S6x0 messages (events and alarms)
- 21 SyncServer S6x0 command history (CLI)

8.2 Severity Codes

- 2 Critical: critical conditions
- 3 Error: error conditions
- 4 Warning: warning conditions
- 5 Notice: normal but significant condition
- 6 Info: Informational

Table 8-1. Mapping of System Alarm Level to Severity Code

System Alarm Level	Severity Code
Major	3
Minor	4
Notify	5

Note: Major and minor alarms are also indicated by the Alarm LED(s) on the front panel.

The local log message format is as follows:

```
Mmm dd  hh:mm:ss
host_name Process-name AlarmID,Index,Severity, MsgText
```

Where:

- mm = 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
- MsgText = (see Table 8-2)

8.3 System Notification Messages

The following table lists the system notification messages. These messages are logged and sent to a remote syslog server, if configured. These messages can also be sent through 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 power-up alarm, Event ID 9 in the following table).

Table 8-2. System Notification Messages

Name/Description	Event ID	MSG Level	Transitory	MSG Text	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
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

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

Name/Description	Event ID	MSG Level	Transitory	MSG Text	Corrective Action
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
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

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

Name/Description	Event ID	MSG Level	Transitory	MSG Text	Corrective Action
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 server switch	53	Notify	Yes	PTP server 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
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 server	77	Notify	Yes	PTP state changed to server 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

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

Name/Description	Event ID	MSG Level	Transitory	MSG Text	Corrective Action
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 10 mA 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
GNSS PPS failure	98	Major	No	Reserved—event is never reported	Reserved—event is never reported

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

Name/Description	Event ID	MSG Level	Transitory	MSG Text	Corrective Action
J1A Input LOS (LOSS OF SIGNAL)[5]	99	Notify	No	J1A Input LOS J1A Input LOS cleared	- Check if the cable is securely connected. - Check if the 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 the cable is securely connected. - Check if the 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.

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

Name/Description	Event ID	MSG Level	Transitory	MSG Text	Corrective Action
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[1]. No action required.
RESERVED	113				•
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.

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

Name/Description	Event ID	MSG Level	Transitory	MSG Text	Corrective Action
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. No action required.
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.

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

Name/Description	Event ID	MSG Level	Transitory	MSG Text	Corrective Action
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
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

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

Name/Description	Event ID	MSG Level	Transitory	MSG Text	Corrective Action
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
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.

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

Name/Description	Event ID	MSG Level	Transitory	MSG Text	Corrective Action
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.
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.

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

Name/Description	Event ID	MSG Level	Transitory	MSG Text	Corrective Action
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.
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[6]	203	Minor	No	GNSS exception: <exception description> GNSS exception cleared: <exception description>	No action required No action required.
AGC Out of Range	204	Minor	No	BlueSky GNSS AGC detector Exit BlueSky GNSS AGC detector	Check for possible jammer/spoofer No action required.
BlueSky GNSS C/No Consistency	205	Minor	No	BlueSky <constellation group> GNSS CNo consistency detector <values> Exit BlueSky <constellation group> GNSS CNo consistency detector <values>	Check for possible spoofer No action required.
BlueSky GNSS C/No Consistency	206	Minor	No	BlueSky <constellation group> GNSS CNo consistency detector <values> Exit BlueSky <constellation group> GNSS CNo consistency detector <values>	Check for possible spoofer No action required.

Notes:

1. The GNSS Signal Low alarm is created if the unit has achieved a position solution, but is not tracking at least four 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, and 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 server) 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 10 MHz output adjustments are being limited from changing too fast to maintain optimal 10 MHz output phase noise performance.
5. Input LOS alarms could be generated if the input is slower than 1 PPS. Microchip recommends disabling the LOS alarm actions on the Admin->Alarms page under this condition.
6. The SyncServer provides a GNSS exception alarm, which is asserted if the system identifies timing anomalies with the GNSS input. In these cases, the GNSS input is not meeting expectations. The system compares the GNSS input against the internal oscillator.
   Following four GNSS exception alarms can be raised:
   - 1. Pull-out (fast)—Fast response indicating the frequency offset of the GNSS input exceeds the expected tolerance.
   - 2. Pull-Out (slow)—Slow response indicating the frequency offset of the GNSS input has slowly exceeded the expected tolerance.
   - 3. Stability—System has detected excessive instability of the GNSS input.
   - 4. Phase-Step—System has detected a significant fast phase step of the GNSS input.

9. Specifications

This section provides mechanical and electrical specifications and factory defaults for SyncServer S6x0.

9.1 Input and Output Signal Specifications

This section provides the specifications for input and output signals of SyncServer S6x0.

9.1.1 Mechanical

Table 9-1. SyncServer S6x0 Mechanical Specifications

Parameter	Description
Mounting	19i-nch or 23-inch rack
Rack Mounting	See Figure 2-2 for drawings with detailed chassis dimensions.
Width	17.24 inch/438 mm
Height	1.73 inch/44 mm; 1 RU
Depth	15.00 inch/81 mm 15.88 inch/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 ℃, –4 °F to 149 °F—Standard or OCXO [startup > –20 ℃ (–4 °F)] • 5 ℃ to 55 ℃, 23 °F to 131 °F—Rubidium oscillator
Storage temperature	40 ℃ to 85 ℃, –40 °F 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 V_{AC} (90 V_{AC} to 250 V_{AC}), 50 Hz/60 Hz
AC Power— operating	50W, 417 mA at 120V

Table 9-4. SyncServer S6x0 Dual DC Power Specifications

Parameter	Description
Input voltage range	20 $_{AC}$ to 75 V_{AC}

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

Parameter	Description
DC Power— operating	50W
Cable connector parts	Housing—Molex 03-12-1036 Terminals—0018121222 (16–18 AWG tin plated)

9.1.4 Compliance and Certifications

Table 9-5. SyncServer S6x0 Compliance Specifications

Parameter	Description
Safety certifications	UL 62368-1/CSA C22.2 62368-1, EN/IEC 62368-1 Second Edition
EMC	
Emissions	• FCC Part 15, Class A • EN 55011 • CISPR 32, Class A • EN55014 • VCCI
Immunity radiated	ENV50140 RF immunity, 10V/m, 80 MHz–1000 MHz, 80% modulation; 900 MHz pulsed at 200 Hz
Immunity conducted	• ENV50140 RF common mode immunity, 0.15 MHz–80 MHz, 10V, 80% modulation • EN61000-4-8 Magnetic Field immunity, 50 Hz, 40 A/m continuous, 1000 A/m for 1s
Environmental and Physical	
Environmental compliance	• PSE • RoHS3 with exemptions
Shock and vibration:	
Operational	ETSI EN-300 019-2-3, Mil-STD-810H
Storage	IEC 60068-2-6 Fc (sinusoidal vib), Mil-Std-810H, figure 514.6C-3
Transportation—bounce	IEC 60068-2-27Ea (shock 18g)
Transportation—vibration	IEC 60068-2-64Fh (random vib)
Transportation—package drop	IEC 60068-2-31 Ec
Seismic	EN300 019-2-3, NEBS GR-63-CORE
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

9.1.5 General Protocols

Following is the list of general protocols.

- 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 1–8 servers
- Key management protocols can be individually disabled
- PORT 1: Management and Time protocols
- PORT 2, 3 and 4: Time protocols only

9.1.6 Serial Port

Table 9-6. SyncServer S6x0 Console Serial Port Specifications

Item	Description
Connector type	9-pin, female D connector
Connector abel	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

9.1.7 Input Signals

9.1.7.1 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	50Ω
Coupling	DC (center pin provides DC power to the GNSS antenna or in-line amplifier)
Output to antenna voltage current	9.7 V_{DC} 100 mA (maximum)

...........continued	
Parameter	**Specification**
Connector type	BNC connector, female
Connector label	GNSS

9.1.7.2 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	50Ω or high impedance (> 50 kΩ)
Connector type	BNC
Connector label	J1
Signal level	AM: Ratio 2:1 to 3.5:1 Amp: 1V to 8V p-p, into 50Ω DCLS: <0.8V for logic 0, >2V 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 µm fiber

9.1.7.3 NTP Input

Table 9-10. SyncServer S6x0 NTP Input Signal Specifications

Parameter	Specification
Connector type	RJ45
Connector label	1, 2, 3, and 4

9.1.7.4 PPS Input

1 PPS 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	50Ω or high impedance (> 50k Ω)
Connector type	BNC
Connector label	J1

1 PPS 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

9.1.7.5 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	< 0.8V for logic 0 > 2V for logic 1
Impedance	50Ω or high impedance (> 50k Ω)
Connector type	BNC
Connector label	J1

9.1.7.6 10 MHz, 5 MHz, and 1 MHz Input

The 10 MHz, 5 MHz, and 1 MHz 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 V_{PP} to 8 V_{PP}
Impedance	50Ω
Connector type	BNC
Connector label	J2

9.1.7.7 T1 and 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 V_{PP} to 6.5 V_{PP}
Impedance	110Ω
Connector type	RJ48C, balanced pair
Connector label	J7

9.1.7.8 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 1 PPS input.

Table 9-16. SyncServer S6x0 HaveQuick Input Signal Specifications

Parameter	Specification
Signal type	HaveQuick HaveQuick 1 PPS
Amplitude	5V or TTL
Impedance	50Ω
Connector type	BNC
Connector label	J1 for HaveQuick J2 for HaveQuick 1 PPS (only available if J1 is used for HaveQuick input).

9.1.7.9 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
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

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

Reference	Timing Accuracy to Reference	Comments
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

9.1.8 Output Signals

9.1.8.1 NTP Output

Table 9-18. SyncServer S6x0 NTPOutput Signal Specifications

Parameter	Specification
Connector type	RJ45
Connector label	Ports 1, 2, 3, and 4

The timestamps have been compensated for 1000BT. For 100BT, the NTP packets have a bias of up to 1 ms.

9.1.8.2 PTP Server 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, and 4
PTP profile	Enterprise

9.1.8.3 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, and J8

...........continued	
Parameter	**Specification**
Impedance	50Ω
Signal level	AM: Ratio 10:3 ±10% Amp: 3.5 ±0.5 V_{PP} DCLS: < 0.8V for logic 0, > 2.4V 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 and fiber optic
Connector label	J3, J5, and J7
Wavelength	820 nm
Fiber	Multimode
Maximum length	1000m using 62.5/125 um fiber

9.1.8.4 T1 and 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 and 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, 100Ω
E1 amplitude	3 V ±0.3V, 120Ω
CC amplitude	3 Vpk ±0.4V
JCC amplitude	1 Vpk ±01V, nominal
JSW amplitude	0 DBm ±3 dB, 120Ω
1.054 or 2.048 MHz square wave amplitude	3 V_{PP} ±0.3V
Connector type	RJ48C, balanced pair
Connector label	J7 and J8

9.1.8.5 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 1 PPS or 1 PPM outputs.

Table 9-23. SyncServer S6x0 HaveQuick Output Signal Specifications

Parameter	Specification
Signal type	HaveQuick TTL HaveQuick 5V
Amplitude	5V or TTL
Impedance	50Ω
Connector type	BNC
Connector label	J3–J6

Table 9-24. SyncServer S6x0 1 PPS/1 PPM Output Signal Specifications on Timing I/O Module with HaveQuick/PTTI

Parameter	Specification
Signal type	1 PPS 1 PPM
Amplitude	5V or 10V
Impedance	50Ω
Connector type	BNC
Connector label	J3–J6

9.1.8.6 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 ToD, day of year, and TFOM Transmitted at 50 bps.
Amplitude	±2V minimum to 100Ω, ±3V typical
Impedance	110Ω
Connector type	RJ48C, balanced pair
Connector label	J7–J8

9.1.8.7 ToD Output

Table 9-26. SyncServer S6x0 1 PPS+ToD Output Signal Specifications

Parameter	Specification
Connector type	9-pin, female D connector
Connector label	DATA/TIMING
Signal level	RS-232

...........continued	
Parameter	**Specification**
Timing Relationship between 1 PPS and ToD	Transmission of a ToD message starts 10 ms (default) after the rising edge of 1 PPS signal, and the transmission is completed within 500 ms. 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 checksum 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.
See ToD Transmission Parameters. SyncServer S6x0 1 PPS+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

9.1.8.8 PPS Output

Table 9-27. SyncServer S6x0 1 PPS + TOD Output Signal Specifications

Parameter	Specification
Connector type	BNC female connector
Connector label	1 PPS
Impedance	50
Signal level	3.25V, typical
Timing relationship between 1 PPS and TOD	Transmission of a TOD message starts 10 ms (default) after the rising edge of 1 PPS 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—1 PPS pulse	1.5 ns, typical
Pulse width	20 µs
Active edge	Rising

9.1.8.9 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	50Ω

...........continued	
Parameter	**Specification**
Signal Level	2 V_{PP}–3 V_{PP}

9.1.8.10 1 PPS x N Output Signal Specifications

The 1 PPS x N outputs are available with the Optional Timing I/O module (090-15201-006), and on ports J3–J6 on the Telecom (090-15201-011) and the HaveQuick/PTTI modules (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 1 PPS Output Signal Specifications

Parameter	Specification
Signal type	Rising edge on-time TTL or optical
Settings—fixed rate	• 10/5/1 MPPS • 100/10/1/k PPS • 100/10/1/0.5 PPS • 1 PPM
Settings—programmable period	100 ns to 86400 seconds, step size of 10 ns
Pulse width	• 50% for programmable pulse • 20 µs 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	50Ω for electrical

9.1.8.11 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
Allan Deviation: 1s 10s	 <3.0 × 10^{-12} <4.5 × 10^{-12}
Output level	13 dBm ±1.5 dB
Channel-to-Channel isolation	100 dB at 10 MHz
Connector type	BNC male

...........continued	
Parameter	**Specification**
Connector label	J1–J8
Impedance	50Ω

9.1.8.12 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 1s 10s	 $<4.5 \times 10^{-13}$ $<2.0 \times 10^{-12}$
Output level	13 dBm ±1 dB
Channel isolation	100 dB at 10 MHz
Connector type	BNC male
Connector label	J1–J8
Impedance	50Ω

Table 9-32. Holdover Performance

Oscillator	Holdover—24 Hour (µsec)
Standard	400
OCXO	25
Rubidium	<1

Note: Holdover values are approximate and consider operation at constant temperature, no initial frequency or phase offset, and that the unit has been powered on for two weeks and locked to GNSS for three consecutive days.

Attention:
Information contained in this publication 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. 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 ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. 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.

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 another 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 lists the 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 gm
Environmental	
Operating temperature	40 °C 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 at 1590 MHz, 8 dB typical at band-edges

...........continued	
Characteristic	**Specification**
Filtered LNA Frequency	1575 MHz to 1606 MHz
Gain	40 dB minimum
Gain	flatness ±2 dB 1575 MHz 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 V_{DC} nominal (12 V_{DC} recommended maximum)
Supply current	20 mA maximum at 85 ℃

9.2.2 Wideband GNSS Antennas with Internal LNA Specifications

The following table lists the 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 bands (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 feet 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 gm
Environmental	
Operating temperature	40 ℃ to 85 ℃
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 maximum
Filtered LNA frequency	1559 MHz 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 V_{DC} to 16 V_{DC} nominal (12 V_{DC} recommended maximum)
Supply current	19 mA maximum at 85 ℃

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, R Ohs 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 V_{DC} (spark over)
RF power	25W
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 lists 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 inch (59 mm)
Operating temperature	40 ℃ to 85 ℃
Environmental	RoHS, REACH, and IP67

...........continued	
Characteristic	**Specification**
Electrical	
Nominal gain	25 dB +4/–0 dB typical
Pass band ripple	±2 dB
Impedance	50Ω
Noise figure	2 dB typical
Bandwidth	1.2 GHz 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 lists the 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 is chosen to power the antenna while the pther inputs are switched to DC loads. If the selected DC bias input fails, the DC bias is automatically switched 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	50Ω
Frequency range	1 GHz to 2 GHz
Noise figure	2 dB maximum
Port-to-port isolation	30 dB–40 dB
DC power	3.3 $_{DC}$ to 12 V_{DC}
Operating current	18 mA to 20 mA
Pass through current	250 mA
Group delay and L1	5 ns
RF connectors	Female N-type
RoHS 6/6	Compliant

9.2.6 GPS Antenna Coaxial Cable Specifications

Other cable types are also available. The following table lists the 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 (at 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 —0.00053Outer conductor—0.0012	.176-inch diameter solid BCCAI	—

Attention:
Information contained in this publication 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. 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 ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. 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.

