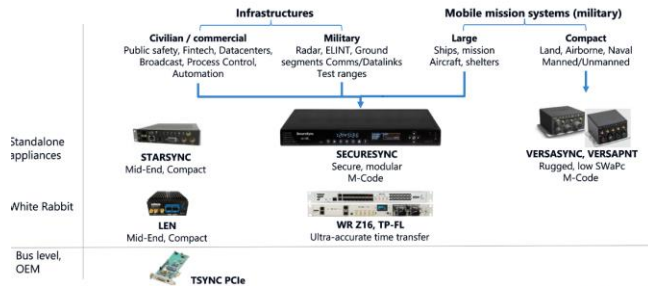


CUSTOMER SERVICE ASSISTANCE

Note: This document contains both “Public Information” and “Internal Use Only Information” (do not release this document in its entirety)

PNTSN portfolio – high level	17
------------------------------------	----

PNTSN portfolio – high level application perspective



SAFRAN

.....	17
Azure Software/Orolia Data Classifications	17
Orolia Online Store	18
Super 6 customers and Associated Sales Account Managers	19
Spectracom blogs about various topics.....	19
Orolia Rochester (ROC1) Contact list	21
OGSI (ROC2) contact list.....	21
OGSI Supported Products	21
McMurdo/Kannad contact info	22
Sarbe beacons (such as FastFind)	22
Net Promoter Score (eNPS system)	24
Sales/Repairs in Rochester.....	25
**SpectraTime Repairs/RMAs.....	25
**Repair centers	25
***APAC (Asia/Pacific) Singapore (Danny Loke)	25
***EZU (Hong Kong)	26
***Aimil (India)	26
SCATS (shipping labels for Northrop Grumman)	26
FMECA (Failure Mode, Failure Mechanism, Failure Effect, Failure Detection Method and probability)	26
1PPS / Antenna cable delay calculations	27
Ethernet/network cable loss/cable delay/cable attenuation calculator	28
Cable impedance (50 ohm versus 75 ohm)	30

Antenna cabling	31
Our Standard length CA01xxx and CA07xxx coax cables	31
UL94HB level rating (Flammability Standard)	31
(CA01-0N0N-xxxx GNSS antenna cables)	32
(CA01-0N0N-3xxx) Belden 7810A (RF-400) / or can be Times Microwave LMR-400 cable	32
Fire retardancy of Belden 7810A/Times Microwave LMR-400	33
UL/ELV ratings, CE Declaration of Conformity/RoHS statements for CA01-0N0N-3xxx	33
(used to be CAL7xxx cable)	34
Minimum Bend Radius for cable(Install)/Minor Axis	35
CA01-0N0N-6xxx (Plenum-rated Times LMR-400-LLPL cable) (was CALP7xxx cable)	37
CA01-0N0N-9xxx (outdoor/watertight Times Microwave LMR-400-DB cable)	39
Other cable types	41
*Times Microwave LMR-600 cable	41
*Times Microwave LMR-240 (“ultra-flex”)	42
*Times Microwave LMR-195 cable	42
*Belden 9914 RG8-U cable	43
Alternate cable types (RG-59, RG-59, RG-8/RF400, etc)	44
**Bent center plate on Type N connector (due to cross-threaded connector)	46
Conduit interference (other cables run in same conduit as the antenna cable)	46
Adapters/Coax cable connectors	46
**Type N barrel connector (P/N 067022)	46
Type N connectors for cable termination	48
Formula for calculating allowable cable length/configurations	49
5VDC voltage drop through long antenna cable runs	50
Desire to use different antenna cable with GPS products	51
CW04-FLFL-xxxx RS-485 twisted-pair cable	53
General info on Fiber cable/SFP Modules	54
Satelles STL (Iridium) antenna	58
*Available outdoor/rooftop STL antenna (E050-0006-0001)	58
*Active STL antenna (E050-0004-0001)	58
*Passive STL antenna (E050-0001-0001)	58
GNSS Satellite constellations (GPS/Glonass/Galileo/Beidou/QZSS/NavIC)	59

GNSS (GPS, Glonass, etc) INFO, GPS ANTENNAS AND GPS RECEIVER INFORMATION	62
GNSS Constellation Status info.....	62
GPS: USCG NAVIGATION CENTER: NANUs/ GPS SERVICE INTERRUPTIONS-OUTAGES / GPS TESTING NOTICES/ REPORT STATUS	62
*GPS INFO.....	63
GPS Signal Structure	63
WAAS/EGNOS/GAGAN/MSAS (Systems that Aid GPS)	63
Controlling agencies/controlling documents for GPS (ICD-GPS-200, IS-GPS-200)	64
ICD-GPS-153/ ICD-GPS-153c (documentation for the DAGR receiver).....	66
GPS leap second insertion.....	66
**LEAP SMEAR (SMEARING THE LEAP SECOND INSTEAD OF JUMPING ONE SECOND)	66
Solar flares and effects on GPS.....	66
Using a smart phone/cell phone to test for GPS/GNSS reception	67
Security considerations/PCI audits	68
GPS/Glonass Signals, Frequencies/Bands	69
**GPS Signal Modernization	69
GPS week numbers (date/time info GPS transmits)	69
April 2019: 20 year GPS Week roll-over issue due to number of bits in the message (2019, 2036, etc..)	70
YEAR 2036	70
GPS/UTC 1PPS timing error with several satellites (26 Jan 2016)	72
**Change made to GPS signal January 11, 2010	73
GPSD (GPS service daemon).....	73
Orolia Intelligent Repeater Systems / Zone Based Indoor Location Using GNSS Simulators	73
*"Trimble GNSS Planning tool" / GPS prediction software (freeware)	74
U.S. Coast Guard Navigation Center (NAVCEN): GPS Situational awareness (problem reports/outages/GPS Interference testing, etc)	76
GNSS Security framework (GNSS jamming/spoofing)	78
Broadshield software /Local interference/ GPS jamming (anti-jamming) and GPS spoofing (anti-spoofing)	81
***GPS Jammers/GPS transmitters/GPS spoofers	82
Jamming detection/Mitigation.....	83
***Opt-BSH:.....	83
***Talen-X Broadsense.....	85
**Talen-X Broadsense Handheld (BSE-HH)	85

***Talen-X Broadsense Micro (BSE-MICRO)	85
***Talen-X Broadsense Nano (BSE-NANO-S)	85
Threatblocker (sold thru OGSi).....	87
Elevation Masks	89
**Non-Spectracom ANTI-JAM GPS Antennas	92
****Novatel Model GAJT antenna	92
GPS/GNSS ANTENNAS	94
General Cabling/Antenna installation info provided to/available for customers	94
**Antenna installation Tech Note (“Outdoor GNSS Antenna Installation Considerations”) on our website.....	94
* Corrosion on outdoor connectors/cleaning corrosion off connectors	94
Available weatherproofing kit for outdoor cable install	95
International shipping Regulations (HTS code, ECCN Number, EAR, CCATS, etc).....	95
**GPS Antenna Height/Altitude/Elevation	95
*** Interference from other transmitters (near a GNSS antenna).....	97
**Cross-talk/ multiple GPS antennas installed near each other.....	98
****PVC mast assembly for the Model 8225/8230 antenna /included items	99
****Model 8213 / Antenna mounting for Models 8230 and 8225:	101
Custom brackets/Mounting	104
****Wind resistance for the Models 8230, 8225 and 8213 (flat roof-mount base)	105
Model 8235 / Model 8238 antenna mounting kits	106
Optional Model ANT-KT “Rugged Post Mount Kit” for 8230 or ANT-35 antenna onto a vertical or horizontal post..	108
InfiniDome’s GPSDome (inline add-on Anti-jammer from InfiniDome in Israel)	112
GPSDome P/Ns.....	117
GPSdome Installation	121
**Model 8230 and Model 8230-00 (TW3740/TW3742) GNSS Antennas	124
Model 8230AJ (Anti-Jam GNSS antenna)	142
**Model 8225 GPS antennas (prior to ~Dec 2013)	148
**Model 8225S (GPS L1/L2 antenna for SAASM GPS receivers)	155
Dept of Defense Form DD-1494 (DD1494 for SAASM)	157
Model 235884 LP-TP lightning suppressor for Epsilon Clocks (EC20S, EC22S, etc)	167
Indoor GPS antennas	167
Skylight antenna (1213-0000-0600)	167
Model 8228 window-mount antenna (8228-0002-0600)	167