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
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 value)	[<printable ASCII>], 1 —49 chars
Priv Phrase (v3 user)	Blank (no value)	[<printable ASCII>], 1 —49 chars
Auth Phrase (v3 user)	Blank (no value)	[<printable ASCII>], 1 –49 chars
Min Priv (v3 user)	Authentication	Authentication | Authentication and 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

...........continued		
Description	**Default Value**	**Value Range**
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 Server Configuration Parameters for Default 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	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
TTL	16	1 to 255

Table 9-45. PTP > PTP Server 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
TTL	16	1 to 255

Table 9-46. PTP > PTP Server Configuration Parameters for ITU-G.8265.1 Profile

Description	Default Value	Value Range
Domain	4	4 to 23
Two-Step	Disable	Disable | Enable
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

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

Description	Default Value	Value Range
TTL	64	1 to 255

Table 9-47. PTP > PTP Server Configuration Parameters for ITU-G.8275.1 Profile

Description	Default Value	Value Range
Domain	24	24 to 43
Two-Step	Disable	Disable | Enable
Priority 2	128	0 to 255
Announce timeout	3	3 to 10
Client timeout	300	10 to 3600
Offset scaled log variance override	Not checked	Not checked or checked
Offset scaled log variance	0x4e5d	0x0 to 0xffff

Table 9-48. PTP > PTP Server Configuration Parameters for ITU-G.8275.2 Profile

Description	Default Value	Value Range
Domain	44	44 to 63
Two-Step	Disable	Disable | Enable
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
TTL	64	1 to 255

Table 9-49. PTP > PTP Server 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
VLAN	Disable	Disable | Enable
VLAN ID	0	0 to 4094

...........continued		
Description	**Default Value**	**Value Range**
VLAN priority	4	0 to 7

Table 9-50. PTP > PTP Server Configuration Parameters for Power C37-238-2017 Profile

Description	Default Value	Value Range
Domain	254	0 to127, 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	10s to 3600s
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 9-51. PTP > PTP Server 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
Pdelay resp followup	Disable	Disable | Enable
Announce timeout	3	2 to 10
Client timeout	300	10s to 3600s

...........continued		
Description	**Default Value**	**Value Range**
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 9-52. PTP > PTP Server Configuration Parameters for SMPTE Profile—Hybrid

Description	Default Value	Value Range
Delay mechanism	E2E	E2E
Domain	127	0–127
Two-Step	Disable	Enable/Disable
Priority 1	128	0–255
Priority 2	128	0–255
PTP state	Enable	Enable/Disable
Announce interval	–2	–3 to 1
Sync interval	–3	–7 to 1
Delay Pdelay interval	–3	–7 to 4
Announce timeout	3	2–10
Diffserv code	0	0–63
TTL	64	1–255
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

...........continued		
Description	**Default Value**	**Value Range**
Time adders 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, and 50

Table 9-53. PTP > PTP Server 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
TTL	64	1 to 255
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

...........continued		
Description	**Default Value**	**Value Range**
Daily jam	None	None Local Time: Hour 0–23 Minute 0, 10, 20, 30, 40, and 50

Table 9-54. PTP > PTP Server 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
TTL	64	1 to 255
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: Hours 0–23 Minute 0, 10, 20, 30, 40, and 50

Table 9-55. PTP > PTP Server Configuration Parameters for Data Center Profile

Description	Default Value	Value Range
Domain	0	0 to 255
Two-Step	Disable	Disable | Enable
Priority 2	128	0 to 255
Management message	Enable	Disable | Enable
Diffserv code	46	0 to 63
Offset scaled log variance override	Not checked	Not checked or checked
Offset scaled log variance	0x4e5d	0x0 to 0xffff
TTL	64	1 to 255

Table 9-56. 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
Server 1	—	Valid IP address
Server 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
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 SyncServer S6x0.

Table 9-57. PTP > PTP Client Configuration Parameters for Enterprise Profile

Description	Default Value	Value Range
Addressing	Hybrid	Hybrid | Multicast
Domain	0	0 to 255
Delay request interval	–6	–6 to –4
Announce timeout	3	3 to 4
Diffserv code	0	0 to 63
TTL	64	1 to 255
FPP cluster width 1	10000	1000 to 10000000
FPP cluster width 2	100000	1000 to 10000000

Table 9-58. PTP > PTP Client Configuration Parameters for Default Profile

Description	Default Value	Value Range
Domain	0	0 to 255
Delay request interval	–6	–6 to –4
Announce timeout	3	2 to 10
Diffserv code	0	0 to 63
TTL	64	1 to 255
FPP cluster width 1	10000	1000 to 10000000
FPP cluster width 2	100000	1000 to 10000000

Table 9-59. PTP > PTP Client Configuration Parameters for ITU-G.8265.1 Profile

Description	Default Value	Value Range
Domain	4	4 to 23
Lease duration	300	60 to 1000
Server 1	—	Valid IP address
Server 2	—	Valid IP address
Announce interval	1	–3 to 4
Sync interval	–6	–6 to –4
Delay request interval	–6	–6 to –4
Announce timeout	3	2 to 10
Unicast negotiation	Enable	Enable | Disable
Diffserv code	0	0 to 63
TTL	64	1 to 255
FPP cluster width 1	10000	1000 to 10000000
FPP cluster width 2	100000	1000 to 10000000

Table 9-60. PTP > PTP Client Configuration Parameters for ITU-G.8275.1 Profile

Description	Default Value	Value Range
Domain	24	24 to 43
Client local priority	128	1 to 255
Announce timeout	3	3 to 10
Server 1 clock ID	—	Valid clock ID
Server 2 clock ID	—	Valid clock ID
Server 1 local priority	128	1 to 255
Server 2 local priority	128	1 to 255
FPP cluster width 1	10000	1000 to 10000000
FPP cluster width 2	100000	1000 to 10000000

Table 9-61. PTP > PTP Client Configuration Parameters for ITU-G.8275.2 Profile

Description	Default Value	Value Range
Domain	44	44 to 63
Lease duration	300	60 to 1000
Client local priority	128	1 to 255
Announce interval	0	–3 to 0
Sync interval	–6	–6 to –4
Delay request interval	–6	–6 to –4
Announce timeout	3	2 to 10
Unicast negotiation	Enable	Enable | Disable
Server 1 IP address	—	Valid IPv4/IPv6 address
Server 2 IP address	—	Valid IPv4/IPv6 address
Server 1 local priority	128	1 to 255
Server 2 local priority	128	1 to 255
Diffserv code	0	0 to 63
TTL	64	1 to 255
FPP cluster width 1	10000	1000 to 10000000
FPP cluster width 2	100000	1000 to 10000000

Table 9-62. 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
Server 1	n/a	n/a
Server 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
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 SyncServer S6x0.

Table 9-63. 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
Server 1	n/a	n/a
Server 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
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 SyncServer S6x0.

Table 9-64. 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 to 1000
Server 1	—	Valid IP address
Server 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
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 9-65. Timing > Holdover Configuration Parameters

Description	Default Value	Value Range
Time error limit	Computed from Holdover Duration default, result depends on the oscillator type.	0.000100 ms–100 ms
Holdover duration	1 day	0.001 days–200.00 days

Table 9-66. Timing > Serial Parameters

Description	Default Value	Value Range
Output	Off	Off | NMEA | NENA | Legacy
NMEA detail	All Off	Any combination of the following is allowed: ZDA on/off, GGA on/off, GSV on/off, RMV on/off
NENA detail	DDD…	DDD… | WWW … | YYYY …

9.3.5 References

Table 9-67. References > GNSS Configuration Parameters

Description	Default Value	Value Range
GNSS constellation	GPS	{GPS, Galileo, QZSS}, GLONASS, BeiDou (up to two groups)
SBAS enable	Not checked	Checked or Not checked
Elevation mask	10	5 degrees 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 degree 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)	0.0m	1000.0m to 12000.0m
Antenna cable delay	0	0 ns to 10000 ns
GNSS receiver reset	unchecked	Checked | Unchecked

9.3.6 Security

Table 9-68. 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

...........continued		
Description	**Default Value**	**Value Range**
Special character required	Checked	Not Checked | Checked

Table 9-69. Security > Users > Password Expiration

Description	Default Value	Value Range
Password expiry	Enable	Enable/Disable
Number of days	365	1 to 365

Table 9-70. 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
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 eight 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 the 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 9-71. 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 9-72. 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 minutes to 1440 minutes

Table 9-73. Security > LDAP Settings

Description	Default Value	Value Range
Port–Server binding	389	1 to 65535
Time limit for searching	300	120s to 65535s
Time Limit for binding	300	120s to 65535s
LDAP protocol version	LDAPv3	LDAPv2 | LDAPv3
Scope to search server	sub	base | one | sub

9.3.7 Admin

Table 9-74. Admin > General Parameters

Description	Default Value	Value Range
Hostname	SyncServer	
Web session timeout	10 minutes	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 9-75. 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 9-76. 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

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

Description	Default Value	Value Range
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
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 9-77. Admin > Serial Port Configuration 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 9-78. Admin > Serial Port Configuration 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 9-79. Timing I/O Module Default Parameters

Description	Value Range
J1	Timecode; IRIG B; 1 kHz, with year; 50Ω; 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; 1 PPS; squelch never; phase offset of 0 ns
J7	Off
J8	Off

Table 9-80. Timing I/O Module—Telecom E1/T1 Default Parameters

Description	Value Range
J1	Timecode; IRIG B; 1 kHz, with year; 50Ω; 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; 1 PPS; squelch never; phase offset of 0 ns
J7	T1 output; ESF
J8	E1 output; CCS; SSMbit 4; CRC enable; zero suppress on

Table 9-81. Timing I/O Module—HaveQuick/PTTI Default Parameters

Description	Value Range
J1	Timecode; IRIG B; 1 kHz, with year; 50Ω; 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; 1 PPS; squelch never; phase offset of 0 ns
J7	Off
J8	Off

Table 9-82. Timing I/O Module—Fiber Input Default Parameters

Description	Value Range
J1	Pulse; Fixed rate; 1 PPS; cable delay of 0 ns
J2	Sine; 10 MHz

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

Description	Value Range
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; 1 PPS; squelch never; phase offset of 0 ns
J7	Off
J8	Off

Table 9-83. Timing I/O Module—Fiber Output Default Parameters

Description	Value Range
J1	Timecode; IRIG B; 1 kHz, with year; 50Ω; 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; 1 PPS; squelch never; phase offset of 0 ns
J7	Off
J8	Off

Table 9-84. Timing I/O Module—LPN/ULPN Default Parameters

Description	Default	Value Range
10 MHz to 1 PPS coherency	Disable	Enable | Disable

9.3.9 BlueSky-Related Factory Default Configuration

This section describes factory presets for all user-settable parameters related to the BlueSky capabilities. These are the settings that a new unit has on arrival from factory, but also can be accomplished at any time through the `Admin > Config Backup/Restore` form. All settings are retained through power-cycle.

Table 9-85. BlueSky Related Factory Defaults

Parameter	Factory Default Configurations	Details
Tracking group action, **Spoofing group** action, **validator anomalies group** action, and **RF Health group** action	Stopped. Action column appears as for each, indicating that it can be started.	Configured with BlueSky GNSS Detector Summary form (Figure 6-38).
GNSS site survey action	Stopped. Action column appears as for each, indicating that it can be started.	Configured with BlueSky GNSS Detector Summary form (Figure 6-38).
Tracked satellites detector threshold	4 satellites	Set with BlueSky Configuration form (Figure 6-39).
Max C/No detector threshold	60	Set with BlueSky Configuration form (Figure 6-39).

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

Parameter	Factory Default Configurations	Details
Position dispersion threshold	100 meters	Set with BlueSky Configuration form (Figure 6-39).
CW Jamming threshold	50%	Set with BlueSky Configuration form (Figure 6-39).
C/No Consistency Sensitivity	5	Set with BlueSky Configuration form (Figure 6-39).
C/No Drop Sensitivity	5	Set with BlueSky Configuration form (Figure 6-39).
AGC threshold	High: 60% Low: 30%	Set with BlueSky Configuration form (Figure 6-39).
Alarm Enable checkbox (applies to all detectors on configuration form)	NOT checked (alarm function is disabled)	Set with BlueSky Configuration form (Figure 6-39).
GNSS action on alarm (applies to all detectors on configuration form)	None (no GNSS action taken on alarm)	Set with BlueSky Configuration form (Figure 6-39).

Table 9-86. BlueSky Alarms—Generic Alarm Factory Presets

Parameter	Factory Default Configurations
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	0s (applies to all BlueSky alarms)
Reporting delay	0s (applies to all BlueSky alarms)
Send trap	Checked (enabled. It applies to all BlueSky alarms)
Write log	Checked (message log is written to. It applies to all BlueSky alarms)
Send Email	Not checked (email is not sent. It 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 accessories for your GNSS antenna system provided by Microchip. These accessories deliver precise GNSS signals over a wide temperature range and in harsh environmental conditions.

10.1 Antenna Kits Overview

The key factor to decide which of the available antenna kits is required, the distance between the GNSS antenna and SyncServer S6x0 must be considered. Several coaxial cable lengths are available to assist in receiving proper gains from the GNSS antenna. Microchip offers eight antenna kits for SyncServer S6x0, plus separate GNSS antenna accessory parts including antenna, cable, amplifier, lightning arrestor, and splitter.

10.1.1 Considerations for Antenna Installation

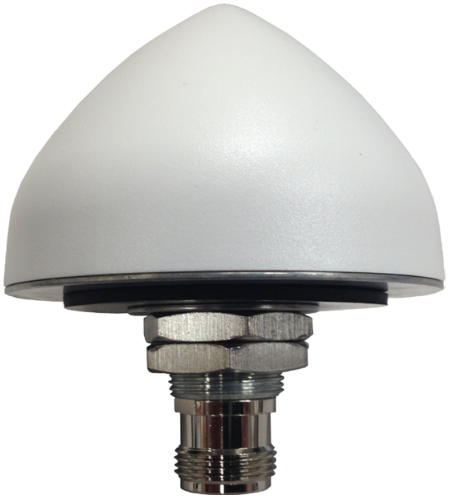
- The GNSS engine requires a net gain at the antenna connector input of the chassis to be between 15 dB–30 dB.
- All antenna kits include the GNSS L1 antenna, a mounting bracket, and a BNC cable adapter.
- The antennas, in-line amplifiers, and the lightning arrestor have N connectors.
- All the supplied antenna kits 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.

For more information, see 10.3. Antenna Coaxial Cable.

10.1.1.1 GNSS Antennas with Low Noise Amplifiers

The antenna used with SyncServer S600/S650 is a high-gain (40 dB) GNSS antenna covering the GPS L1, GLONASS L1, and SBAS (WAAS, EGNOS and MSAS) frequency band (1575 MHz–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-feet BNC(m) to N(f) cable is also included.

Figure 10-1. GNSS Antenna



Accuracy of the antenna position that is determined by using receiver survey depends on providing RF gain to the GNSS receiver within a required range of 15 dB–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 either requires longer than 20 minutes to complete or does not complete, preventing the GNSS input from being used by the system as a reference. Also, timing stability is not optimized if these conditions are not met.