**Trimble Acutime GPS/GNSS Antennas (2000, Gold, GG and 360)	172
Acutime 100 foot extension cable	185
**Non-Spectracom ANTI-JAM GPS Antennas	186
****Novatel Model GAJT antenna	186
Model 1169 GPS Fiber Optic Isolator (TX and RX) for GPS:	188
Symmetricom/Microsemi GPS/GNSS antennas (for use with SecureSyncs/NetClocks)	190
GPS/GNSS COMBINERS / SPLITTERS / SURGE SUPPRESSORS / PREAMPS / FILTERS	192
GPS/GNSS Combiners	192
Model 235896: 2/4/8 way GPS power splitter for Epsilon Clocks	192
**Model 8224 GPS Splitters	193
International shipping Regulations (HTS code, EAR and ECCN Number)	193
Variants of the Model 8224 GPS splitters (Configurations/Part numbering scheme)	193
8224-41050	197
8224-20151	197
8224-20052	197
8224-40052	197
8224-20152	197
8224-40152	197
8224-40152	197
8224-40153	197
8224-20051	197
8224-40151	197
8224-81150	197
8224-80151	197
8224-40053	197
8224-21150	197
8224-20153	197
8224-40000	197
8224-20053	197
8224-20154	198
8224-40154	198
8224-41150	198
8224-80153	198

8224-80154	198
***Troubleshooting Model 8224	204
**Model 8226 GPS Surge Suppressor	207
General information on surge protectors	207
**Field installable clamp connectors supplied with 8226	216
**Ground cable for surge suppressors	220
**Custom surge suppressors (not supplied by Spectracom)	220
*Model 8226-0002-0600 (Surge Suppressor Grounding Kit)	221
**Model 8227 GPS amplifier	227
**GPS filters (Prevent signals from escaping through the GPS cable):	234
GPS OPTIC ISOLATORS/ CABLE/ MEDIA CONVERTERS (COAX AND FIBER)	234
**Model 1169 GPS Optic Isolator (TX and RX) for Invensys timing boards:	234
**1201-KIT-RF1-DUC ("StarLink") Raven/Forsberg DUC	235
RMA's/repairs of the DUC	236
CE and Declaration of Conformity/ PSE (for Japan), RoHS and FCC compliancy	237
Troubleshooting the DUC system	248
** ("StarLink") "RavenLink" 1201-KIT-FIB1-DUC Fiberlink system Kit (Discontinued)	250
Propagation speed and cable delay for Fiber Optic cable	258
Optical Zonu Fiber Optic Antenna Link kits (1201-KIT-FIB1-C kit and 1201-KIT-FIB2-C kit)	259
Status LEDs	281
Pendulum FL-15 GPS Antenna Fibre link (not available from Spectracom)	285
Other GPS Fiber converters (not available from Spectracom)	286
GPS/GNSS RECEIVERS	286
Noise Figure	286
TRAIM (Timing Receiver Autonomous Integrity Monitoring)	286
Clearing Antenna problem alarm when GPS antenna is not connected:	289
Desire to block DC voltage output from the GPS receiver	289
Rockwell Collins GB-Gram SAASM receiver (MPE-S receiver)	289
uBlox Model M8T GNSS receiver (used in SecureSyncs,TSync boards and Versas)	290
"GPS0 UBX Message receive Checksum Error" / "GPS0 UBX Message receive buffer overflow" (observed in SecureSync logs)	302
ublox receiver used in Legacy VelaSyncs (Smart GXClok-500 from SpectraTime)	303
Trimble Tech support contact info	305

Trimble Res-SMT-GG / Resolution SMT-GG Multi-GNSS receiver (Multi-GNSS GPS/Glonass)	306
**Receiver accuracy based on GPS/Glonass vs Glonass only operation	307
**RES-SMT-GG Receiver Sensitivity	307
**(Ju//Aug 2016) Leap second asserted upon GPS notification of Dec 2016 leap second	312
**Desire to Blacklist (Mask/Unmask) a Satellite from being received by a Trimble RES-SMT-GG receiver	313
Known firmware issues with Res-SMT receiver (SecureSyncs, TSyns, EC20S)	314
Trimble RES-T (Resolution T) GPS receiver (NetClock, TSync, SecureSync)	318
Resolution-T GPS receiver RAM and Flash memory storage	323
**Mobile/Stationary/Single Satellite modes with a Resolution-T receiver	324
Anti-jamming for both Trimble RES-T and RES-SMT-GG receivers	327
** Naelcom-RSMT receiver (Original Skylight phase 1 receiver)	330
** Trimble Force 22E SAASM receivers (Model 9300s and SecureSyncs)	331
**GB-GRAM (GBGRAM/GB Gram): SAASM GPS receiver	332
Motorola VP/GT/UT receivers	333
PRODUCTS	336
Diff progams (such as WinMerge or KDiff) to compare files	336
RoHS Directive (Restriction of Hazardous Substances)	336
Export Control (CCATS numbers HTS, ECCN numbers) for all products	338
Bug/issue in Intel's Atom C2000 processor ("Clock Signal Component Issue")	339
Product Registration/register your product	339
Premium Support Packages (PSP and GPSP)	339
"In country" terms (for PSP loaners)	340
SpectraTime / SpectraTime oscillators	341
**Warranty period on repairs and new units	341
**SpectraTime contact for RMA Status	341
Obtaining RMA Numbers for SpectraTime oscillator repair requests	341
Spectracom Cage Code and NSN Numbers (National Stock Numbers)	342
Lists of all Spectracom NSN numbers	343
Conflict Minerals postion report/Smelter list	345
Taking remote control of a customer's PC (gotomeeting/teamviewer)	345
Gotomeeting	346
Linux BASH terms commonly used with Linux-based products	347

file text editors (vi, nano, etc)	347
Time of Day conversion (seconds since midnight)	351
MTBF/MTTR (for all products).....	355
IP rating/Ingress Protection rating (for all products)	364
Power packs (for all products).....	367
Time Scales (UTC/GPS/TAI) for all products	376
Chemicals (for all products)	376
REST API interface/Postman (alternate to using the standard web browser or CLI).....	377
Python program used to create or run scripts/script files.....	389
COMPLIANCY (for all products)	393
**UL and CE Testing / Declarations of Conformity statements (for all products)	393
MIL-STD-461 (ELECTROMAGNETIC INTERFERENCE CHARACTERISTICS).....	395
Article 3.2 of the EU Radio Equipment Directive (RED) / ETSI EN 303 417: Wireless power transmission systems (WPT)	396
ISO 8601 (ISO-8601) compliancy (internationally accepted way to represent dates and times).....	399
**DISA/STIG (Security Technical Implementation Guide) for all products	400
CIP/Cyber Security/Potential Vulnerabilities/Anti-virus software.....	401
**Information Assurance (IA) / Common Criteria (CC) / EAL levels	402
Scada Systems	404
Telcordia GR-63-CORE (NEBS Earthquake/seismic-related enclosures)	405
Y2k38 (year 2038 rollover) (“Unix Millennium Bug”).....	405
Voluntary Product Accessibility Template (VPAT)“Section 508 form / Form 508 of The Rehabilitation Act (for people with disabilities: Blind, hearing impaired. etc).....	406
NETWORK RELATED (for all products)	407
**Static IP addresses assigned to Customer Service/Tech Support	407
Assigning a temporary static address using MAC address (arp)	407
*nslookup (DNS lookup of hostnames/IP addresses)	407
*netstat commands	407
*Ping command.....	411
*HyperTerminal (for all products that can use RS-232 CLI interface).....	412
**Logout button/ web browser opening a connection already logged in.....	413
**Web browser page caching/refresh	413
Assigning a static IP address on a laptop/stand-alone PC	414

**Accessing the web browser using Internet Explorer (IE)	417
**Securing unused network RJ-45 ports	419
**Packlayers	419
**Network cross-over cable	420
**Port assignments and RFCs (NTP, HTTP, HTTPS, SNMP, Syslog, etc) for all products	421
**Network ports	422
Network Discovery/Network Auto Discovery/Auto-Discovery	424
*NWay auto-negotiation (auto sensing) / port duplex	424
*Telnet (for all products)	425
*FTP (for all products)	425
**IPv6 addresses (for all products that support IPv6)	426
**RFC-2462: SLAAC addresses (Stateless Address Autoconfiguration for IPv6)	426
**NTP support for IPv6	427
Load Balancing / Load Balancers	428
**LibreSSL/OpenSSL (Libraries for encryption)/ Ciphers List for encryption	430
**AES (Advanced Encryption Standard)	431
IP addresses/subnet masks	432
**HTTP/HTTPS web browser connection/ error messages (for all products)	432
**Parallel Redundancy Protocol (PRP)	435
**IPSec / IP Security (for all products)	436
***How IPSec works	436
Syslog (Remote logs/remote logging)	441
SNMP/Net-SNMP from Sourceforge (for all products)	442
**Troubleshooting issues with SNMP	445
**SSH (for all products)	445
**VLANS / VLAN Tagging	447
**RLOGIN	447
**tcpdump/WireShark packet capture (all products with Ethernet connectivity)	449
**PAUSE frames on the network	451
Enterprise-level Network Monitoring Tools (NMS)/ NRPE (such as Nagios, Zabbix Cacti, Splunk Integration, QRadar, etc)	453
Veritas NetBackup ("OS NetBackup")	453
Oscillators/10MHz outputs (for all products)	454

Fractional Frequency Error (FFE) for 10 MHz	456
** TCXO/OCXO Oscillator disciplining.....	458
***Simulcast radio systems 10 MHz inputs	458
**10 MHz Phase Noise and distribution devices (for all products)	459
**10 MHz output distribution units.....	460
Spectracom 10 MHz generators/ phase noise	460
10 MHz generators Phase Noise measurement comparisons.....	461
**Phase noise for other devices that don't produce 10MHz.....	463
**Rubidium oscillators	464
****SpectraTime SRO-100 Rubidium oscillators	464
MSDS/Hazardous material for Rubidium oscillators.....	464
**Stratum timing levels for all Frequency products	471
Max cable distances for 10 MHz output.....	472
**Allan Variance measurements (for all products).....	474
Time is derived from Frequency	475
**Max cable distances that can be run for 1PPS outputs	476
**1PPS Propagation/Cable delays.....	479
**1PPS Fiber Optic distribution.....	480
***SI Tech Fiber converter equipment	480
Various SI Tech products.....	481
Model 2062 - Optical Repeater Mini Bit-Driver®	481
AFNOR NFS 87-500	483
General Time distribution (Master to one or more Slaves via IRIG, NTP, PTP)	484
ASCII, IRIG and STANAG/HAVEQUICK (for all products)	485
**Synchronous/Asynchronous:.....	485
**DATA FORMATS/ NMEA 0183 (for all products)	485
***China Mobile Format.....	501
***Cisco TOD	501
**NAV-TIMEGPS with UBX format	502
RS-232 data	502
** RS-485/RS-232 distribution over Ethernet connection (RJ-45).....	503
**IRIG for all products	505
****IRIG Distribution amps from Spectracom	505

Fiber converters for long distance IRIG runs	506
*IRIG Cabling/Surge Protection/Output	508
***IRIG design specs.....	509
***IRIG Format codes.....	510
***IRIG Year info.....	511
**Control functions (CF) info.....	513
***IRIG G format and IEEE 1344.....	513
****Year value/ "Spectracom Format" versus "RCC 200-04" format	514
****Time sync status/Time Quality.....	517
****IRIG PID marker for ON Time Point (OTP) / IRIG Accuracies	518
***IRIG Cabling/max recommended cable distances	522
***IRIG signal cable/processing delays	524
****IRIG fiber converters (for long distance runs):	524
****IEEE-1344 extensions (IEEE C37.118-2005) and "Spectracom IEEE C37.118-2005"	526
Manchester coding	529
****FAA IRIG	530
****CTQ (Continuous Time Quality) (part of IEEE C37.118.1- 2011).....	531
IRIG Input/Output (for Models 9383 and 9283 and 9183).....	532
IRIG for TPRO-TSAT/ PCI, PCI-U, PCI-66U	532
IRIG for TSynC-PCIe	533
Available TSynC-PCIe Outputs	533
****IRIG/ASCII Event Count Status messages (CS1, CS2, CS3, CS4 and CS5)	533
Timing board synchronization via IRIG playback from a tape.....	535
SMPTE time code.....	535
**Stanag/HaveQuick input/output (for all products)	536
Leap Second insertion.....	537
Daytime and Time protocols (for all products)	539
Packet capture of daytime (TCP and UDP from NetClock and SecureSync)	539
**Time protocol	540
**Daytime protocol.....	540
**Interface with daytime/time protocols.....	541
Chrony/chronyd (Crony) (replacement to NTP).....	541
NTP (for all products).....	544

Good NTP documentation.....	544
NTP versions/NTP version in gentoo package	544
NTP Best practices document (Written by Denis Reilly)	544
RFC 8915: Network Time Security (NTS) for the Network Time Protocol (NTS)	544
**NTPSec (more secure NTPd)	545
**NTP Vulnerabilities	545
**W32Time (Windows Time Service)	546
Syncing Virtual Machines/VMs (such as VMware/ESX and ESXI, Hyper-V)	547
Using TSyn boards/TSync drivers in Virtual Machines/VMs/Virtual environments	547
**Windows Hyper-V (ESXI hypervisor) and W32Time (Windows Time Service).....	549
***Report the time offset between a Windows PC and an NTP server	549
**Change the desired Windows Time Format display from 12 hour to 24 hour	550
Desire to very accurately synchronize Windows	551
**Troubleshooting Linux box not syncing to NTP server (using CLI commands).....	552
***errno error messages	552
***Using the ntpdate command	552
**NTP Stress Test / Stress test results	555
**NTP packets.....	556
NTP Stratum level.....	556
NTP filters and algorithms.....	557
“tos” commands and other commands for tweaking NTP settings in clock selection and clock cluster algorithms ..	561
“Time Reset” when NTP starts up.....	566
Sync status at start-up (LI bits and Stratum value)	567
NTP at Stratum 16	568
**NTP operational modes/states (.INIT, Step, etc).....	569
.INIT refID being reported by an NTP reference	569
**NTP Leap Seconds	574
NTP Peering.....	576
***NTP log entries associated with NTP peering.....	576
****NTP performance/algorithms for reference selection	577
***Clock Status / NTP Precision value	578
**NTP Status graphs.....	579
Block diagram/system description of an NTP server / NTP operation (tailored for SecureSync).....	579

NTP Multicast mode.....	581
**Accuracy of NTP in Holdover (Oscillator free-run specs)	582
Falseticker vs Truechimer / NTP sanity check (time change of greater than 1000 seconds occurs while NTP is running)	582
NetClock 9300 and 9200 series.....	587
**NTP transmission modes- Anycast, Broadcast and Multicast modes	587
**NTP software:	590
NTP main versions	591
PKI (Public Key Infrastructure/Public Key cryptography) for NTP security	591
****NTP Authentication/NTP Symmetric key (MD5 Authentication).....	591
***FIPS compliancy (FIPS 140-2) for all Spectracom NTP servers	593
****NTP Autokey:	596
**NTP Burst/IBurst modes.....	598
Electrical substation specs	599
**IEEE 1613:.....	599
IEC 60945 (Maritime Navigation and Radiocommunication Equipment and Systems)	600
**IEC 61850: Synchronization of IEC 61850 devices via SNTP (electrical substation automation specifications)	601
**NTPSTAT / NTPQ (ntpq -p) / NTPDC.....	603
ntpqstat command	603
NTPQ/NTPDC (Mode 7).....	603
List of CLI commands available for ntpq	603
NTPQ -p /ntpq -p (peers command)	604
**Ref ID (RefID) (such as .gps, .pps, .init, .drop, .step, .xfac, rtc)	608
*NTP Status Symbols (Tally Codes)	615
**NTP Reach Value.....	615
ntpq associations (show ntp associations, as command).....	616
rv and rvi commands (readvar)	619
Kerninfo (display kernel information).....	620
NTPDC.....	620
NTPQ	620
***ntpq -p sysinfo / ntpq -c sysinfo commanda (system information)	620
Ntpdc -> Sysinfo command	621
Stability.....	622