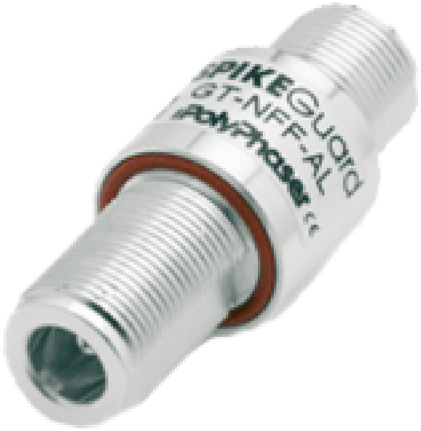
10.2 Antenna Kits Accessories

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. For specifications, see 9.2.3. GNSS Lightning Arrestor Specifications.

Lightning does not have to strike the antenna to significantly damage the antenna or the GNSS receiver. Damage is often because of a lightning strike on a nearby structure, not a direct strike on the antenna itself. As lightning strikes might induce damaging voltages in the antenna system when striking nearby objects, effort must be made 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.

Figure 10-2. GNSS Lightning Arrestor

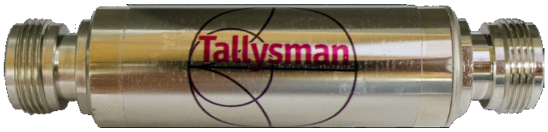


10.2.2 GNSS L1 In-line Amplifier

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. For specifications, see 9.2.4. GNSS L1 Inline Amplifier 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.

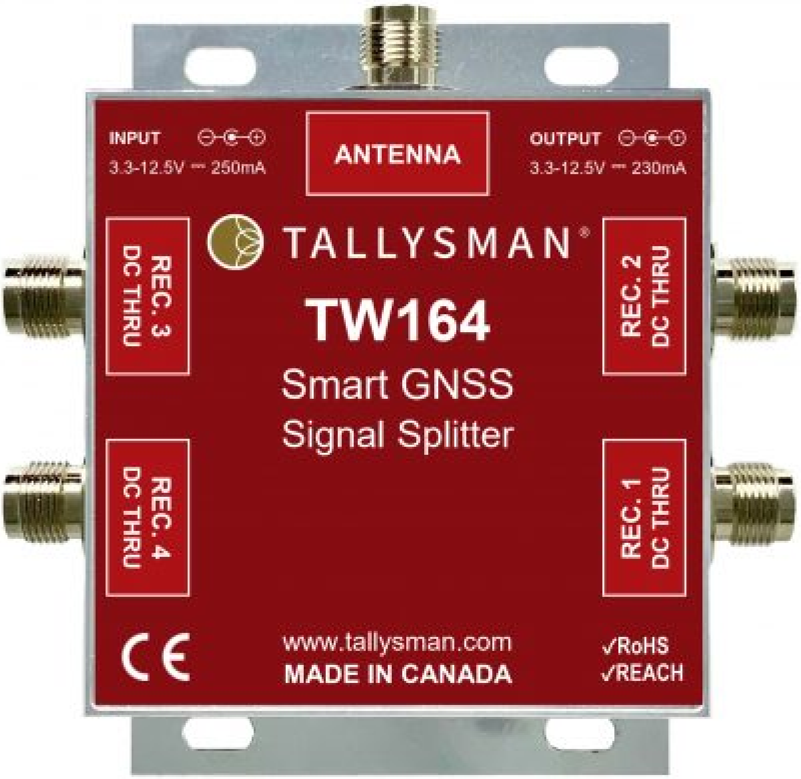
Figure 10-3. Inline Amplifier



10.2.3 GPS/Galileo/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 is chosen to power the antenna while other inputs are switched to DC loads. If the selected DC bias input fails, the DC bias automatically switches to another DC input to ensure an uninterrupted supply to the active antenna.

Figure 10-4. GPS/GLONASS/BeiDou Splitter



10.3 Antenna Coaxial Cable

Microchip provides coaxial cables with N-type connectors on both the ends. The following table lists the part numbers for the cables and their crimp kit. For more information, see 9.2.6. 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).

Note: Contact your sales office for available cable lengths and specific cable item number.

10.4 Legacy SyncServer Down/Up Converter

For very long antenna cable runs, GPS signal down/up converters were deployed. Microchip used to sell the now-discontinued 142-6150 family of down/up converters, which supported the L1 frequency. Therefore, it only supported GPS, Galileo, QZSS, and SBAS for GPS. This system used a coaxial cable between the converters. The up converter was inserted between the end of the coaxial cable and SyncServer. It was powered by an external power supply. The up converter was designed to also operate from power supplied on the RF connector. However, SyncServer S6x0 does not have sufficient power output to power the up converter. The up converter might not operate correctly if SyncServer S6x0 is powered up before the up converter's external power supply. Therefore, Microchip recommended that users install a DC-block between the up converter and SyncServer S6x0.

For very long antenna cable runs Microchip now recommends the 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.

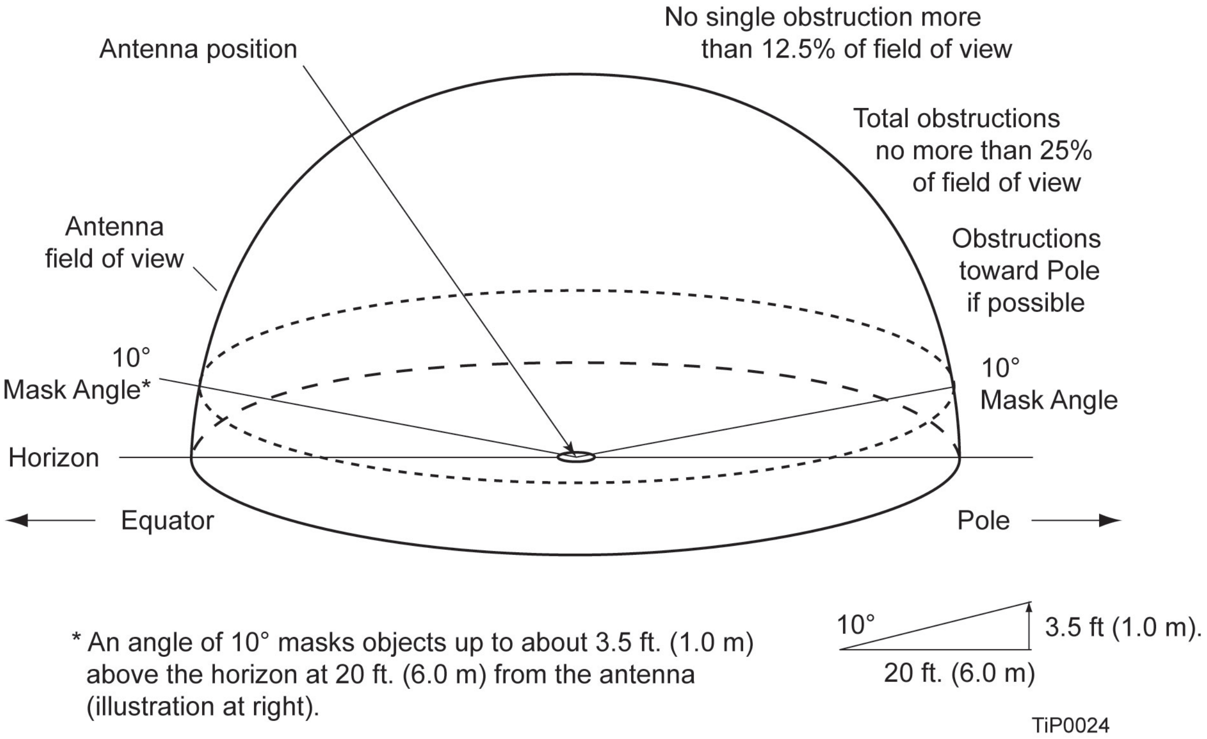
10.5.1 Planning the Antenna Location

Prior to installing the antenna, you must plan the site, antenna location, grounding scheme, cable route, and all other details.

10.5.2 Locating the Antenna

The following figure can be used as a guide to locate the antenna.

Figure 10-5. Locating the GNSS Antenna


No single obstruction more than 12.5% of field of view
Antenna position
Total obstructions no more than 25% of field of view
Antenna field of view
Obstructions toward Pole if possible
10° Mask Angle*
10° Mask Angle
Horizon
Equator
Pole
* An angle of 10° masks objects up to about 3.5 ft. (1.0 m) above the horizon at 20 ft. (6.0 m) from the antenna (illustration at right).
10°
3.5 ft (1.0 m).
20 ft. (6.0 m)
TiP0024

⚠WARNING

- 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 SyncServer S6x0 does not detect any current, it considers a failed GNSS antenna and consequently generates an alarm and switch to another timing (non-GNSS) source.

  Some GNSS splitters can block the DC current, and if used with SyncServer S6x0, cause the alarm condition as described in the previous section. Usage of such GNSS splitters with SyncServer S6x0 requires the installation of a 50Ω load, so that the SyncServer S6x0 GNSS interface is able to detect current and operate normally.
- To avoid severe injury to personnel or damage to equipment, exercise caution when working near high voltage lines:
  - 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.

⚠ 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.

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 preceding figure.
- 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 3.7m (12 feet) 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 9.1m (30 feet) of the point at which the antenna cable enters the building.
- Allow at least 3.0m (10 feet) 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 the location and mounting of antenna and cabling, you must develop a grounding scheme. The purpose of the grounding scheme is to provide protection against voltage surges and static discharge. If lightning arrestors are used, they must also 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 9.1m (30 feet) radius for any bends made.
- Ensure that no painted surface insulates the lightning arrestor or grounding clamps.
- Ensure that the 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 maintains 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 might be required for installing the GNSS antenna.

- Extra cable ties or acceptable cable clamps
- #6 AWG (16 mm^2) copper ground wire (minimum)
- Eight feet (2.9m) ground electrode
- Custom mounting plates, U-bolts, PVC pipes, masonry bolt, and so on, as needed for mounting to a tower, roof, or wall of a building
- A cable puller might be required for installing the antenna coaxial cable
- Digital Voltmeter (DVM)

⚠ CAUTION To avoid damage to the connectors, do not use the connectors to pull the cable. 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.

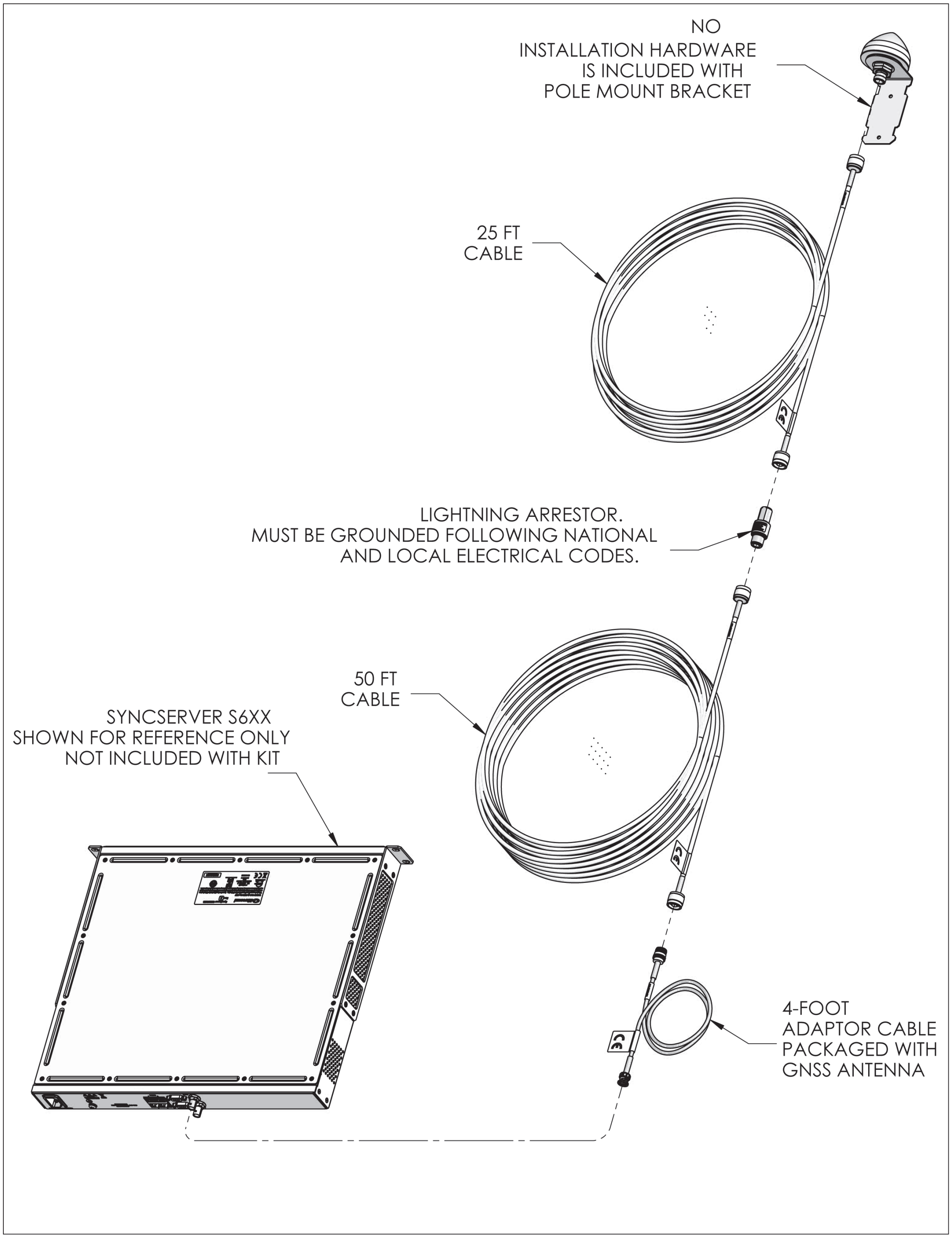
10.5.6 Installing the Antenna

This section describes procedures for installing the GNSS antenna, as shown in Figure 10-6.

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 an eight inch cable ties or appropriate cable clamps.
4. Adhere to local building codes to determine the type and number of fasteners, screws, bolts, and so on, that might be required.

Note: Follow local building electrical codes when installing the GNSS antenna.

Figure 10-6. 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. For more information, see the preceding figure.

1. Connect the 25 feet cable to the antenna.

⚠ CAUTION To avoid damage to the connectors, do not use the connectors to pull the cable. If 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 feet 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 feet 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 must be installed in accordance with your antenna system grounding scheme. Perform the following steps to install a lightning arrestor:

1. Mount the lightning arrestor within 30 feet (9m) 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 must 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 must install the antenna cable from the lightning arrestor to 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. 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.

Perform the following steps to connect the GNSS antenna:

1. Using a DVM, verify that the center conductor is not shorted to the shield.
   If the reading shows a short or open, you might 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 SyncServer S6x0.

Tip: Microchip recommends coiling excess cable to avoid gain mismatch between the GNSS antenna and SyncServer S6x0. Coiling the excess cable also allows you to use the factory-installed crimped connector.

10.5.10 Antenna Installation Completion Checklist

Perform the following steps to verify that the 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 the 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 might be charged to obtain the source code.