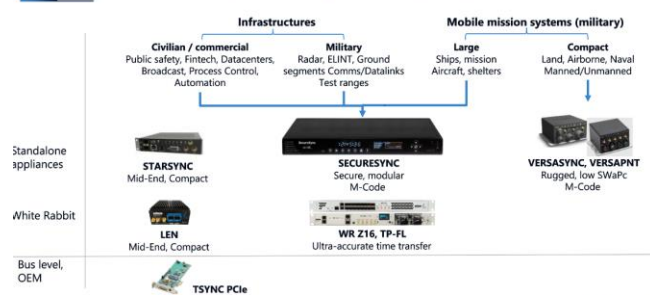
NTPDC -> monlist command (And DRDoS/Amplification Attack)	622
Monlist command	622
**NTP Statistics (NTP ClockStats, NTP loopstats and NTP Peerstats).....	625
**Monitoring and Controlling NTP	628
**127.127.1.0 (Atom clock driver), 127.127.22.0 (PPS driver) AND 127.127.45.0 (Spectracom Clock driver)	628
Spectracom Reference Clock driver (127.127.45.0) - "TSync(0)"	628
NTP Mode 6 and Mode 7 (NTPQ and NTPDC).....	632
**Who is using my NTP server?.....	632
MONlist- monlist [version]	632
**Automachron program: Time Program for testing NTP with Time Servers.....	634
**Syncing Virtual Servers (VMWare)	635
NTP operation	635
**Number of NTP requests per second/NTP Stress test	635
Signal 15 ("NTP Exiting on Signal 15") or other Signals	635
** Automatic FTP of NTP Statistics	637
**NTP broadcast/ NTP Multicast modes.....	638
Desire to output NTP Multicast on more than one Ethernet port (Gigabit Option card installed).....	641
NTP drift file	641
NTP clockstats, loopstats and peerstats.....	642
**RFC 2783 (PPS disciplining).....	642
NTP Orphan mode	642
**SNMP/Notifications (SNMP/MIBS/OID numbers)	642
****Troubleshooting issues with SNMP	642
Leap Second insertion.....	643
PTP Precision Timing Protocol (IEEE 1588) (for all products)	648
IEEE-1588 PTP specifications	648
PTP v2.1 Authentication	648
*PTP v1 versus PTP v2.....	649
GENERAL INFO ABOUT PTP	649
**Accuracies of PTP	649
Ordinary Clocks/Transparent Clocks/Boundary Clocks	649
Known issues/Specific configurations with PTP boundary switches	650
*IEEE 802.1AS (PTP Timing and Synchronization for time-sensitive applications)	654

** IEEE 802.1Q (VLANs/VLAN trunking / VLAN tagging)	654
ITU-T Standards (g.8265 series)	658
ITU-T Standard G.8262 – SyncE (Sync-E) (Synchronous Ethernet mode)	659
***ITU-T Standard G.8264 (ESMC)/ Messaging Channel for PTP	660
***ITU-T Standard G.8265 (Packet over Transport aspects- quality and availability targets)	660
ITU-T Standards (g.8275 series) (8275 series not currently supported)	660
*ITU-T Standard G.8275.1/ G.8275.2 (PTP “Telecom profile” for phase/time synchronization with full timing support from the network)	660
Cont*Contract Negotitation/Unicast/Multicast/Minicast/Hybrid modes	662
IGMP (Internet Group Management Protocol)	663
*Best Master Clock algorithm (BMCA)	667
Best Master Clock Failover to another PTP master	668
**Number of hops / Boundary and Transparent clocks/ delay mechanisms	670
Transparent Clocks	671
One-Step/Two-step modes:	673
Types of PTP messages	676
TLVs and Signaling Messages (labeled “Signalling” in wireshark)	677
Announce message (Announce packet)	684
**“GrandmasterClockVariance” (AKA “OffsetScaledLog Variance”-OSLV)	689
Follow-up Message:.....	697
Delay Request messages.....	699
Delay Response messages.....	704
Peer Delay Request/Peer Delay Response (Path_delay_Resp) message.....	710
PTP Management messages.....	712
Mean path delay	716
Packet Delay Variation (PDV)	716
Link State Parameter	717
Sending PTP through a firewall	719
***SMPTE profile	719
**FAQs for PTP.....	720
PTP Client Software (Windows client software PTP/TimeKeeper/PTPd).....	721
**Windows PTP client software.....	721
*Linux PTPD/PTP4L client software	722

PTP Slave manufacturers/Models	726
**SolarFlare network adapters	726
Frame Check Sequence (FCS) errors in a packet capture.....	726
**Exfo PTP slaves	726
Specific network/PTP switch/Boundary Clock info	727
**Layer 2 / Layer 3	727
**Model 7705 router.....	727
**Arista switches/boundary clocks	727
Arista Boundary clock	727
8725 Arista switch / Myricom link flap issue.....	727
**Hirschmann switch.....	728
**Nexus switch	728
**Alcatel 7705 Router	731
Monitoring PTP performance/operation	732
Schweitzer Engineering Laboratories (SEL) equipment (Orolia Competitor)	734

PNTSN portfolio – high level

PNTSN portfolio – high level application perspective



Azure Software/Oroliia Data Classifications

Four Data Classifications

- 1) **“Public Information”**: lowest level of risk
- 2) **“Internal Use Information”**:
- 3) **“Proprietary Information”**:
- 4) **“Company Restricted Information”** (ITAR info)

Orolia Online Store

- Direct Link: <https://store.orolia.com/>

Order Status

On the Online Store website, we offer two ways for people to check their order status:

- Contact Us Form (need to submit a request): <https://store.orolia.com/pages/contact-us>
- Or (email address) store@orolia.com

Going forward, please point people in those two directions.

Super 6 customers and Associated Sales Account Managers

Scott informed us this morning of a new effort to more involve key account managers with the SUPER 6 customers. In the future, if we have any major concerns or issues with these customers we should involve these account managers and also keep them informed of any major issues we might encounter. There is no need to CC them on the everyday cases and activities, just any concerns that would affect the product lines or service as a whole.

- 1) **Harris:** Jeremy Onyan
- 2) **Raytheon:** Mike Messina
- 3) **BAE Systems:** Mike Messina
- 4) **Northrop Grumman:** Trevor Dougherty
- 5) **Lockheed Martin:** Trevor Dougherty
- 6) **Hughes:** Tony DiFlorio

Spectracom blogs about various topics

at: <https://spectracom.com/resources/blog>

- Can either “**Explore by Subject**” or “**Explore by Author**” (under “**Spectracom Blog**”)

[home page](#)
[SAP](#)
[Case 0012623 - Safe...](#)
[Arena](#)
[Log in](#)
[Material Overview 120...](#)
[time servers](#)
[Google](#)
[W Epoch Times - Wikipa...](#)

[https://spectracom.com/resources/blog](#)
80%

[Search](#)

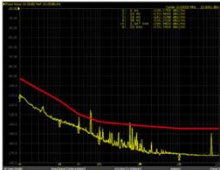
[Spectracom](#)
an Orbia brand

[essential ingenuity](#)
[SOLUTIONS](#)
[RESOURCES](#)
[WHY SPECTRACOM](#)
[PRODUCTS & SERVICES](#)
[SUPPORT](#)

[Resources](#)
[Spectracom Blog](#)

Spectracom Blog


[Explore By Subject](#)
[Explore By Author](#)



Need Low Phase Noise Under Vibration?
August 29, 2018
By Scott Hildebrandt, Program Manager

To improve performance of your radar system or signal intelligence (SIGINT) receiver, you need a time and frequency reference that can deliver a low phase noise signal. If your mission is signal intelligence gathering, then that means deeper penetration and more intelligence gathered.

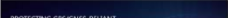
[READ MORE](#)



The REST API: A Powerful Interface for Remote Control of PNT Devices
August 23, 2018
By Ron Davis, Applications Engineer

With the built-in REST API of Orbia PNT products, any functionality that can be done manually through the web GUI can also be scripted, allowing for machine-to-machine communication and control. The REST API utilizes JSON (JavaScript Object Notation) formatted data for sending commands and receiving status information from the devices.

[READ MORE](#)



Protecting GPS-Reliant Military Customers - Part 2

Orolia Rochester (ROC1) Contact list

- Refer to **Bamboo** -> **Employees** for contact info: <https://orolia.bamboohr.com/login.php>

OGSI (ROC2) contact list

- Refer to **Bamboo** -> **Employees** for contact info: <https://orolia.bamboohr.com/login.php>
- **Hiro Sasaki**, VP or PNT Technologies (585-250-1545 ext 110 hiro.sasaki@oroliads.com)
- **Scott Hildebrandt** 585.483.0767 scott.hildebrandt@oroliads.com
- **Paul Myers**: 585.684.0123 paul.myers@oroliads.com
- **Tim Tetreault** (585) 684-0752 tim.tetreault@oroliads.com
- **Mike Sutton** 585.321.5873 mike.sutton@oroliads.com

OGSI Supported Products

Email from Scott Zmuda (13 Oct 2020) Team – Anything with an “A” in the serial number and or product number is a special OGSI build and should be forwarded to support@oroliads.com (585.250.1545)

Orolia USA should not attempt to troubleshoot or support until evaluated and requested by OGSI.

McMurdo/Kannad contact info

- main support website for all Orolia organizations: <https://www.orolia.com/support>

Websites

Kannad website: <https://www.orolia.com/support/kannad>
<https://www.oroliamaritime.com/support/kannad-marine/>

Sarbe support website: <https://www.orolia.com/support/sarbe>

McMurdo support email: support@mcmurdogroup.com

McMurdo support website: <https://www.oroliamaritime.com/support/mcmurdo/>

- Kannad Aviation support (no phone number available for customers) support@orolia.com

(per Scott Z, 27 March 2019) for Kannad aviation support, you steer them to the support@orolia.com email (which is posted on the Kannad Aviation Page) and you can also let Bruno Poyti or Isabel LaRomance know that someone is in need of support.

(email from Jennifer Hewitt to Scott Z 27 March 2019) Anyone looking for Kannad ELT information can find it on Orolia.com under **Solutions**, then **Aviation Solutions**. The **Support** button at top right on Orolia.com shows how to ask for support on any product by brand.

Kannad Aviation Support Locations Listing page: <https://www.orolia.com/support/kannad/locations-listing>

- Path to this page from Orolia.com is **Support -> Kannad Product Support -> Kannad Partner Listing**
- There are various tabs (such as "North America") at the top of the page for geographical areas:

Contacts w/Kannad

Kannad Customer Service: Support.Sar@orolia.com +33297024949

Thomas lefebvre: thomas.lefebvre@orolia.com +33297024942

B) Maritime and SARSAT product support support@mcmurdogroup.com

(per Scott Z, 27 March 2019) For Maritime support, you steer them to support@mcmurdogroup.com (which is posted on the Orolia Maritime web site and navigated to from the Orolia site)

(excerpt from Jennifer Hewitt email below to Scott Z, 27 March 2019) For maritime and SARSAT product support, OroliaMaritime.com has a similar Support button at top right, where you can find product support for McMurdo, Netwave and Kannad Maritime products.

(email from Jennifer Hewitt to Scott Z 27 March 2019) For further clarification on where things are located on the new sites, Orolia.com has all products except McMurdo, Netwave and Kannad's maritime products, which are on OroliaMaritime.com.

Anyone looking for Kannad ELT information can find it on Orolia.com under Solutions, then Aviation. The Support button at top right on Orolia.com shows how to ask for support on any product by brand.

For maritime and SARSAT product support, OroliaMaritime.com has a similar Support button at top right, where you can find product support for McMurdo, Netwave and Kannad Maritime products.

Sarbe beacons (such as FastFind)

PRODUCTS FROM OTHER DIVISIONS

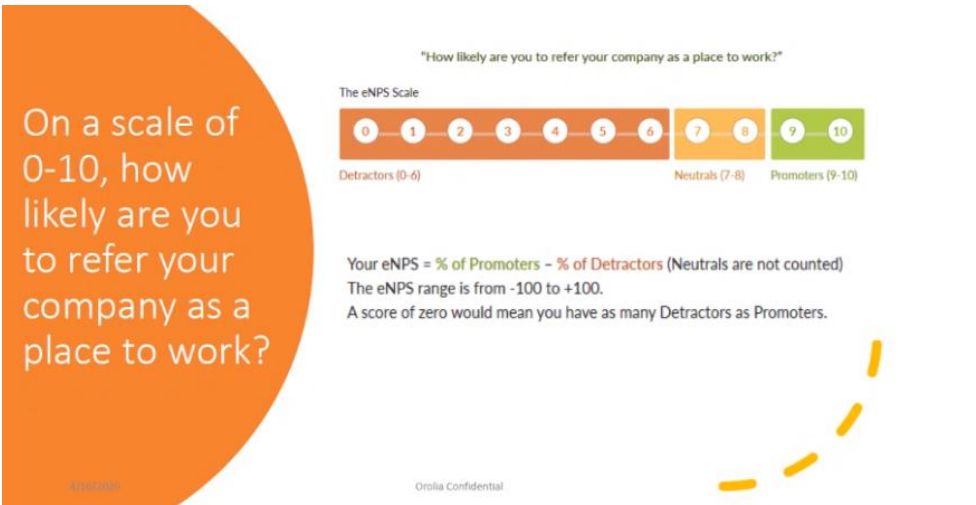
SARBE – Military Beacons for Personnel Recovery

- Locator beacons, Position Identity Tracking, ELTs
- Tri-Force users on every continent for over 70 years
- U.S. Army contract win - SARBE FastFind Personnel Recovery Device



Net Promoter Score (eNPS system)

Range of scores: 0 to 10 (where 10 is best)



- **Promoter:** 10 or 9
- **Neutral:** 8 or 7
- **Detractor:** 6 and below

Overall score: %Promoters

– %Detractor

Total NPS Score

	Life			Business	TS	OA
Response Rate	13%	4%	9%			
Promoters	21	2	23	72%	78%	40%
Neutrals	3	2	5	16%	11%	40%
Detractor	3	1	4	13%	11%	20%
					67%	20%
Monthly Score				59%	67%	20%

Sales/Repairs in Rochester

A) Sales

B) RMA's / Repair pricing

➤ Refer to either:

- <I:\Customer Service\Repair information>
- Sharepoint:
https://oroliagroup.sharepoint.com/sites/serviceteam/_layouts/15/WopiFrame.aspx?sourcedoc={03459565-9C36-44F0-BE73-E15EBCFDA509}&file=Spectracom%20repair%20pricing%20document.doc&action=default

Salesforce Price Books

Spectracom Repair Prices <https://orolia.lightning.force.com/lightning/r/Pricebook2/01sC00000007s4tIAA/view>

Note: if the **Details** tab is selected, switch to the **Related** Tab to see all the data.

**SpectraTime Repairs/RMAs

- Procedure for SpectraTime RMA's: <I:\Customer Service\Spectratime RMAs>
- The **Spectratime RMA form** is on the Support site and found here: <https://www.orolia.com/sites/default/files/document-files/QF%2004%20011%20%20Product%20return.pdf>

Point of contact for SpectraTime (in Les Ulis)

Walter Rojas

Per Wade Sober "Spectratime Clock related inquiries, please reach out to Walter Rojas – walter.rojas@orolia.com 585-321-5832
- All other inquiries please email **sales@orolia.com**"

Florise Breiner florise@spectratime.com

Email from Eric Girard (Oct 2020) I will forward this to Florise who also work for Spectratime

**Repair centers

***APAC (Asia/Pacific) Singapore (Danny Loke)

Danny LOKE

Applications Engineer

kokseng.loke@orolia.com

Mobile: +65 96544462

Skype: kokseng.loke@orolia.com

OROLIA ASIA PACIFIC PTE LTD

pg. 25

PLAZA 8@CBP
1 Changi Business Park
Crescent #03-08A Plaza 8 @ Changi Business Park,
Singapore 486025

*****EZU (Hong Kong)**

Janis Lee - Senior Administrative Officer
EZU Rentals Ltd
EZU Calibration Lab is ISO17025 accredited
Direct Line: +852-2666-2068
www.ezu.hk
janis@ezu.hk

*****Aimil (India)**

SCATS (shipping labels for Northrop Grumman)

- See Caitlin for info or assistance with this.

Email from Caitlin B (3 Jun 16) SCATS is a website that Northrop Grumman uses to make shipping labels. I will need the ship date, weight and dimensions of the shipment. Then on the ship date, I go into the website, create the labels and give them to shipping.

FMECA (Failure Mode, Failure Mechanism, Failure Effect, Failure Detection Method and probability)

Email from John Fischer (19 July 2016) Tony,
I think what they are looking for is what we used to call FMECA – Failure Modes, Effects, and Criticality Analysis. It's related to the MTBF calculation, but goes a step further. For example, in a SecureSync, if the front panel display fails, do you count it against the MTBF? Probably not since it is not a mission critical failure. A fan failure is more difficult – eventually it might cause a mission critical failure, but maybe not. So you do an analysis, looking at all the possible failure modes, their probability of occurring, and the critical effects they might cause.

Ryan has his hands full with another high priority issue at the moment, so let me help here by pulling in Laurent and Justin. We might have something here, but we might not.

1PPS / Antenna cable delay calculations

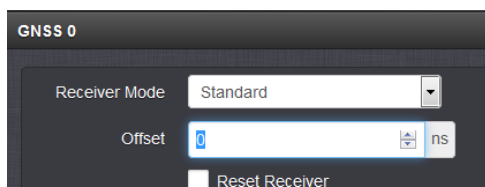
Configuration via Model

A) Legacy VelaSyncs

- Refer to “**Cable Delay for GPS:** in the Legacy VelaSyncandGeoCustAssist doc: <..\Legacy VelaSyncAndGeoCustAssist.pdf>

B) SecureSync/Model 9400 series NTP servers:

1. Newer browser: Interfaces -> GNSS 0 page, press Edit, Offset field



2. Classic interface browser: Setup -> Inputs -> Onboard reference page of the browser, “Offset” field)

C) Acutime antenna cable delay (for TSAT and TSync boards with external GPS input)

With the Acutime GPS antennas, David Higgins with CCUR emailed me:

For whatever reason this order was for a TSyncE-PCIe, which comes with a Trimble Acutime Gold external receiver, and for that unit the inter-connect is a multi-wire cable, not a length of coax. I measured ~1.7 nS/foot for the supplied cable – this value assumes the cable is 100 feet long (I didn’t uncoil and measure it).