By using 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 SyncServer S6x0:

- PACKAGE NAME: ace-elements.min.js and ace.min.js
- LICENSE: BSD, https://cdnjs.com/libraries/ace

- PACKAGE NAME: adcsysmon
- PACKAGE VERSION: 1.0
- RECIPE NAME: adcsysmon
- LICENSE: GPLv2

- PACKAGE NAME: adduser
- PACKAGE VERSION: 3.118
- RECIPE NAME: adduser
- LICENSE: GPLv2

- PACKAGE NAME: apache2
- PACKAGE VERSION: 2.4.51
- RECIPE NAME: apache2
- LICENSE: Apache-2.0

- PACKAGE NAME: apr

- PACKAGE VERSION: 1.7.0
- RECIPE NAME: apr
- LICENSE: Apache-2.0

- PACKAGE NAME: apr-util
- PACKAGE VERSION: 1.6.1
- RECIPE NAME: apr-util
- LICENSE: Apache-2.0

- 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: 5.0
- RECIPE NAME: bash
- LICENSE: GPLv3+

- PACKAGE NAME: bind-libs
- PACKAGE VERSION: 9.11.22
- RECIPE NAME: bind
- LICENSE: ISC & BSD

- PACKAGE NAME: bind-utils
- PACKAGE VERSION: 9.11.22
- RECIPE NAME: bind
- LICENSE: ISC & BSD

- PACKAGE NAME: boost
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-atomic
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-chrono
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-container
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-context
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-contract
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-coroutine
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-date-time
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-filesystem
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-graph
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-iostreams
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-locale
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-log
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-math
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-program-options
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-python
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-random
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost

- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-regex
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-serialization
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-system
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-test
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-thread
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-timer
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: boost-wave
- PACKAGE VERSION: 1.72.0
- RECIPE NAME: boost
- LICENSE: BSL-1.0 & MIT & Python-2.0

- PACKAGE NAME: bootstrap-colorpicker.min.js
- LICENSE: Apache/MIT, https://cdnjs.com/libraries/bootstrap-colorpicker

- PACKAGE NAME: bootstrap.min.js
- LICENSE: MIT, https://getbootstrap.com/docs/4.0/about/license/

- PACKAGE NAME: bootstrap-tag.min.js
- LICENSE: Apache/MIT, https://github.com/bootstrap-tagsinput/bootstrap-tagsinput

- PACKAGE NAME: bootstrap-wysiwig.min.js
- LICENSE: Apache/MIT, https://github.com/mindmup/bootstrap-wysiwyg

- PACKAGE NAME: busybox
- PACKAGE VERSION: 1.31.1
- RECIPE NAME: busybox
- LICENSE: GPLv2 & bzip2-1.0.4

- PACKAGE NAME: busybox-udhcpc
- PACKAGE VERSION: 1.31.1
- RECIPE NAME: busybox
- LICENSE: GPLv2 & bzip2-1.0.4

- PACKAGE NAME: bzip2

- PACKAGE VERSION: 1.0.8
- RECIPE NAME: bzip2
- LICENSE: bzip2-1.0.6

- PACKAGE NAME: ca-certificates
- PACKAGE VERSION: 20211016
- RECIPE NAME: ca-certificates
- LICENSE: GPL-2.0+ & MPL-2.0

- PACKAGE NAME: Chart.js
- PACKAGE VERSION: 2.9.3
- LICENSE: MIT

- PACKAGE NAME: chosen.jquery.min.js
- PACKAGE VERSION: 0.11.1
- LICENSE: MIT

- PACKAGE NAME: CodeIgniter
- PACKAGE VERSION: 3.1.11
- LICENSE: MIT

- PACKAGE NAME: conntrack-tools
- PACKAGE VERSION: 1.4.6
- RECIPE NAME: conntrack-tools
- LICENSE: GPLv2+

- PACKAGE NAME: coreutils
- PACKAGE VERSION: 8.31
- RECIPE NAME: coreutils
- LICENSE: GPLv3+

- PACKAGE NAME: coreutils-stdbuf
- PACKAGE VERSION: 8.31
- RECIPE NAME: coreutils
- LICENSE: GPLv3+

- PACKAGE NAME: cpio
- PACKAGE VERSION: 2.13
- RECIPE NAME: cpio
- LICENSE: GPLv3

- PACKAGE NAME: cronie
- PACKAGE VERSION: 1.5.5
- RECIPE NAME: cronie
- LICENSE: ISC & BSD-3-Clause & BSD-2-Clause & GPLv2+

- PACKAGE NAME: d3.js
- PACKAGE VERSION: 5.15.0
- LICENSE: BSD

- PACKAGE NAME: db
- PACKAGE VERSION: 5.3.28
- RECIPE NAME: db
- LICENSE: Sleepycat

- PACKAGE NAME: dbus
- PACKAGE VERSION: 1.12.16
- RECIPE NAME: dbus

- LICENSE: AFL-2.1 | GPLv2+

- PACKAGE NAME: dbus-lib
- LICENSE: AFL-2.1 | GPLv2+
- PACKAGE VERSION: 1.12.16
- RECIPE NAME: dbus

- PACKAGE NAME: dhcp-client
- PACKAGE VERSION: 4.4.2
- RECIPE NAME: dhcp
- LICENSE: ISC

- PACKAGE NAME: dhcp-libs
- PACKAGE VERSION: 4.4.2
- RECIPE NAME: dhcp
- LICENSE: ISC

- PACKAGE NAME: diffutils
- PACKAGE VERSION: 3.7
- RECIPE NAME: diffutils
- LICENSE: GPLv3+

- PACKAGE NAME: directc
- PACKAGE VERSION: 0.1
- RECIPE NAME: directc
- LICENSE: GPLv2

- PACKAGE NAME: drivertestprogs
- PACKAGE VERSION: 0.1
- RECIPE NAME: drivertestprogs
- LICENSE: GPLv2

- PACKAGE NAME: e2fsprogs
- PACKAGE VERSION: 1.45.4
- RECIPE NAME: e2fsprogs
- LICENSE: GPLv2 & LGPLv2 & BSD & MIT

- PACKAGE NAME: e2fsprogs-badblocks
- PACKAGE VERSION: 1.45.4
- RECIPE NAME: e2fsprogs
- LICENSE: GPLv2

- PACKAGE NAME: e2fsprogs-dumpe2fs
- PACKAGE VERSION: 1.45.4
- RECIPE NAME: e2fsprogs
- LICENSE: GPLv2

- PACKAGE NAME: e2fsprogs-e2fsck
- PACKAGE VERSION: 1.45.4
- RECIPE NAME: e2fsprogs
- LICENSE: GPLv2

- PACKAGE NAME: e2fsprogs-mke2fs
- PACKAGE VERSION: 1.45.4
- RECIPE NAME: e2fsprogs
- LICENSE: GPLv2

- PACKAGE NAME: ed

- PACKAGE VERSION: 1.15
- RECIPE NAME: ed
- LICENSE: GPLv3+

- PACKAGE NAME: elfutils
- PACKAGE VERSION: 0.178
- RECIPE NAME: elfutils
- LICENSE: GPLv3+

- PACKAGE NAME: ethtool
- PACKAGE VERSION: 5.4
- RECIPE NAME: ethtool
- LICENSE: GPLv2+

- PACKAGE NAME: expat
- PACKAGE VERSION: 2.2.9
- RECIPE NAME: expat
- LICENSE: MIT

- PACKAGE NAME: expect
- PACKAGE VERSION: 5.45.4
- RECIPE NAME: expect
- LICENSE: PD

- PACKAGE NAME: factorycfg
- PACKAGE VERSION: 1.0
- RECIPE NAME: factorycfg
- LICENSE: BSD

- PACKAGE NAME: file
- PACKAGE VERSION: 5.38
- RECIPE NAME: file
- LICENSE: BSD-2-Clause

- PACKAGE NAME: findutils
- PACKAGE VERSION: 4.7.0
- RECIPE NAME: findutils
- LICENSE: GPLv3+

- PACKAGE NAME: fullcalendar.js
- PACKAGE VERSION: 1.6.1
- LICENSE: MIT

- PACKAGE NAME: fuse
- PACKAGE VERSION: 2.9.9
- RECIPE NAME: fuse
- LICENSE: GPLv2 & LGPLv2

- PACKAGE NAME: fuse-utils
- PACKAGE VERSION: 2.9.9
- RECIPE NAME: fuse
- LICENSE: GPLv2 & LGPLv2

- PACKAGE NAME: fuse3
- PACKAGE VERSION: 3.9.2
- RECIPE NAME: fuse3
- LICENSE: GPLv2 & LGPLv2

- PACKAGE NAME: fuse3-utils
- PACKAGE VERSION: 3.9.2
- RECIPE NAME: fuse3
- LICENSE: GPLv2 & LGPLv2

- PACKAGE NAME: fuser
- PACKAGE VERSION: 23.3
- RECIPE NAME: psmisc
- LICENSE: GPLv2

- PACKAGE NAME: gator
- PACKAGE VERSION: 5.22
- RECIPE NAME: gator
- LICENSE: GPL-2

- PACKAGE NAME: gawk
- PACKAGE VERSION: 5.0.1
- RECIPE NAME: gawk
- LICENSE: GPLv3

- PACKAGE NAME: gdb
- PACKAGE VERSION: 9.1
- RECIPE NAME: gdb
- LICENSE: GPLv2 & GPLv3 & LGPLv2 & LGPLv3

- PACKAGE NAME: gdbm
- PACKAGE VERSION: 1.18.1
- RECIPE NAME: gdbm
- LICENSE: GPLv3

- PACKAGE NAME: gdbm-compat
- PACKAGE VERSION: 1.18.1
- RECIPE NAME: gdbm
- LICENSE: GPLv3

- PACKAGE NAME: gdbserver
- PACKAGE VERSION: 9.1
- RECIPE NAME: gdb
- LICENSE: GPLv2 & GPLv3 & LGPLv2 & LGPLv3

- PACKAGE NAME: glib-2.0
- PACKAGE VERSION: 2.62.6
- RECIPE NAME: glib-2.0
- LICENSE: LGPLv2.1+ & BSD & PD

- PACKAGE NAME: glibc
- PACKAGE VERSION: 2.31+gitAUTOINC+f84949f1c4
- RECIPE NAME: glibc
- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: glibc-dbg
- PACKAGE VERSION: 2.31+gitAUTOINC+f84949f1c4
- RECIPE NAME: glibc
- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: glibc-thread-db
- PACKAGE VERSION: 2.31+gitAUTOINC+f84949f1c4
- RECIPE NAME: glibc

- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: gmp
- PACKAGE VERSION: 6.2.0
- RECIPE NAME: gmp
- LICENSE: GPLv2+ | LGPLv3+

- PACKAGE NAME: gnutls
- PACKAGE VERSION: 3.6.14
- RECIPE NAME: gnutls
- LICENSE: LGPLv2.1+

- PACKAGE NAME: grep
- PACKAGE VERSION: 3.4
- RECIPE NAME: grep
- LICENSE: GPLv3

- PACKAGE NAME: gzip
- PACKAGE VERSION: 1.10
- RECIPE NAME: gzip
- LICENSE: GPLv3+

- PACKAGE NAME: inetutils
- PACKAGE VERSION: 1.9.4
- RECIPE NAME: inetutils
- LICENSE: GPLv3

- PACKAGE NAME: inetutils-ping
- PACKAGE VERSION: 1.9.4
- RECIPE NAME: inetutils
- LICENSE: GPLv3

- PACKAGE NAME: inetutils-telnet
- PACKAGE VERSION: 1.9.4
- RECIPE NAME: inetutils
- LICENSE: GPLv3

- PACKAGE NAME: inetutils-telnetd
- PACKAGE VERSION: 1.9.4
- RECIPE NAME: inetutils
- LICENSE: GPLv3

- PACKAGE NAME: inetutils-tftp
- PACKAGE VERSION: 1.9.4
- RECIPE NAME: inetutils
- LICENSE: GPLv3

- PACKAGE NAME: inetutils-traceroute
- 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-functions

- PACKAGE VERSION: 1.0
- RECIPE NAME: initscripts
- LICENSE: GPLv2

- PACKAGE NAME: initscripts-microchip
- PACKAGE VERSION: 1.0
- RECIPE NAME: initscripts-microchip
- LICENSE: BSD

- PACKAGE NAME: ipdynaddrd
- PACKAGE VERSION: 1.1
- RECIPE NAME: ipdynaddrd
- LICENSE: BSD

- PACKAGE NAME: iperf2
- PACKAGE VERSION: 2.0.13
- RECIPE NAME: iperf2
- LICENSE: BSD-2-Clause

- PACKAGE NAME: iproute2
- PACKAGE VERSION: 5.5.0
- RECIPE NAME: iproute2
- LICENSE: GPLv2+

- PACKAGE NAME: iptables
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-ah
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-dnat
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-dnpt
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-dst
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-eui64
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-frag
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-hbh
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-hl
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-icmp6
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-ipv6header
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-log
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-masquerade
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-mh
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-netmap
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-redirect
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-reject
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-rt
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-snpt
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables

- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-srh
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ipt-ah
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ipt-clusterip
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ipt-dnat
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ipt-ecn
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ipt-icmp
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ipt-log
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ipt-masquerade
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ipt-netmap
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ipt-realm
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ipt-redirect
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ipt-reject

- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ipt-snat
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ipt-ttl
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ipt-ulog
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-addrtype
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-audit
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-bpf
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-cgroup
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-checksum
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-classify
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-cluster
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-comment
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-connbytes
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-connlimit
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-connmark
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-connsecmark
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-conntrack
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-cpu
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-ct
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-dccp
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-devgroup
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-dscp
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-ecn
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-esp
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables

- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-hashlimit
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-helper
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-hmark
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-idletimer
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-ipcomp
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-iprange
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-ipvs
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-led
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-length
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-limit
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-mac
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-mark

- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-multiport
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-nfacct
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-nflog
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-nfqueue
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-osf
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-owner
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-physdev
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-pkttype
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-policy
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-quota
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-rateest
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-recent
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-rpfilter
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-sctp
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-secmark
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-set
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-socket
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-standard
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-statistic
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-string
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-synproxy
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-tcp
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-tcpmss
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables

- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-tcpoptstrip
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-tee
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-time
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-tos
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-tproxy
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-trace
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-u32
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-udp
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iptables-modules
- PACKAGE VERSION: 1.8.4
- RECIPE NAME: iptables
- LICENSE: GPLv2+

- PACKAGE NAME: iputils
- PACKAGE VERSION: s20190709
- RECIPE NAME: iputils
- LICENSE: BSD & GPLv2+

- PACKAGE NAME: iputils-arping
- PACKAGE VERSION: s20190709
- RECIPE NAME: iputils
- LICENSE: BSD & GPLv2+

- PACKAGE NAME: iputils-clockdiff

- PACKAGE VERSION: s20190709
- RECIPE NAME: iputils
- LICENSE: BSD & GPLv2+

- PACKAGE NAME: iputils-ninfod
- PACKAGE VERSION: s20190709
- RECIPE NAME: iputils
- LICENSE: BSD & GPLv2+

- PACKAGE NAME: iputils-ping
- PACKAGE VERSION: s20190709
- RECIPE NAME: iputils
- LICENSE: BSD & GPLv2+

- PACKAGE NAME: iputils-rarpd
- PACKAGE VERSION: s20190709
- RECIPE NAME: iputils
- LICENSE: BSD & GPLv2+

- PACKAGE NAME: iputils-rdisc
- PACKAGE VERSION: s20190709
- RECIPE NAME: iputils
- LICENSE: BSD & GPLv2+

- PACKAGE NAME: iputils-tftpd
- PACKAGE VERSION: s20190709
- RECIPE NAME: iputils
- LICENSE: BSD & GPLv2+

- PACKAGE NAME: iputils-tracepath
- PACKAGE VERSION: s20190709
- RECIPE NAME: iputils
- LICENSE: BSD & GPLv2+

- PACKAGE NAME: iputils-traceroute6
- PACKAGE VERSION: s20190709
- RECIPE NAME: iputils
- LICENSE: BSD & GPLv2+

- PACKAGE NAME: jqBarGraph.js
- LICENSE: Artistic/GPL, https://code.google.com/archive/p/jqbargraph/

- PACKAGE NAME: jquery.dataTables.*
- PACKAGE VERSION: 1.9.4
- LICENSE: MIT, https://datatables.net/faqs/index#Licensing

- PACKAGE NAME: jquery.easy-pie-chart.min.js
- PACKAGE VERSION: 1.6.2
- LICENSE: MIT, https://github.com/rendro/easy-pie-chart