A Wikipedia article mentions that plenum data cable typically has velocity factors ranging from 0.42 to 0.72, which is a bit slower than coax (Times Microwave’s datasheet for LMR-400 gives the VF as 85%). So I guess I can believe my measured value. If you have a more authoritative value for whatever cable is being used with the Acutime Gold I’d appreciate it, but I think I’m in the ballpark.

Email Dave Lorah sent to a customer (9 Nov 2012)

The cable used for the External Acutime antenna is simple copper multi-conductor cable. The typical velocity of propagation for copper cable is .66, so the 100 foot cable would result in a 66nS delay. This is not even worth bothering to enter a cable delay for.

1PPS Delay values for various cable types (Fiber and coax)

Fiber Optic cable delays

- ~5 nS for 1m fiber optic cable (from the Optical Zonu data sheet excerpted below)

SYSTEM SPECIFICATION

Frequency Range	1 GHz – 2 GHz
Noise Figure P2P	3.3 dB (GPS antenna Gain not included)
IIP3	-10dBm
Link Gain	42 dB (GPS antenna Gain not included)
Group Delay	< 1nS
Fiber Optic Cable	~5 nS for 1m fiber optic cable
Power	Master Unit: 110-240V AC or -48VDC
RF Connector	50 Ohm SMA
Bias-T Option	+5V or +12V
Fiber Optic	SC/APC (LC/APC or FC/APC are optional)

Coax cable 1PPS delays

A) For cable type RF400/RG-8 (CAL7-XXX) use 1.17ns per foot (3.84ns/meter)

➤ **Actual cable used:** Belden RF400 (RG-8)

<http://www.datasheetarchive.com/dl/Datasheet-026/DSA00451533.pdf> (page 2 “Nominal delay)

(loss for feet of cable= Multiply 1.17 times the feet of cable)

Examples:

- 100 foot cable= enter 117 ns
- 200 foot cable= enter 234 ns
- 300 foot cable= enter 351 ns
- 400 foot cable= enter 468 ns
- 500 foot cable= enter 580 ns

B) For Plenum cable type LMR-400/(CAL7P-XXX) use 1.34ns per foot.

➤ **Actual cable used:** Times Microwave LMR-400-LLPL

<http://www.timesmicrowave.com/products/lmr/downloads/82-85.pdf> (page 2 time delay)

(Multiply 1.2 times the length of cable)

Examples:

- 100 foot cable= enter 134 ns
- 200 foot cable= enter 268 ns
- 300 foot cable= enter 402 ns
- 400 foot cable= enter 536 ns
- 500 foot cable= enter 670 ns

C) For cable type RG-58/U (CA01-XXX) use 1.54ns per foot.

➤ **Actual Cable used:** Belden 8259

<http://www.belden.com/techdatas/english/8259.pdf> (page 2 nominal delay)

(Multiply 1.54 times the length of cable)

D) For cable type RG-8 (CAL7-XXX) use 1.17ns per foot.

➤ **Actual cable type used:** Belden 7810A

<http://pdf2.datasheet.su/belden/7810a%20010500.pdf> (page 2 nominal delay).

(Multiply 1.17 times the length of cable)

Ethernet/network cable loss/cable delay/cable attenuation calculator

- Refer to calculator at:
<http://www.timesmicrowave.com/calculator/?productId=123&frequency=1500&runLength=100&mode=calculate#form>
- 1) Select desired type of cable
 - 2) Enter frequency as “**1500**”
 - 3) Enter Run length as “**100**”

Cable impedance (50 ohm versus 75 ohm)

Q Will RG-59 (75 ohm cable - not 50 ohm) work with the raw GPS signal and the down-converted GPS signal?

A Per Tom Richardson (9 May 16) "Short answer is yes. There might be some mismatch because of the different impedance but it should be minimal"

For more info on transmission line impedance, refer to sites such as:

<http://www.bluejeanscable.com/articles/impedance.htm> (info from this informational site excerpted below):

Transmission Line Impedance:

So, when we say that the input impedance of your TV's composite video jack is 75 ohms, that's what we mean. But what does it mean to say that the impedance of the cable between the VCR and TV is 75 ohms? Well, first, it doesn't mean that the cable itself presents a 75 ohm load. If it did, the total load would now be 150 ohms, and you'd have an impedance mismatch. Furthermore, if the cable itself constituted a 75 ohm load, that load would be dependent on length--so a cable twice as long would be 150 ohms, a cable half as long would be 37.5 ohms, and so on.

And, in case it's not obvious by now, another thing that it doesn't mean is that the resistance of the cable will be 75 ohms. Since a simple volt-ohmmeter will measure resistance, we sometimes will get a call from a customer who says that he's measured his cable and it isn't anywhere close to 75 ohms. But resistance, which also confusingly happens to be measured in ohms, has nothing to do with characteristic impedance, which can't be measured by using a VOM.

When we say that the characteristic impedance of a cable is 75 ohms--or 50, 110, 300, or what-have-you--what we mean is that if we attach a load of the specified impedance to the other end of the cable, it will look like a load of that impedance regardless of the length of the cable between. The object of a 75 ohm cable is simply to "carry" that 75 ohm impedance from point A to point B, so that as far as the devices are concerned, they're right next to one another. If we take a hundred feet of 300-ohm television twin-lead cable, solder it to RCA connectors, and stick that in between the TV and VCR, the load, as "seen" by the VCR, will not be 75 ohms. How bad the mismatch is, and what the consequences of it are, will depend on a variety of factors, but it's fair to say that this sort of mismatch needs to be avoided.

So, Why's It Important?

Transmission line impedance is critical in some applications, and not so critical in others. In analog audio, particularly, impedance is basically a nonfactor--because at the relatively low frequencies involved in analog audio, and at anything approaching ordinary lengths, any reasonably designed cable will effectively "pass through" the impedance of the devices at either end--and the input and output impedances of line-level analog audio devices themselves are usually not critical. For analog audio cables, other design considerations like shielding and capacitance may be very important, but impedance really is not.

But the behavior of cables changes as signal frequencies increase. This is so because as frequency increases, the electrical "wavelength" of a signal becomes shorter and shorter; at video frequencies, signal wavelength is short enough to start causing problems. As the length of a cable becomes closer to a large fraction of the electrical wavelength of the signal it carries, the likelihood of significant, picture-altering reflections from impedance mismatch increases. The whole cable can resonate at the wavelength of the signal, or of a portion of the signal, and the impact on signal quality will be anything but good. Video signals, too, are complex; they occupy not a single frequency, but a whole range of frequencies--this is why we so often speak of the "bandwidth" of a signal--and so a mismatch will affect different parts of the signal differently.

Because the effects of impedance mismatch are dependent upon frequency, the issue has particular relevance for digital signals. Where analog audio or video signals consist of electrical waves which rise or fall continuously through a range, digital signals are very different--they switch rapidly between two states representing bits, 1 and 0. This switching creates something close to what we call a "square wave," a waveform which, instead of being sloped like a sine wave, has sharp, sudden transitions (in practice, the "square waves" in digital signals aren't really quite square). Although a digital signal can be said to have a "frequency" at the rate at which it switches, electrically, a square wave of a given frequency is equivalent to a sine wave at that frequency accompanied by an infinite series of harmonics--that is, multiples of the frequency. If all of these harmonics aren't faithfully carried through the cable--and, in fact, it's physically impossible to carry all of them faithfully--then the "shoulders" of the digital square wave begin to round off. The more the wave becomes rounded, the higher the possibility of bit errors becomes. The device at the load end will, of course, reconstitute the digital information from this somewhat rounded wave, but as the rounding becomes worse and worse, eventually there comes a point where the errors are too severe to be corrected, and the signal can no longer be reconstituted. The best defense against the problem is, of course, a cable of the right impedance: for digital video or SPDIF digital audio, this means a 75 ohm cable like Belden 1694A; for AES/EBU balanced digital audio, this means a 110 ohm cable like Belden 1800F.

Choosing the Right Impedance Cable and Connectors:

Fortunately, for most applications, it's very easy to choose the right impedance cable. All common home analog video standards use 75 ohm cable, as do coaxial digital audio connections. If you have balanced AES/EBU type digital audio lines, you'll want 110 ohm AES/EBU cable. There are a few others you may bump into, however, and it's good to be aware of them. RG-58 coax, such as is often used for coaxial computer network connections or for CB or ham radio antenna lines, is 50 ohms--not suitable for video use. Twin-lead cable--the two wires separated by a band of insulation that used to be the most common way to hook up a TV antenna--is a 300 ohm balanced line, also unsuited for home video interconnection, and if you need to hook a 300 ohm antenna line to a 75 ohm video jack, or a 75 ohm antenna line to an old two-screw antenna connection on your TV, you'll want a little impedance transformer/balun, readily available at any electronics shop, to link the two properly.