- PACKAGE NAME: jquery.min.js
- PACKAGE VERSION: 3.6.0
- LICENSE: MIT, https://github.com/jquery/jquery/blob/main/LICENSE.txt

- PACKAGE NAME: jquery.mobile.custom.min.js
- PACKAGE VERSION: 1.3.1
- LICENSE: MIT, https://jquerymobile.com/about/

- PACKAGE NAME: jquery.slimscroll.min.js

- PACKAGE VERSION: 1.3.8
- LICENSE: MIT, https://github.com/rochal/jQuery-slimScroll

- PACKAGE NAME: jquery.sparkline.min.js
- PACKAGE VERSION: 2.1.2
- LICENSE: This plugin is copyright Splunk Inc and licensed using the New BSD License. https://omnipotent.net/jquery.sparkline/#s-docs

- PACKAGE NAME: jquery-ui-1.10.3.custom.min.js
- PACKAGE VERSION: 1.10.3
- LICENSE: MIT, https://jqueryui.com/download/all/

- PACKAGE NAME: jquery.ui.touch-punch.min.js
- PACKAGE VERSION: 0.2.2
- LICENSE: MIT/GPL License, https://cdnjs.com/libraries/jqueryui-touch-punch

- PACKAGE NAME: jsoncpp
- PACKAGE VERSION: 1.9.2
- RECIPE NAME: jsoncpp
- LICENSE: MIT

- PACKAGE NAME: k2-pythonadds
- PACKAGE VERSION: 1.0
- RECIPE NAME: k2-pythonadds
- LICENSE: CLOSED

- PACKAGE NAME: kbd
- PACKAGE VERSION: 2.2.0
- RECIPE NAME: kbd
- LICENSE: GPLv2+

- PACKAGE NAME: kbd-consolefonts
- PACKAGE VERSION: 2.2.0
- RECIPE NAME: kbd
- LICENSE: GPLv2+

- PACKAGE NAME: kbd-keymaps
- PACKAGE VERSION: 2.2.0
- RECIPE NAME: kbd
- LICENSE: GPLv2+

- PACKAGE NAME: kernel-base
- PACKAGE VERSION: 5.4.124-lts+gitAUTOINC+d8c0c60a53
- RECIPE NAME: linux-altera-lts
- LICENSE: GPLv2

- PACKAGE NAME: kernel-image
- PACKAGE VERSION: 5.4.124-lts+gitAUTOINC+d8c0c60a53
- RECIPE NAME: linux-altera-lts
- LICENSE: GPLv2

- PACKAGE NAME: kernel-image-zimage
- PACKAGE VERSION: 5.4.124-lts+gitAUTOINC+d8c0c60a53
- RECIPE NAME: linux-altera-lts
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-ansi-cprng-5.4.124-altera
- PACKAGE VERSION: 5.4.124-lts+gitAUTOINC+d8c0c60a53
- RECIPE NAME: linux-altera-lts

- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-g-mass-storage-5.4.124-altera
- PACKAGE VERSION: 5.4.124-lts+gitAUTOINC+d8c0c60a53
- RECIPE NAME: linux-altera-lts
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-gpio-altera-5.4.124-altera
- PACKAGE VERSION: 5.4.124-lts+gitAUTOINC+d8c0c60a53
- RECIPE NAME: linux-altera-lts
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-libcomposite-5.4.124-altera
- PACKAGE VERSION: 5.4.124-lts+gitAUTOINC+d8c0c60a53
- RECIPE NAME: linux-altera-lts
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rng-core-5.4.124-altera
- PACKAGE VERSION: 5.4.124-lts+gitAUTOINC+d8c0c60a53
- RECIPE NAME: linux-altera-lts
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-aux-serial-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-clock-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-csrs-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-eth-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-evt-timestamp-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-fan-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-gpio-5.4.124-altera

- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-heater-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-i2c-remote-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-keypad-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-netlink-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-pkteng-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-rb-serial-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-remote-card-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-serial-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-tdc-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-tod-serial-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-vfd-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-rwi-wdog-5.4.124-altera
- PACKAGE VERSION: 0.1
- RECIPE NAME: rwi-mod
- LICENSE: GPLv2

- PACKAGE NAME: kernel-module-usb-f-mass-storage-5.4.124-altera
- PACKAGE VERSION: 5.4.124-lts+gitAUTOINC+d8c0c60a53
- RECIPE NAME: linux-altera-lts
- LICENSE: GPLv2

- PACKAGE NAME: kernel-modules
- PACKAGE VERSION: 5.4.124-lts+gitAUTOINC+d8c0c60a53
- RECIPE NAME: linux-altera-lts
- LICENSE: GPLv2

- PACKAGE NAME: killall
- PACKAGE VERSION: 23.3
- RECIPE NAME: psmisc
- LICENSE: GPLv2

- PACKAGE NAME: kmod
- PACKAGE VERSION: 26
- RECIPE NAME: kmod
- LICENSE: GPL-2.0+ & LGPL-2.1+

- PACKAGE NAME: ldconfig
- PACKAGE VERSION: 2.31+gitAUTOINC+f84949f1c4
- RECIPE NAME: glibc
- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: ldd
- PACKAGE VERSION: 2.31+gitAUTOINC+f84949f1c4
- RECIPE NAME: glibc
- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: less
- PACKAGE VERSION: 551
- RECIPE NAME: less
- LICENSE: GPLv3+ | BSD-2-Clause

- PACKAGE NAME: libacl
- PACKAGE VERSION: 2.2.53
- RECIPE NAME: acl
- LICENSE: LGPLv2.1+

- PACKAGE NAME: libasm
- PACKAGE VERSION: 0.178
- RECIPE NAME: elfutils
- LICENSE: GPLv2 | LGPLv3+

- PACKAGE NAME: libattr
- PACKAGE VERSION: 2.4.48
- RECIPE NAME: attr
- LICENSE: LGPLv2.1+

- PACKAGE NAME: libbz2
- PACKAGE VERSION: 1.0.8
- RECIPE NAME: bzip2

- LICENSE: bzip2-1.0.6

- PACKAGE NAME: libcap
- PACKAGE VERSION: 2.32
- RECIPE NAME: libcap
- LICENSE: BSD | GPLv2

- PACKAGE NAME: libcap-ng
- PACKAGE VERSION: 0.7.10
- RECIPE NAME: libcap-ng
- LICENSE: GPLv2+ & LGPLv2.1+

- PACKAGE NAME: libcomerr
- PACKAGE VERSION: 1.45.4
- RECIPE NAME: e2fsprogs
- LICENSE: GPLv2 & LGPLv2 & BSD & MIT

- PACKAGE NAME: libcrypto
- PACKAGE VERSION: 1.1.1k
- RECIPE NAME: openssl
- LICENSE: openssl

- PACKAGE NAME: libcurl
- PACKAGE VERSION: 7.69.1
- RECIPE NAME: curl
- LICENSE: MIT

- PACKAGE NAME: libdw
- PACKAGE VERSION: 0.178
- RECIPE NAME: elfutils
- LICENSE: GPLv2 | LGPLv3+

- PACKAGE NAME: libe2p
- PACKAGE VERSION: 1.45.4
- RECIPE NAME: e2fsprogs
- LICENSE: GPLv2 & LGPLv2 & BSD & MIT

- PACKAGE NAME: libedit
- PACKAGE VERSION: 20191231-3.1
- RECIPE NAME: libedit
- LICENSE: BSD-3-Clause

- PACKAGE NAME: libelf
- PACKAGE VERSION: 0.178
- RECIPE NAME: elfutils
- LICENSE: GPLv2 | LGPLv3+

- PACKAGE NAME: libext2fs
- PACKAGE VERSION: 1.45.4
- RECIPE NAME: e2fsprogs
- LICENSE: GPLv2 & LGPLv2 & BSD & MIT

- PACKAGE NAME: libffi
- PACKAGE VERSION: 3.3
- RECIPE NAME: libffi
- LICENSE: MIT

- PACKAGE NAME: libgcc

- PACKAGE VERSION: 9.3.0
- RECIPE NAME: libgcc
- LICENSE: GPL-3.0-with-GCC-exception

- PACKAGE NAME: libgcrypt
- PACKAGE VERSION: 1.8.5
- RECIPE NAME: libgcrypt
- LICENSE: LGPLv2.1+

- PACKAGE NAME: libgpg-error
- PACKAGE VERSION: 1.37
- RECIPE NAME: libgpg-error
- LICENSE: GPLv2+ & LGPLv2.1+

- PACKAGE NAME: libicudata
- PACKAGE VERSION: 66.1
- RECIPE NAME: icu
- LICENSE: ICU

- PACKAGE NAME: libicui18n
- PACKAGE VERSION: 66.1
- RECIPE NAME: icu
- LICENSE: ICU

- PACKAGE NAME: libicuuc
- PACKAGE VERSION: 66.1
- RECIPE NAME: icu
- LICENSE: ICU

- PACKAGE NAME: libidn2
- PACKAGE VERSION: 2.3.0
- RECIPE NAME: libidn2
- LICENSE: (GPLv2+ | LGPLv3)

- PACKAGE NAME: libjitterentropy
- PACKAGE VERSION: 2.2.0
- RECIPE NAME: libjitterentropy
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: libkmod
- PACKAGE VERSION: 26
- RECIPE NAME: kmod
- LICENSE: LGPL-2.1+

- PACKAGE NAME: liblzma
- PACKAGE VERSION: 5.2.4
- RECIPE NAME: xz
- LICENSE: PD

- PACKAGE NAME: libmnl
- PACKAGE VERSION: 1.0.4
- RECIPE NAME: libmnl
- LICENSE: LGPLv2.1+

- PACKAGE NAME: libnetfilter-conntrack
- PACKAGE VERSION: 1.0.8
- 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: 1.0.3
- RECIPE NAME: libnetfilter-queue
- LICENSE: GPLv2+

- PACKAGE NAME: libnfnetlink
- PACKAGE VERSION: 1.0.1
- RECIPE NAME: libnfnetlink
- LICENSE: GPLv2+

- PACKAGE NAME: libnsl2
- PACKAGE VERSION: 1.2.0+gitAUTOINC+4a062cf418
- RECIPE NAME: libnsl2
- LICENSE: LGPL-2.1

- PACKAGE NAME: libnss-myhostname
- PACKAGE VERSION: 244.5
- RECIPE NAME: systemd
- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: libpam
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: libpam-runtime
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: libpcap
- PACKAGE VERSION: 1.9.1
- RECIPE NAME: libpcap
- LICENSE: BSD-3-Clause

- PACKAGE NAME: libpci
- PACKAGE VERSION: 3.6.4
- RECIPE NAME: pciutils
- LICENSE: GPLv2+

- PACKAGE NAME: libpcre
- PACKAGE VERSION: 8.44
- RECIPE NAME: libpcre
- LICENSE: BSD-3-Clause

- PACKAGE NAME: libpq
- PACKAGE VERSION: 12.7
- RECIPE NAME: postgresql

- LICENSE: BSD-0-Clause

- PACKAGE NAME: libpython2
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: libpython3
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: libsqlite3
- PACKAGE VERSION: 3.31.1
- RECIPE NAME: sqlite3
- LICENSE: PD

- PACKAGE NAME: libss
- PACKAGE VERSION: 1.45.4
- RECIPE NAME: e2fsprogs
- LICENSE: GPLv2 & LGPLv2 & BSD & MIT

- PACKAGE NAME: libssl
- PACKAGE VERSION: 1.1.1k
- RECIPE NAME: openssl
- LICENSE: openssl

- PACKAGE NAME: libstdc++
- PACKAGE VERSION: 9.3.0
- 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: 244.5
- RECIPE NAME: systemd
- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: libtirpc
- PACKAGE VERSION: 1.2.6
- RECIPE NAME: libtirpc
- LICENSE: BSD-3-Clause

- PACKAGE NAME: libudev
- PACKAGE VERSION: 244.5
- RECIPE NAME: systemd
- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: libulockmgr
- PACKAGE VERSION: 2.9.9
- RECIPE NAME: fuse
- LICENSE: GPLv2 & LGPLv2

- PACKAGE NAME: libunistring

- PACKAGE VERSION: 0.9.10
- RECIPE NAME: libunistring
- LICENSE: LGPLv3+ | GPLv2

- PACKAGE NAME: libuv
- PACKAGE VERSION: 1.36.0
- RECIPE NAME: libuv
- LICENSE: MIT

- PACKAGE NAME: libwebsockets
- PACKAGE VERSION: 4.0.1
- RECIPE NAME: libwebsockets
- LICENSE: MIT & Zlib & BSD-3-Clause

- PACKAGE NAME: libwrap
- PACKAGE VERSION: 7.6
- RECIPE NAME: tcp-wrappers
- LICENSE: BSD-1-Clause

- PACKAGE NAME: libxcrypt
- PACKAGE VERSION: 4.4.15
- RECIPE NAME: libxcrypt
- LICENSE: LGPLv2.1

- PACKAGE NAME: libxerces-c
- PACKAGE VERSION: 3.1.4
- RECIPE NAME: xerces-c
- LICENSE: Apache-2.0

- PACKAGE NAME: libxml2
- PACKAGE VERSION: 2.9.10
- RECIPE NAME: libxml2
- LICENSE: MIT

- PACKAGE NAME: libxml2-utils
- PACKAGE VERSION: 2.9.10
- RECIPE NAME: libxml2
- LICENSE: MIT

- PACKAGE NAME: logrotate
- PACKAGE VERSION: 3.15.1
- RECIPE NAME: logrotate
- LICENSE: GPLv2

- PACKAGE NAME: ltrace
- PACKAGE VERSION: 7.91+gitAUTOINC+c22d359433
- RECIPE NAME: ltrace
- LICENSE: GPLv2

- PACKAGE NAME: microchip-app
- PACKAGE VERSION: 0.1
- RECIPE NAME: microchip-app
- LICENSE: BSD

- PACKAGE NAME: microchip-misc
- PACKAGE VERSION: 1.0
- RECIPE NAME: microchip-misc
- LICENSE: GPLv2

- PACKAGE NAME: modernizer.js
- PACKAGE VERSION: 1.7
- LICENSE: MIT, https://modernizr.com/license/

- PACKAGE NAME: msmtp
- PACKAGE VERSION: 1.4.33
- LICENSE: GPLv3

- PACKAGE NAME: msmtp
- PACKAGE VERSION: 1.8.7
- RECIPE NAME: msmtp
- LICENSE: GPLv3

- PACKAGE NAME: mtd-utils
- PACKAGE VERSION: 2.1.1
- RECIPE NAME: mtd-utils
- LICENSE: GPLv2+

- PACKAGE NAME: ncurses
- PACKAGE VERSION: 6.2
- RECIPE NAME: ncurses
- LICENSE: MIT

- PACKAGE NAME: ncurses-libncurses
- PACKAGE VERSION: 6.2
- RECIPE NAME: ncurses
- LICENSE: MIT

- PACKAGE NAME: ncurses-libncursesw
- PACKAGE VERSION: 6.2
- RECIPE NAME: ncurses
- LICENSE: MIT

- PACKAGE NAME: ncurses-libpanelw
- PACKAGE VERSION: 6.2
- RECIPE NAME: ncurses
- LICENSE: MIT

- PACKAGE NAME: ncurses-libtic
- PACKAGE VERSION: 6.2
- RECIPE NAME: ncurses
- LICENSE: MIT

- PACKAGE NAME: ncurses-libtinfo
- PACKAGE VERSION: 6.2
- RECIPE NAME: ncurses
- LICENSE: MIT

- PACKAGE NAME: ncurses-terminfo-base
- PACKAGE VERSION: 6.2
- RECIPE NAME: ncurses
- LICENSE: MIT

- PACKAGE NAME: ncurses-tools
- PACKAGE VERSION: 6.2
- RECIPE NAME: ncurses
- LICENSE: MIT

- PACKAGE NAME: net-tools
- PACKAGE VERSION: 1.60-26
- RECIPE NAME: net-tools
- LICENSE: GPLv2+