Connectors have impedance, too, and should be matched to the cable and equipment; many BNC connectors, especially on older cables, are 50 ohm types, and so it's important to be sure that you're using 75 ohm BNCs--like those from Canare--when connecting video lines. RCA connectors can't quite meet the 75 ohm

impedance standard because their physical dimensions just aren't fully compatible with it, but there are RCA plugs--Canare, again, being a prime example--which are designed for the best possible impedance match with 75 ohm cable and equipment.

Transmission line impedance can be a bit confusing, and of course this discussion just scratches the surface; but we hope it's been helpful to you in understanding just what "impedance" means and why it's important in video and digital audio applications.

Antenna cabling

Our Standard length CA01xxx and CA07xxx coax cables

Standard cable lengths we offer (See Sales to confirm, this list was made a long time ago)

- CA01 BNC to BNC cables (ft): 10, 25, 50, 100 and 200
- CA01-BNBN-4xxx (such as CA01-BNBN-4010 for 10 foot cable)
- CA07 RF400 (RG-8) cables (ft): 10, 25, 50, 100, 200 and 300
- CA01-0N0N-3xxx (such as CA01-0N0N-3025 for 25 foot cable)

UL94HB level rating (Flammability Standard)

- Refer to sites such as <http://web.rtpcompany.com/info/ul/ul94hb.htm> (excerpt below)

Requirements for HB certification

- A) The specimens may not have a burn rate exceeding 40 mm per minute over a 75mm span for specimens having a thickness of 3.0 mm to 13 mm, or
- B) The specimens may not have a burn rate exceeding 75 mm per minute over a 75mm span for specimens having a thickness less than 3.0 mm, or
- C) The specimens cease to burn before the flame reaches the 100mm mark.

(CA01-0N0N-xxxx GNSS antenna cables)

Variants of CA01-0N0N-XXXX cables we offer

- **CA01-0N0N-3xxx: Belden 7810A (“RF-400”)** Low loss antenna cable for indoor/outdoor use (used to be our P/N CAL7xxx cable, such as CAL7100)
- **CA01-0N0N-6xxx: Times Microwave (“LMR-400-LLPL”)**, Low loss antenna cable, **indoor** and **Plenum-rated** (used to be our P/N CALP7xxx, such as CALP7100)
- **CA01-0N0N-9xxx: Times Microwave (“LMR-40-DB”)** Low loss antenna cable, outdoor/watertight

(CA01-0N0N-3xxx) Belden 7810A (RF-400) / or can be Times Microwave LMR-400 cable

- Our P/N for the raw cable itself (no connectors/not cut to length: **W010-L400-0102** (in Arena https://app.bom.com/items/detail-sourcing?item_id=1289123760&version_id=11765886448)
- This is our standard (non-Plenum rated) antenna cable (example in Arena at: https://app.bom.com/items/detail-sourcing?item_id=1289123760&version_id=11765886448)
- Belden makes a Times Microwave LMR-400 equivalent cable known as Belden P/N: **7810A RF400** (Wireless 6GHz 50 ohm). This is the cable that we currently ship to customers.
- **Refer to sites such as:**
https://catalog.belden.com/index.cfm?event=pd&p=PF_7810A
<https://edeskv2.belden.com/Products/index.cfm?event=showproductdetail&partid=1820> or
<http://www.datasheetarchive.com/dl/Datasheet-026/DSA00451533.pdf> for the cable specs
- **Shortcut to LMR-400/RF400 Manufacturer data sheets:** <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\Antenna cables>

Mfg/ Mfg. P/N: Belden 7810A (Belden RF-400) (RG-8)

Our P/N: CA01-0N0N-3xxx (such as “**CA01-0N0N-3025**” for 25 foot cable, OR “**CA01-0N0N-3400**” for 400 foot cable)

Data sheet for our Belden RF-400 cable

Q Could I get some documentation on this series of cables, please? I would like to spec a few different lengths.

A reply from Dave Lorah (10 Mar 17) Answer; We do not have a specific data sheet or written documentation on cable. We use a LMR400 type cable for low loss at the GPS Frequency.



Low-loss GPS RF Cable

Spectracom offers LMR-400 equivalent cable assemblies terminated with type N connectors. Order CAL-7xxx, where xxx = length in feet. Contact us for special requirement cable.

The cable comes in various standard and also custom lengths. If you need pricing, please contact

Fire retardancy of Belden 7810A/Times Microwave LMR-400

- Refer also to the following (previous) section of this doc: [UL94HB level rating \(Flammability Standard\)](#)
- For plenum-rated cable (for flame retardancy) refer to: [CAL7xxx cable \(Plenum grade Times Microwave LMR-400 cable\)](#)

A) CA01-0N0N-3xxx antenna cable (our standard cable- used to be CAL7xxx cable)

Q What is the UL94HB level (V2, V1, V0, 5VB, 5VA) for the Antenna cable (CAL710)

A Email from Josh to TOYO (12 Jan 18) We have just got confirmation that the LMR cable in our price lists does not have a UL94HB level rating. In lieu of their urgency to purchase our time server, I recommend that we do not sell them our cable, but that TOYO looks for cable sources whose products have UL94HB rating.

B) CA01-0N0N-6xxx: Times indoor/Plenum Rated cable (used to be CALP7xxx cable) Temperature and Fire ratings of Time LMR-400 cable (per Times Microwave)

From: Mendenhall, Rachel (Times Microwave, US) [<mailto:Rachel.Mendenhall@timesmicro.com>]
Sent: Wednesday, April 22, 2015 1:00 PM
To: Jeremy Onyan
Subject: LMR-400

Per our phone conversation today, please find the temperature rating specs for the LMR-400 as follows.

Installation Temperature Range -40/+185 -40/+85
Storage Temperature Range -94/+185 -70/+85
Operating Temperature Range -40/+185 -40/+85

There is no fire rating on this cable, would be LMR-400-FR.

For Sales and technical information on LMR 400, contact Times Microwave Systems at 203-949-8400. They are in Wallingford, CT.

UL/ELV ratings, CE Declaration of Conformity/RoHS statements for CA01-0N0N-3xxx

(used to be CAL7xxx cable)

- The Declaration of Conformity for the CA01-0N0N-3xxx cable is included in the SecureSync's Declaration of Conformity Certificate.
- Refer to: <\\rocfnp02\drive\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\CE Declaration of Conformity>
- Refer to Belden 7810A datasheet at: https://catalog.belden.com/index.cfm?event=pd&p=PF_7810A

Standards and Compliance	
Environmental Suitability:	Indoor/Outdoor, Indoor
Sustainability:	CA Prop 65
European Directive Compliance:	EU CE Mark, EU Directive 2015/863/EU, EU Directive 2011/65/EU (ROHS II), EU Directive 2012/19/EU (WEEE)
APAC Compliance:	China RoHS II (GB/T 26572-2011)

Per Dave Sohn (15 Jun 15): it includes EN 60950-1:2006/A11:2009 for safety. We don't test to EN61000-6-1:2007 or EN 61000-6-3:2007, instead testing against EN 55022:2006/A1:2007 for Class A emissions, and EN55024:1998/A2:2003 for immunity.

RoHS statements

- A) **Belden cable:** in Arena at: https://app.bom.com/supplier-items/detail-compliance?item_id=1289113123&version_id=
- B) **Time Microwave cable:** The **RoHS** statement for **Times Microwave** cable is at: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\Antenna cables>

Minimum Bend Radius for cable(Install)/Minor Axis

- The *minimum bend radius* is the [radius](#) below which an object such as a [cable](#) should not be bent.
- minimum recommended bend radius for LMR-400 or equivalent cable is **4 inches Min**

info below from https://www.anixter.com/en_us/resources/literature/wire-wisdom/minimum-bend-radius.html

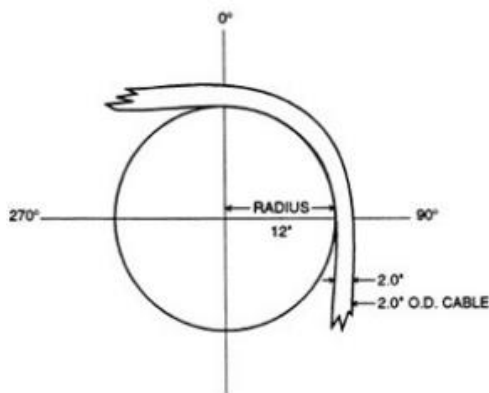
The minimum bend radius is the smallest allowed radius the cable is allowed to be bent around. During installation, [cables](#) are bent or flexed in various environmental conditions. Cables are often bent around a curve in conduits or underground ducts. Cables are also bent when [pulling a cable](#) around a sheave, which is a pulley set up in a manhole to help ease a cable around a curve.