- PACKAGE NAME: netbase
- PACKAGE VERSION: 6.1
- RECIPE NAME: netbase
- LICENSE: GPLv2

- PACKAGE NAME: net-snmp
- PACKAGE VERSION: 5.9
- LICENSE: BSD

- PACKAGE NAME: nettle
- PACKAGE VERSION: 3.5.1
- RECIPE NAME: nettle
- LICENSE: LGPLv3+ | GPLv2+

- PACKAGE NAME: network-scripts
- PACKAGE VERSION: 1.0
- RECIPE NAME: network-scripts
- LICENSE: BSD

- PACKAGE NAME: NTP
- PACKAGE VERSION: 4.2.8p15
- LICENSE: BSD like

- PACKAGE NAME: openldap
- PACKAGE VERSION: 2.4.57
- RECIPE NAME: openldap
- LICENSE: OpenLDAP

- PACKAGE NAME: openssh
- PACKAGE VERSION: 8.2p1
- RECIPE NAME: openssh
- LICENSE: BSD & ISC & MIT

- PACKAGE NAME: openssh-keygen
- PACKAGE VERSION: 8.2p1
- RECIPE NAME: openssh
- LICENSE: BSD & ISC & MIT

- PACKAGE NAME: openssh-scp
- PACKAGE VERSION: 8.2p1
- RECIPE NAME: openssh
- LICENSE: BSD & ISC & MIT

- PACKAGE NAME: openssh-sftp-server
- PACKAGE VERSION: 8.2p1
- RECIPE NAME: openssh
- LICENSE: BSD & ISC & MIT

- PACKAGE NAME: openssh-ssh
- PACKAGE VERSION: 8.2p1
- RECIPE NAME: openssh
- LICENSE: BSD & ISC & MIT

- PACKAGE NAME: openssh-sshd
- PACKAGE VERSION: 8.2p1
- RECIPE NAME: openssh
- LICENSE: BSD & ISC & MIT

- PACKAGE NAME: openssl
- PACKAGE VERSION: 1.1.1k
- RECIPE NAME: openssl
- LICENSE: openssl

- PACKAGE NAME: openssl-bin
- PACKAGE VERSION: 1.1.1k
- RECIPE NAME: openssl
- LICENSE: openssl

- PACKAGE NAME: openssl-conf
- PACKAGE VERSION: 1.1.1k
- RECIPE NAME: openssl
- LICENSE: openssl

- PACKAGE NAME: os-release
- PACKAGE VERSION: 1.0
- RECIPE NAME: os-release
- LICENSE: MIT

- PACKAGE NAME: packagegroup-core-base-utils
- PACKAGE VERSION: 1.0
- RECIPE NAME: packagegroup-core-base-utils
- LICENSE: MIT

- PACKAGE NAME: packagegroup-core-boot
- PACKAGE VERSION: 1.0
- RECIPE NAME: packagegroup-core-boot
- LICENSE: MIT

- PACKAGE NAME: packagegroup-core-utils
- PACKAGE VERSION: 1.0
- RECIPE NAME: packagegroup-core-utils
- LICENSE: MIT

- PACKAGE NAME: packagegroup-database
- PACKAGE VERSION: 1.0
- RECIPE NAME: packagegroup-database
- LICENSE: MIT

- PACKAGE NAME: packagegroup-libs
- PACKAGE VERSION: 1.0
- RECIPE NAME: packagegroup-libs
- LICENSE: MIT

- PACKAGE NAME: packagegroup-network-utils
- PACKAGE VERSION: 1.0
- RECIPE NAME: packagegroup-network-utils
- LICENSE: MIT

- PACKAGE NAME: packagegroup-pkgs
- PACKAGE VERSION: 1.0
- RECIPE NAME: packagegroup-pkgs

- LICENSE: MIT

- PACKAGE NAME: packagegroup-python
- PACKAGE VERSION: 1.0
- RECIPE NAME: packagegroup-python
- LICENSE: MIT

- PACKAGE NAME: packagegroup-python2
- PACKAGE VERSION: 1.0
- RECIPE NAME: packagegroup-python2
- LICENSE: MIT

- PACKAGE NAME: packagegroup-support-apps
- PACKAGE VERSION: 1.0
- RECIPE NAME: packagegroup-support-apps
- LICENSE: MIT

- PACKAGE NAME: packagegroup-tzdata
- PACKAGE VERSION: 1.0
- RECIPE NAME: packagegroup-tzdata
- LICENSE: MIT

- PACKAGE NAME: packagegroup-webserver
- PACKAGE VERSION: 1.0
- RECIPE NAME: packagegroup-webserver
- LICENSE: MIT

- PACKAGE NAME: pam_ldap
- PACKAGE VERSION: 186
- LICENSE: GPLv2

- PACKAGE NAME: pam-plugin-access
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-deny
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-env
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-faildelay
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-group
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-keyinit
- PACKAGE VERSION: 1.3.1

- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-lastlog
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-limits
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-loginuid
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-mail
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-motd
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-nologin
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-permit
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-rootok
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-securetty
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-shells
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-succeed-if
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-tally2
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-unix
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam-plugin-warn
- PACKAGE VERSION: 1.3.1
- RECIPE NAME: libpam
- LICENSE: GPLv2+ | BSD

- PACKAGE NAME: pam_radius
- PACKAGE VERSION: 1.3.17
- LICENSE: GPLv2

- PACKAGE NAME: pam_tacplus
- PACKAGE VERSION: 1.3.8
- LICENSE: GPLv2

- PACKAGE NAME: parted
- PACKAGE VERSION: 3.3
- RECIPE NAME: parted
- LICENSE: GPLv3+

- PACKAGE NAME: patch
- PACKAGE VERSION: 2.7.6
- RECIPE NAME: patch
- LICENSE: GPLv3

- PACKAGE NAME: perl
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-carp
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-config-heavy
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-constant
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-cwd
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-dynaloader
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-errno
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-exporter
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-exporter-heavy
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-fcntl
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-file-basename
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-file-find
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-file-path
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-file-spec
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-file-spec-unix
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-file-temp
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-getopt-long
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl

- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-io
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-io-file
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-io-handle
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-io-seekable
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-list-util
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-mro
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-overload
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-overload-numbers
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-overloading
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-parent
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-pod-usage
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-posix

- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-re
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-scalar-util
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-selectsaver
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-symbol
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-term-cap
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-text-parsewords
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-tie-hash
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-xsloader
- PACKAGE VERSION: 5.30.1
- RECIPE NAME: perl
- LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: php
- PACKAGE VERSION: 7.4.21
- RECIPE NAME: php
- LICENSE: PHP-3.0

- PACKAGE NAME: php-cgi
- PACKAGE VERSION: 7.4.21
- RECIPE NAME: php
- LICENSE: PHP-3.0

- PACKAGE NAME: php-cli
- PACKAGE VERSION: 7.4.21
- RECIPE NAME: php
- LICENSE: PHP-3.0

- PACKAGE NAME: popt
- PACKAGE VERSION: 1.16
- RECIPE NAME: popt
- LICENSE: MIT

- PACKAGE NAME: postgresql
- PACKAGE VERSION: 12.7
- RECIPE NAME: postgresql
- LICENSE: BSD-0-Clause

- PACKAGE NAME: postgresql-client
- PACKAGE VERSION: 12.7
- RECIPE NAME: postgresql
- LICENSE: BSD-0-Clause

- PACKAGE NAME: postgresql-timezone
- PACKAGE VERSION: 12.7
- RECIPE NAME: postgresql
- LICENSE: BSD-0-Clause

- PACKAGE NAME: prettify.js
- LICENSE: None found

- PACKAGE NAME: procps
- PACKAGE VERSION: 3.3.16
- RECIPE NAME: procps
- LICENSE: GPLv2+ & LGPLv2+

- PACKAGE NAME: psmisc
- PACKAGE VERSION: 23.3
- RECIPE NAME: psmisc
- LICENSE: GPLv2

- PACKAGE NAME: pstree
- PACKAGE VERSION: 23.3
- RECIPE NAME: psmisc
- LICENSE: GPLv2

- PACKAGE NAME: python-2to3
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-argparse
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-audio
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-bsddb
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-codecs
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-compile
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-compiler
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-compression
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-contextlib
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-core
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-crypt
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-ctypes
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-curses
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-datetime
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-db
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-debugger
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python

- LICENSE: PSFv2

- PACKAGE NAME: python-difflib
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-distutils
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-doctest
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-email
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-fcntl
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-gdbm
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-hotshot
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-html
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-idle
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-image
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-io
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-json

- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-lang
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-logging
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-mailbox
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-math
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-mime
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-misc
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-mmap
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-modules
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-multiprocessing
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-netclient
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-netserver
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-numbers
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-pickle
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-pkgutil
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-plistlib
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-pprint
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-profile
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-pydoc
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-re
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-resource
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-robotparser
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-runpy
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-shell
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python

- LICENSE: PSFv2

- PACKAGE NAME: python-smtpd
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-sqlite3
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-stringold
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-subprocess
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-syslog
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-terminal
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-textutils
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-threading
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-tkinter
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-unittest
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-unixadmin
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-xml

- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-xmlrpc
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python-zlib
- PACKAGE VERSION: 2.7.18
- RECIPE NAME: python
- LICENSE: PSFv2

- PACKAGE NAME: python3-2to3
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-asyncio
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-audio
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-codecs
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-compile
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-compression
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-core
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-crypt
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-ctypes
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-curses
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-datetime
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-db
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-debugger
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-difflib
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-distutils
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-doctest
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-email
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-fcntl
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-html
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-idle
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-image
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3

- LICENSE: PSFv2

- PACKAGE NAME: python3-io
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-json
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-logging
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-mailbox
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-math
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-mime
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-misc
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-mmap
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-modules
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-multiprocessing
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-netclient
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-netserver

- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-numbers
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-pickle
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-pkgutil
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-plistlib
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-pprint
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-profile
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-pydoc
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-resource
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-shell
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-smtpd
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-sqlite3
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-stringold
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-syslog
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-terminal
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-threading
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-tkinter
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-typing
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-unittest
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-unixadmin
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-venv
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-xml
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: python3-xmlrpc
- PACKAGE VERSION: 3.8.2
- RECIPE NAME: python3
- LICENSE: PSFv2

- PACKAGE NAME: readline
- PACKAGE VERSION: 8.0
- RECIPE NAME: readline

- LICENSE: GPLv3+

- PACKAGE NAME: rng-tools
- PACKAGE VERSION: 6.9
- RECIPE NAME: rng-tools
- LICENSE: GPLv2

- 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: 4.8
- RECIPE NAME: sed
- LICENSE: GPLv3+

- PACKAGE NAME: shadow
- PACKAGE VERSION: 4.8.1
- RECIPE NAME: shadow
- LICENSE: BSD | Artistic-1.0

- PACKAGE NAME: shadow-base
- PACKAGE VERSION: 4.8.1
- RECIPE NAME: shadow
- LICENSE: BSD | Artistic-1.0

- PACKAGE NAME: shadow-securetty
- PACKAGE VERSION: 4.6
- RECIPE NAME: shadow-securetty
- LICENSE: MIT

- PACKAGE NAME: shared-mime-info
- PACKAGE VERSION: 1.15
- RECIPE NAME: shared-mime-info
- LICENSE: GPLv2

- PACKAGE NAME: sipcalc
- PACKAGE VERSION: 1.1.6
- RECIPE NAME: sipcalc
- LICENSE: BSD

- PACKAGE NAME: Smarty
- PACKAGE VERSION: 3.1.39
- LICENSE: LGPLv3

- PACKAGE NAME: smarty
- PACKAGE VERSION: 3.1.39
- RECIPE NAME: smarty
- LICENSE: GPL

- PACKAGE NAME: sqlite3
- PACKAGE VERSION: 3.31.1

- RECIPE NAME: sqlite3
- LICENSE: PD

- PACKAGE NAME: sshfs-fuse
- PACKAGE VERSION: 3.7.0
- RECIPE NAME: sshfs-fuse
- LICENSE: GPLv2

- PACKAGE NAME: strace
- PACKAGE VERSION: 5.5
- RECIPE NAME: strace
- LICENSE: LGPL-2.1+ & GPL-2+

- PACKAGE NAME: sudo
- PACKAGE VERSION: 1.8.32
- RECIPE NAME: sudo
- LICENSE: ISC & BSD & Zlib

- PACKAGE NAME: sysfsutils
- PACKAGE VERSION: 2.1.0
- RECIPE NAME: sysfsutils
- LICENSE: GPLv2

- PACKAGE NAME: syslog-ng
- PACKAGE VERSION: 3.24.1
- RECIPE NAME: syslog-ng
- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: syslog-ng-libs
- PACKAGE VERSION: 3.24.1
- RECIPE NAME: syslog-ng
- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: systemd
- PACKAGE VERSION: 244.5
- RECIPE NAME: systemd
- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: systemd-analyze
- PACKAGE VERSION: 244.5
- RECIPE NAME: systemd
- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: systemd-compat-units
- PACKAGE VERSION: 1.0
- RECIPE NAME: systemd-compat-units
- LICENSE: MIT

- PACKAGE NAME: systemd-conf
- PACKAGE VERSION: 244.3
- RECIPE NAME: systemd-conf
- LICENSE: MIT

- PACKAGE NAME: systemd-extra-utils
- PACKAGE VERSION: 244.5
- RECIPE NAME: systemd
- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: systemd-serialgetty
- PACKAGE VERSION: 1.0
- RECIPE NAME: systemd-serialgetty
- LICENSE: GPLv2+

- PACKAGE NAME: systemd-vconsole-setup
- PACKAGE VERSION: 244.5
- RECIPE NAME: systemd
- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: tar
- PACKAGE VERSION: 1.32
- RECIPE NAME: tar
- LICENSE: GPLv3

- PACKAGE NAME: tcl
- PACKAGE VERSION: 8.6.10
- RECIPE NAME: tcl
- LICENSE: tcl & BSD-3-Clause

- PACKAGE NAME: tcl-lib
- PACKAGE VERSION: 8.6.10
- RECIPE NAME: tcl
- LICENSE: tcl & BSD-3-Clause

- PACKAGE NAME: tcpdump
- PACKAGE VERSION: 4.9.3
- RECIPE NAME: tcpdump
- LICENSE: BSD-3-Clause

- PACKAGE NAME: time
- PACKAGE VERSION: 1.9
- RECIPE NAME: time
- LICENSE: GPLv3

- PACKAGE NAME: tzcode
- PACKAGE VERSION: 2.31+gitAUTOINC+f84949f1c4
- RECIPE NAME: glibc
- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: tzdata
- PACKAGE VERSION: 2021a
- RECIPE NAME: tzdata
- LICENSE: PD & BSD & BSD-3-Clause

- PACKAGE NAME: tzdata-africa
- PACKAGE VERSION: 2021a
- RECIPE NAME: tzdata
- LICENSE: PD & BSD & BSD-3-Clause

- PACKAGE NAME: tzdata-americas
- PACKAGE VERSION: 2021a
- RECIPE NAME: tzdata
- LICENSE: PD & BSD & BSD-3-Clause

- PACKAGE NAME: tzdata-antarctica
- PACKAGE VERSION: 2021a
- RECIPE NAME: tzdata

- LICENSE: PD & BSD & BSD-3-Clause

- PACKAGE NAME: tzdata-arctic
- PACKAGE VERSION: 2021a
- RECIPE NAME: tzdata
- LICENSE: PD & BSD & BSD-3-Clause

- PACKAGE NAME: tzdata-asia
- PACKAGE VERSION: 2021a
- RECIPE NAME: tzdata
- LICENSE: PD & BSD & BSD-3-Clause

- PACKAGE NAME: tzdata-atlantic
- PACKAGE VERSION: 2021a
- RECIPE NAME: tzdata
- LICENSE: PD & BSD & BSD-3-Clause

- PACKAGE NAME: tzdata-australia
- PACKAGE VERSION: 2021a
- RECIPE NAME: tzdata
- LICENSE: PD & BSD & BSD-3-Clause

- PACKAGE NAME: tzdata-core
- PACKAGE VERSION: 2021a
- RECIPE NAME: tzdata
- LICENSE: PD & BSD & BSD-3-Clause

- PACKAGE NAME: tzdata-europe
- PACKAGE VERSION: 2021a
- RECIPE NAME: tzdata
- LICENSE: PD & BSD & BSD-3-Clause

- PACKAGE NAME: tzdata-misc
- PACKAGE VERSION: 2021a
- RECIPE NAME: tzdata
- LICENSE: PD & BSD & BSD-3-Clause

- PACKAGE NAME: tzdata-pacific
- PACKAGE VERSION: 2021a
- RECIPE NAME: tzdata
- LICENSE: PD & BSD & BSD-3-Clause

- PACKAGE NAME: tzdata-posix
- PACKAGE VERSION: 2021a
- RECIPE NAME: tzdata
- LICENSE: PD & BSD & BSD-3-Clause

- PACKAGE NAME: tzdata-right
- PACKAGE VERSION: 2021a
- RECIPE NAME: tzdata
- LICENSE: PD & BSD & BSD-3-Clause

- PACKAGE NAME: udev
- PACKAGE VERSION: 244.5
- RECIPE NAME: systemd
- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: udev-hwdb

- PACKAGE VERSION: 244.5
- RECIPE NAME: systemd
- LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: unzip
- PACKAGE VERSION: 6.0
- RECIPE NAME: unzip
- LICENSE: BSD-3-Clause

- PACKAGE NAME: update-alternatives-opkg
- PACKAGE VERSION: 0.4.2
- RECIPE NAME: opkg-utils
- LICENSE: GPLv2+

- PACKAGE NAME: update-rc.d
- PACKAGE VERSION: 0.8
- RECIPE NAME: update-rc.d
- LICENSE: GPLv2+

- PACKAGE NAME: util-linux
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-addpart
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-agetty
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-blkdiscard
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-blkid
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-blkzone
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-blockdev
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-cal
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-cfdisk
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-chcpu
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-chmem
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-choom
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-chrt
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-col
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-colcrt
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-colrm
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-column
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-ctrlaltdel
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-delpart
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-dmesg
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux

- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-eject
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-fallocate
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-fdformat
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-fdisk
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-fincore
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-findfs
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-findmnt
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-flock
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-fsck
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-fsck.cramfs
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-fsfreeze
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-fstrim

- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-getopt
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-hardlink
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-hexdump
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-hwclock
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-ionice
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-ipcmk
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-ipcrm
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-ipcs
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-isosize
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-kill
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-last
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-ldattach
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-libblkid
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-libfdisk
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-libmount
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-libsmartcols
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-libuuid
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-logger
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-look
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-losetup
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-lsblk
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-lscpu
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-lsipc
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux

- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-lslocks
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-lslogins
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-lsmem
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-lsns
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-mcookie
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-mesg
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-mkfs
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-mkfs.cramfs
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-mkswap
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-more
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-mount
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-mountpoint

- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-namei
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-nologin
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-nsenter
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-partx
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-pivot-root
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-prlimit
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-raw
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-readprofile
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-rename
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-renice
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-resizepart
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-rev
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-rfkill
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-rtcwake
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-runuser
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-script
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-scriptlive
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-scriptreplay
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-setarch
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-setpriv
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-setsid
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-setterm
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-sfdisk
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux

- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-su
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-sulogin
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-swaplabel
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-swapoff
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-swapon
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-switch-root
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-taskset
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-ul
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-umount
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-unshare
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-utmpdump
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-uuidd

- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-uuidgen
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-uuidparse
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-wall
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-wdctl
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-whereis
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-wipefs
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-write
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: util-linux-zramctl
- PACKAGE VERSION: 2.35.1
- RECIPE NAME: util-linux
- LICENSE: GPLv2+ & LGPLv2.1+ & BSD-3-Clause & BSD-4-Clause

- PACKAGE NAME: valgrind
- PACKAGE VERSION: 3.15.0
- 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: which
- PACKAGE VERSION: 2.21
- RECIPE NAME: which
- LICENSE: GPLv3+

- PACKAGE NAME: xerces-c
- PACKAGE VERSION: 3.1.4
- RECIPE NAME: xerces-c
- LICENSE: Apache-2.0

- PACKAGE NAME: xinetd
- PACKAGE VERSION: 2.3.15
- RECIPE NAME: xinetd
- LICENSE: BSD

- PACKAGE NAME: xz
- PACKAGE VERSION: 5.2.4
- RECIPE NAME: xz
- LICENSE: GPLv2+

- PACKAGE NAME: zlib
- PACKAGE VERSION: 1.2.11
- RECIPE NAME: zlib
- LICENSE: Zlib

12. Port Details

This section provides port information of the SyncServer device.

12.1 Ethernet Port Electrical

By design, SyncServer network ports are galvanically isolated.

12.2 Ethernet Port Isolation

SyncServer S600 Series Network Time Servers have four Ethernet ports. These independent ports allow SyncServer to connect to distinct Ethernet subnets. There is only one CPU in SyncServer, so all of the Ethernet traffic, with the exception of NTP Reflector and PTP server traffic, is ultimately handled by the protocol stack of the operating system.

SyncServer uses the operating system IP packet filtering facilities to secure SyncServer from unwanted access. It also creates rules to filter IP packets based on the pre-assigned role of each Ethernet port. 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, 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: The rules allow inbound packets only. The outbound packets that are part of the session are allowed to go out of the port.

12.4 Timing Port Rules

The 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

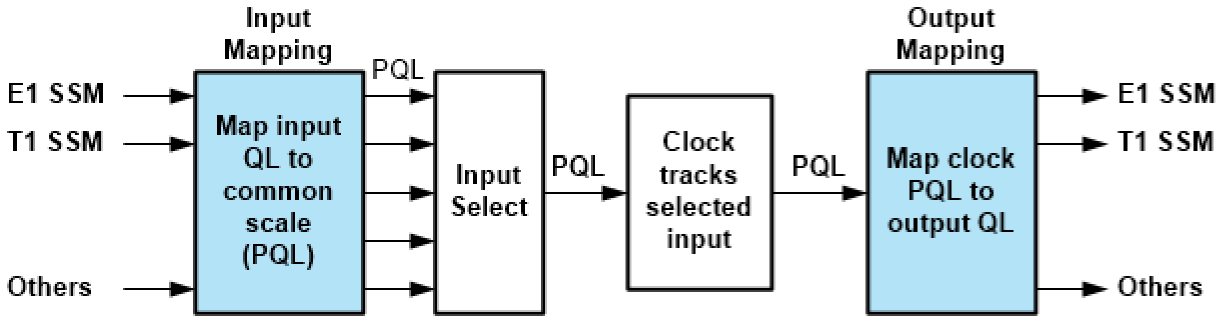
This section provides the PQL mapping details of the SyncServer device.

13.1 Purpose of Input and Output Mapping Tables

When SyncServer S6x0 has 1 or 2 Timing I/O modules with Telecom I/O Connections (090-15201-011), then 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” is the frequency “on the wire”. E1 and T1 frequency references have a long history of support for SSM, but as they do not 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 that 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 figure shows the overall end-to-end process.

Reference inputs might use different scales for quality level. At the input, these different scales of quality level are mapped to a common scale called Priority Quality Level (PQL). 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 only uses PQL as the quality indicator. See 13.2. PQL Input Mapping for PQL mapping of frequency inputs.

Figure 13-1. PQL Input and Output Mapping


Input Mapping
E1 SSM
T1 SSM
Others
Map input QL to common scale (PQL)
PQL
Input Select
PQL
Clock tracks selected input
PQL
Output Mapping
Map clock PQL to output QL
E1 SSM
T1 SSM
Others

13.1.1 E1 and T1 Signals That Embed SSM

For E1 configurations, they all support embedded SSM except for the following:

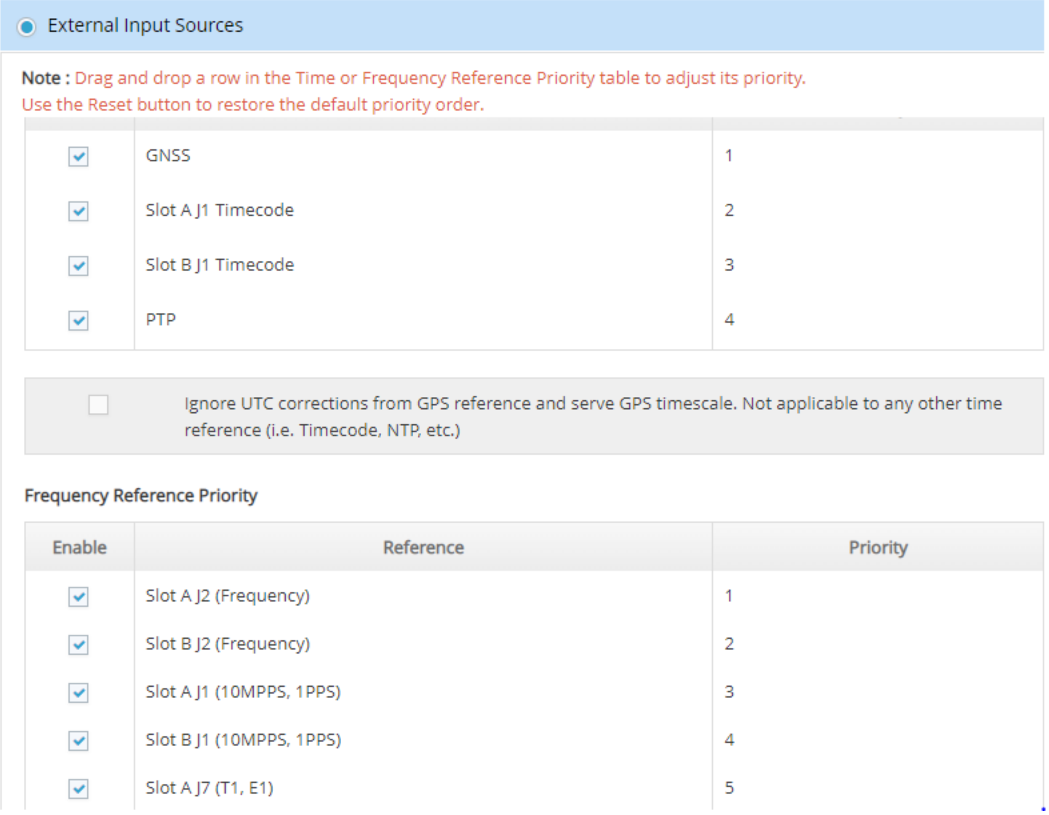
- CAS or CCS frame types with CRC state disabled
- 2.048 MHz SquareWave

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 S6xx, the SSM content is expected and processed as described.

Note: 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



● External Input Sources

Note : Drag and drop a row in the Time or Frequency Reference Priority table to adjust its priority.
Use the Reset button to restore the default priority order.

☑	GNSS	1
☑	Slot A J1 Timecode	2
☑	Slot B J1 Timecode	3
☑	PTP	4

☐ Ignore UTC corrections from GPS reference and serve GPS timescale. Not applicable to any other time reference (i.e. Timecode, NTP, etc.)

Frequency Reference Priority

Enable	Reference	Priority
☑	Slot A J2 (Frequency)	1
☑	Slot B J2 (Frequency)	2
☑	Slot A J1 (10MPPS, 1PPS)	3
☑	Slot B J1 (10MPPS, 1PPS)	4
☑	Slot A J7 (T1, E1)	5

Following are the steps to process the SSM-capable inputs:

1. The SSM value is extracted from the input.
   If it is an E1 signal, then the legal SSM encodings are as per the left column of Table 13-4. Each of these have a mapping to an internal-use-only PQL value, as shown in the rightmost column of Table 13-4. For example, if 0x4 is decoded on the input, it results in PQL = 6. 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, as 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 of Table 13-5.

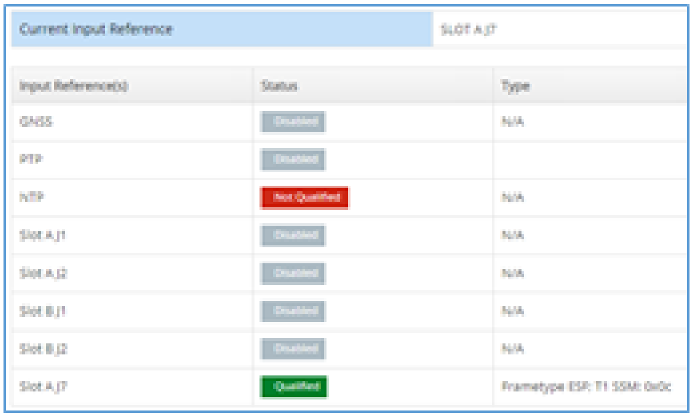
   For any of these signals, if an illegal SSM code is read (anything not in the associated table) then the input is not qualified for use (it remains in red on `Dashboard > Timing, Frequency References` row).
2. Considering that an SSM code is actually being read from the input, that value is shown on the `References > Status` form. Look for the row labeled slot A J7 (or Slot B J7). The Type column summarizes the input signal configuration and show the SSM value. If J7 has been configured as an output, then this is also shown to help with the 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 Table 13-1, a simple decision is made: If the input PQL is a larger number than the internal oscillator PQL, then the input is not 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 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 only use the internal reference and reject the candidate reference.
    If the candidate input is rejected due to failure of this comparison test, it remains red on `Dashboard > Timing frequency references` row, indicating that it is not qualified for use.

    Ensure that the input SSM is continually being read, so if the SSM value from the candidate improves, this reference can become qualified. The process is dynamic.

3. Assuming the candidate reference is not rejected by the prior step, then it can become qualified (it is shown in green on `Dashboard > Timing frequency references` row). For simplicity of this explanation, consider that the T1 or E1 SSM-capable reference is the only external candidate reference being provided. In this case, it is not only qualified for use (that is, it can be selected from the pool of qualified candidates), it is actually selected as the frequency reference for S6xx.
4. To follow the complete SSM input-to-output path, we can 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, as shown in the following figure, the configuration of the J7 input and 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 the 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



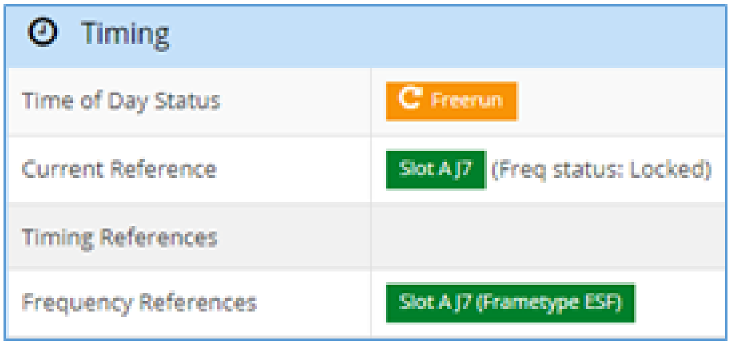
Current Input Reference	SLOT A J7

Input Reference(s)	Status	Type
GNSS	Disabled	N/A
PTP	Disabled	
NTP	Not Qualified	N/A
Slot A J1	Disabled	N/A
Slot A J2	Disabled	N/A
Slot B J1	Disabled	N/A
Slot B J2	Disabled	N/A
Slot A J7	Qualified	Frametype ESF: T1 SSM: 0x0c

- The form does not self-update this status. To ensure that the 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. As there is no time-reference into the system, the ToD Status remains in freerun.

Figure 13-4. S6xx Frequency Locked to T1 ESF Input on Slot A J7



Timing

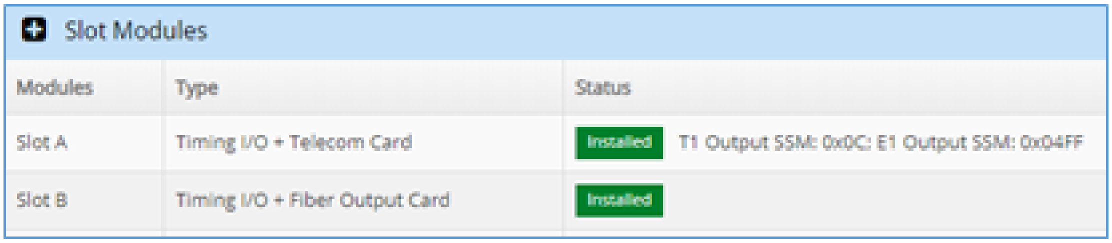
Time of Day Status	Freerun
Current Reference	Slot A J7 (Freq status: Locked)
Timing References	
Frequency References	Slot A J7 (Frametype ESF)

Use Table 13-6 and Table 13-7 to identify the SSM values that are encoded onto E1 or T1 outputs (if they are capable of encoding SSM). As the PQL level of the current reference is already identified as 4, 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 is 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.

S6xx performs this conversion automatically and displays these values on the `Dashboard > Slot Modules` form. As shown, when S6xx contains a telecom module, the T1 and E1 current output SSM values are always shown here, even if there are currently no actual outputs of this type being generated. The values match what was determined from the tables.

Note: T1 must have the appended “FF”, not the E1 that is shown in the form but the actual outputs are encoded correctly.

Figure 13-5. Dashboard > Slot Modules Always Show T1 and E1 Output SSM Encodings



Slot Modules

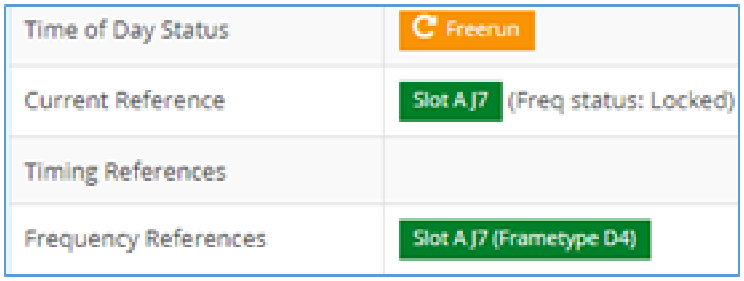
Modules	Type	Status
Slot A	Timing I/O + Telecom Card	Installed T1 Output SSM: 0x0C: E1 Output SSM: 0x04FF
Slot B	Timing I/O + Fiber Output Card	Installed

13.1.2 Frequency References That do not 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, as 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 the same way as the prior section, except for these non-SSM inputs, the PQL value is always assigned the value 1, which is equivalent to considering that this is the best possible frequency quality. From there, the mapping process is identical. Following is 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.

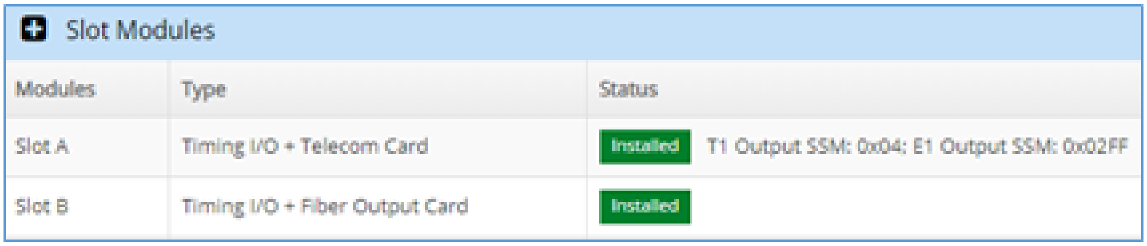
Figure 13-6. Using a Non-SSM Capable Input PQL is Always Assigned Value of 1



Time of Day Status	Freerun
Current Reference	Slot A J7 (Freq status: Locked)
Timing References	
Frequency References	Slot A J7 (Frametype D4)

Use tables F-6 and F-7 to see the values that are encoded onto SSM-capable outputs. From F-6 (E1 encodings), PQL = 1 encodes SSM 0x2. From F-7 (T1 encodings), PQL = 1 encodes 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 must have the appended “FF”: Not the E1 as shown in the form, but the actual outputs are encoded correctly).



Slot Modules

Modules	Type	Status
Slot A	Timing I/O + Telecom Card	Installed T1 Output SSM: 0x04; E1 Output SSM: 0x02FF
Slot B	Timing I/O + Fiber Output Card	Installed

The current set of frequency inputs that are not capable of encoding SSM include the following:

- 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, and 10 MHz).
- Frequency inputs on J1 (1 PPS and 10 MPPS).

Any of these, when selected as the system frequency reference, sets 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. Following 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) is 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. That is, if the PQL of a higher priority reference is worse than the PQL of a lower priority reference, it does 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 becomes disqualified and therefore cannot 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 listed in the following table.

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	It must not be used for synchronization

G.781 defines nine valid QL and SSM values for Option II network (1544 kbps hierarchy), as listed in the following table.

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

...........continued		
QL	**SSM**	**Clock Quality Definition**
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	It must not be used for synchronization

13.2 PQL Input Mapping

The following table lists the PQL values converted from SSM for Option I network frequency references.

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

The following table lists the PQL values converted from SSM for Option II network frequency references.

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

Table 13-1 lists the PQL values associated with clock types for rubidium and quartz oscillators. Table 13-8 lists the PQL values associated with various clock states for rubidium and quartz oscillators.

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. The following table lists the PQL output mapping for Option I networks.

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		

The following table lists the PQL output mapping for Option II networks.

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		

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

From Output PQL	Output T1 SSM	Output QL
12	10FF	QL-ST3
13	22FF	QL-SMC/EEC2
14		
15	40FF	QL-PROV
16	30FF invalid SSM	QL-DUS

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. The following table lists the internal clock quality level for different oscillator types and clock states.

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 Reference	Freq PQL for Selected Reference	Freq PQL for Selected Reference
Bridging	Freq PQL for Selected Reference	Freq PQL for Selected Reference	Freq PQL for Selected Reference
Holdover	4	6	12
Extended Holdover	4	6	12
Relocking	4	6	12

14. Configuring Remote Auth Servers in 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 section describes how to download, build, and install the FreeRADIUS server from source on a 64-bit Ubuntu 14.04/16.04. The instructions are the same for both Ubuntu 14.04 and Ubuntu 16.04.

14.1.1 Download FreeRADIUS

Go to freeradius.org/releases/ to download the latest stable release source. Currently, 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. Go to www.samba.org/ftp/talloc/ to download talloc source code. Currently, 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, as all the files and directories under `/usr/local/etc/raddb` are owned by 'root'.

```
su -
cd /usr/local/etc/raddb
```

Note: It is considered that 'root' is enabled on the Ubuntu installation. If not, add 'sudo' to commands 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, you must disable this check:

1. Open the `radiusd.conf.` search for the security section, starting with:

```
security {
......
}
```

2. Comment:

```
     #allow_vulnerable_openssl = no
     allow_vulnerable_openssl = yes
```

Note: Comment out the line 'allow_vulnerable_openssl = no' (before the '}').

14.1.4.2 Configure Clients

Open `clients.conf`. At the top of file and immediately after the comment line “Define RADIUS clients (usually a NAS, Access Point, etc.).”, add:

```
client k2 {
        ipaddr = *
        proto = *
        secret = myk2secret
}
```

Note: `ipaddr = *` allows any RADIUS client (IPv4 or IPv6) to be authenticated. You can use individual IPs or subnets to restrict the clients that the server is going to authenticate. The secret 'myk2secret' must 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, and 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, and add:

```
admin Cleartext-Password := "myrad-passwd"
testk2user01 Cleartext-Password := "mscck2userpass01"
```

Note: 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', then enter:

```
# radiusd
```

Otherwise, enter:

```
% sudo radiusd
```

On the console, you can watch all of 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 SyncServer

On the `SyncServer Security > RADIUS` page, enter:

```
RADIUS Server IP Address = IP of the RADIUS server
Secret Key               = myk2secret
Timeout                  = 5
```

Now, login to 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: You can still login as 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 pam_radius_auth Module Password Hash

For products using the pam module `pam_radius_auth.so` (used in SyncServer S600) to communicate with the RADIUS server, the module applies an 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

The widely available open source TACACS+ server software tac_plus is used. The following sections describe downloading and configuring of the tac_plus server on a 64-bit Ubuntu 14.04 and Ubuntu 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: manpages.ubuntu.com/manpages/bionic/man5/tac_plus.conf.5.html.

The tac_plus daemon man page: manpages.ubuntu.com/manpages/bionic/man8/tac_plus.8.html.

14.2.4 Configure tac_plus

The configuration files are under `/etc/tacacs+`. You can 'su' to be 'root' before making edits, as the file is owned by 'root'.

```
su -
cd /etc/tacacs+
```

Note: It is considered that 'root' on the Ubuntu installation is enabled. If not, you can add 'sudo' to commands that require the 'root' privilege.

14.2.4.1 Configure Key

After the comment line: “This is the key that clients have to user to access Tacacs+”, edit the key to match the key defined in SyncServer TACACS+ “Secret Key”. Here, change the key to “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 convenient as 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 following line:

```
#default authentication = file /etc/passwd
```

to be:

```
default authentication = file /etc/passwd
```

14.2.4.2.2 Add Users to 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"
}
```

To add a new TACACS+ user with encrypted password, you must run the `tac_pwd` command. 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:
You can use a single number after -d by adding them all as “-d 690”.

14.2.5 Configure TACACS+ Server on SyncServer

On the `SyncServer Security > TACACS+` page, enter:

```
TACACS+ Server IP Address = IP of the TACACS+ server
Secret Key                = k2testing0123456789
Timeout                   = 6
```

You can login to SyncServer with user on the Linix PC, k2testuser, and 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: 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 pam_tacplus Module Password Hash

For products using the pam module `pam_tacplus.so` (used in 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

The widely available open source OpenLDAP server software is used. The following sections describe how to download and configure the OpenLDAP server on a 64-bit 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: manpages.ubuntu.com/manpages/bionic/man5/slapd.conf.5.html.

The slapd daemon page is at manpages.ubuntu.com/manpages/bionic/man8/slapd.8.html.

14.3.4 Re-Configure slapd

When asked to enter a top dn during the installation, if you chose default, the top dn is `dc=example,dc=com`. Here we show you to create a different top `dn dc=utopia,dc=net`. This is done through re-configuration. As re-configuring requires root privilege, you use either 'sudo' or become 'root'.

Note: To stop the slapd daemon first, it is considered that the 'root' on the Ubuntu installation is enabled. If not, then you must add 'sudo' to commands that require '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 following:

```
/etc/init.d/slapd restart
systemctl restart slapd
```

14.3.5 Add Users

A“ou=people” serving is created as the container for the users and then two users “Ashley Simon” and “Jack Kandell” are added. The easiest way to do this is to create a `.ldif` file (`utopia.ldif`). As 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”:

```
slappasswd -h {SSHA}
Letmein
Letmein
```

The output is `{SSHA}wV5U887AlqhE7QKBzKVgjZvYJSdG9ej7`. Your output might not match the output shown here because the slappasswd uses a dynamic salt value.

For “Jack Kendall”, the password is “Whynot!”:

```
slappasswd -h {SSHA}
Whynot!
Whynot!
```

The output is `{SSHA}OG4oszEpvOHctVvSoIaNI8JkvKOCJQ4S`. Your output might not match the output shown here.

Put the following into the `utopia.ldif` file 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
```

You can add the number together for “-d” as “-d 3905”.

14.3.7 Configure LDAP server on the SyncServer

On `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.

You can now login to SyncServer with user Asimov and jkendall.

Login as LDAP 'asimon' user:

```
Username = asimon
Password = Letmein
Login as LDAP 'jkendall' user
Username = jkendall
Password = Whynot!
```

You can also use user's common name to login. On `SyncServer Security -> LDAP` page, enter:

```
Login Attribute               = cn
```

Now, you can login to SyncServer with user's common name (default is 'uid'):

```
Login as LDAP 'Ashley Simon' user
Username = Ashley Simon
Password = Letmein
Login as LDAP 'Jack Kendall' user
Username = Jack Kendall
Password = Whynot!
```

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 pam_ldap Module Password Hash

For products using the pam module `pam_ldap.so` (used in SyncServer S600/S650) to communicate with the LDAP server, the module supports all of the RFC defined challenge response protocols and the 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 following 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 which let you browse your directory and optionally add new element, modify, and delete elements to your directory. The phpLDAPAdmin package is recommended.

15. Related 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. For more information regarding installing or using the product, contact Microchip Frequency and Time Systems (FTS) Services and Support.

16. 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

17. Revision History

Revision	Date	Description
C	05/2022	The following is the summary of changes made in this revision: • Sanitized and formatted the document as per Microchip publishing standards. • Added the following new sections/images: – 4.1.12. logout. – Figure 5-9 – Figure 5-27 – Figure 5-44 – 6.14.5.2.3. Satellite C/No Consistency Check – 6.14.5.2.4. Satellite C/No Drop Monitor – 6.14.7.3. Automatic Gain Control Check – 6.14.9.3. C/No Consistency Status – 6.14.9.4. C/No Drop Status – 6.14.9.9. Automatic Gain Control Status – 6.15.9. Automatic Gain Control Chart – Figure 6-37 – Figure 6-43 – Figure 6-44 – Figure 6-45 • Edited the following: – Table 2-5 – Table 4-2 – 4.1.18. show system – Figure 5-8 – 5.2.1.2. Network—SNMP Configuration – 5.2.1.3. Network—SNMP Trap Configuration – Table 5-7 – 5.2.5.1. Security—Users Window – 5.2.5.6. Security—NTPd Symmetric Keys Configuration Window – 6.2.2. Adding a User. – 6.4.5. Provisioning HaveQuick Input on Timing I/O HaveQuick/PTTI Module – 6.7.1. NTPd Symmetric Keys – 6.12. Provisioning for SNMP – Table 6-33 – 6.12.6. Adding and Removing SNMP v3 Users and Table 6-35 – Table 7-2 – 6.14.5.3.3. Receiver Autonomous Integrity Monitor – 6.14.7.1. Continuous Wave Jamming – 8.1. Facility Codes – 8.2. Severity Codes and added Table 8-1 – Table 8-2

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

Revision	Date	Description
		Edited the following: - – 6.14.8.5. Example 1: Multiple Detectors Alarmed with Disqualify GNSS only While Alarmed Setting – 6.14.9.3. C/No Consistency Status – 6.14.9.4. C/No Drop Status – 6.15.2. Common Attributes of Vs. Time Charts – 11.1. Third-Party Software - Removed the Message Provisioning section
B	05/2021	The following is the summary of changes made in this revision: - 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.
A	—	The following is the summary of changes made in this revision: - 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 server 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
Rev. E of P/N 098-00720-000	—	The following is the summary of changes made in this revision: - 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.

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

Revision	Date	Description
		• Added PTP Output Power Profiles • Added Provisioning Programmable Pulse Output Added Making Time-Interval or Event Timestamps 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.
Rev. D of P/N 098-00720-000		The following is the summary of changes made in this revision: • 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.

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

Revision	Date	Description
Rev. C of P/N 098-00720-000		The following is the summary of changes made in this revision: • 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.
Rev.B of P/N 098-00720-000		The following is the summary of changes made in this revision: • 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 nenaformat, and show nene-format. • Updated screen images for some Web Interface windows to reflect changes to the GUI.
Rev.A of P/N 098-00720-000		This was the initial release of this document.

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

Trademarks

ISBN:

Quality Management System

For information regarding Microchip’s Quality Management Systems, please visit www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS

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

ASIA/PACIFIC

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

ASIA/PACIFIC

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

EUROPE

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