Cables are composed of different components that may become compromised if bent too far and stress is placed on the cable. For example, while bending a medium-voltage cable consisting of a copper tape shield, the cable may form cracks in the outer jacket. To prevent cable damage, cable standards such as The National Electrical Code (NEC) and the Insulated Cable Engineers Association (ICEA) formed requirements for minimum bend radius.

How to Calculate Minimum Bend Radius?

Figure 1 shows a cable with an outer diameter of 2 inches being bent around a radius of 12 inches. The minimum bend radius is based on the diameter of the cable and the type of cable. The following formula is used:

$$\text{Minimum Bend Radius} = \text{Cable Outer Diameter} \times \text{Cable Multiplier}$$



Minimum Bend Radius

Belden RF400 Cable loss/Attenuation

- 5.3 dB/100 feet

From <http://www.datasheetarchive.com/dl/Datasheet-026/DSA00451533.pdf>

Max. Attenuation :				
Description	Frequency (MHz)	Start Frequency (MHz)	Stop Frequency (MHz)	Max. Attenuation (dB/100 ft.)
	30			0.70
	50			0.93
	150			1.58
	220			1.94
	450			2.83
	900			4.06
	1500			5.32
	1800			5.98
	2000			6.35
	2500			7.08
	3000			7.97
	3500			8.80
	4500			10.23
	5800			12.00
	6000			12.73

Belden RF400/RG-8 Exterior use/suitability

From <http://www.datasheetarchive.com/dl/Datasheet-026/DSA00451533.pdf>

Environmental Specifications

	°F	°C
Installation temperature range	-40/+185	-40/+85
Storage temperature range	-94/+185	-70/+85
Operating temperature range	-40/+185	-40/+85

SUITABILITY:

Suitability - Outdoor	Yes
Suitability - Aerial	Yes - When supported by a messenger
Suitability - Burial	Yes
Suggested Connectors	Mates with 9913 and Land Mobile Radio type connectors.

PLENUM/NON-PLENUM:

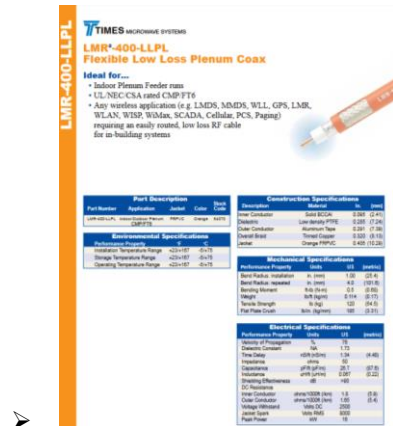
Plenum (Y/N)	N
--------------	---

CA01-0N0N-6xxx (Plenum-rated Times LMR-400-LLPL cable) (was CALP7xxx cable)

We offer Times Microwave LMR-400-LLPL plenum-rated coax cable

- Here's a link to the Cable Datasheet: <https://www.timesmicrowave.com/documents/resources/LMR-400-LLPL.pdf> (or in Arena for an internal-only link) <https://files.bom.com/download/uMoCNgOwDjQu1sr7QN8AcMqSuQs8PILF/qcxguahmeykoxarvgktiwigeddpqxhhml/LMR-400-LLPL.pdf>

Times Microwave P/N: LMR-400-LLPL



Visual part#: CA01-0N0N-6xxx (CA01-0N0N-6100, 100 ft cable, in Arena):

https://app.bom.com/items/detail-spec?item_id=1203165779&version_id=10299090608

RoHS statement for Times Microwave cable

Note: The RoHS statement for Times Microwave cable is at: <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\Antenna cables>

CA01-0N0N-6xxx (CALP7) specs

Flame retardancy/toxicity

Jim Allocco found the following statement on the Internet:

"CATVP (Plenum cable) is the highest rated cable jacket type. Plenum cables can be used anywhere within a building. It has a slow burn rate and emits lower toxic fumes when burning. Plenum cable is typically color coded white, and costs about 75% more than standard cable for similar electrical performance. Plenum cable will often not withstand outdoor conditions as well as standard cable."

Temperature ratings

Environmental Specifications		
Performance Property	F	C
Installation Temperature Range	+23/+187	-5/+75
Storage Temperature Range	+23/+187	-5/+75
Operating Temperature Range	+23/+187	-5/+75

Electrical specs

Electrical Specifications			
Performance Property	Units	US	(metric)
Velocity of Propagation	%	78	
Dielectric Constant	NA	1.73	
Time Delay	nS/ft (nS/m)	1.34	(4.40)
Impedance	ohms	50	
Capacitance	pF/ft (pF/m)	28.7	(87.6)
Inductance	uH/ft (uH/m)	0.087	(0.22)
Shielding Effectiveness	dB	>90	
DC Resistance			
Inner Conductor	ohms/1000ft (/km)	1.8	(5.9)
Outer Conductor	ohms/1000ft (/km)	1.65	(5.4)
Voltage Withstand	Volts DC	2500	
Jacket Spark	Volts RMS	8000	
Peak Power	kW	16	

Weatherability/Outdoor use of Times Plenum cable

- Orange jacketed Plenum cable is NOT intended for outdoor use (black jacket plenum is OK)

Weatherability: LMR-400-LLPL cables are designed for **indoor** Plenum applications. Black jacketed LMRLLPL versions can be supplied for applications that originate outdoors (e.g., rooftop) and subsequently enter the building. (Note we don't offer the black jacket plenum cable).

For Sales and technical information on LMR 400, contact Times Microwave Systems at 203-949-8400. They are in Wallingford, CT.

The specs are as follows:

Cable loss:	5dB/100Feet	LMR-400	Standard outdoor
inner conductor:	0.108 in		-DB Watertight
Dielectric:	0.285 in		-FR Fire Retardant
Outer conductor:	0.291 in		-PVC indoor cable
Overall braid:	0.320 in		-ULTRAFLEX
Standard jacket:	0.405 in	-LLPL	Plenum fire rated,

Min bend radius: 1 in (Note: The Belden cable we sell is 4 inch minimum)

Temp range: -40 F to +185 F

CA01-0N0N-9xxx (outdoor/watertight Times Microwave LMR-400-DB cable)


We offer Times Microwave LMR-400 plenum-rated coax cable

- Here's a link to the Times LMR-400 cable datasheet:
<http://www.timesmicrowave.com/documents/resources/LMR-400.pdf>

LMR-400

TIMES MICROWAVE SYSTEMS
LMR®-400
Flexible Low Loss Communications Coax
Ideal for...

- Drop-in replacement for RG-8/9913 Air-Dielectric type Cable
- Jumper Assemblies in Wireless Communications Systems
- Short Antenna Feeder runs
- Any application (e.g. WLL, GPS, LMR, WLAN, WISP, WiMax, SCADA, Mobile Antennas) requiring an easily routed, low loss RF cable
- **NEW!** Times Protect® LP-18-400 protector-series



Part Description					Stock
Part Number	Application	Jacket	Color	Code	
LMR-400	Outdoor	PE	Black	54001	
LMR-400-DB	Outdoor/Watertight	PE	Black	54091	
LMR-400-FR	Indoor/Outdoor Riser CMR	FRPE	Black	54030	
LMR-400-FR-PVC	Indoor/Outdoor Riser CMR	FRPVC	Black	54073	
LMR-400-PVC	General Purpose	PVC	Black	54218	
LMR-400-PVC-W	General Purpose	PVC	White	54204	

Construction Specifications		
Description	Material	In. (mm)
Inner Conductor	Solid BCCAI	0.108 (2.74)
Dielectric	Foam PE	0.285 (7.24)
Outer Conductor	Aluminum Tape	0.291 (7.39)
Overall Braid	Timed Copper	0.320 (8.13)
Jacket	(see table)	0.405 (10.29)

Environmental Specifications		
Performance Property	°F	°C
Installation Temperature Range	-40/+185	-40/+85
Storage Temperature Range	-94/+185	-70/+85
Operating Temperature Range	-40/+185	-40/+85

Mechanical Specifications		
Performance Property	Units	US (metric)
Bend Radius: installation	in. (mm)	1.00 (25.4)
Bend Radius: repeated	in. (mm)	4.0 (101.6)
Bending Moment	ft-lb (N-m)	0.5 (0.68)
Weight	lb/ft (kg/m)	0.068 (0.10)
Tensile Strength	lb (kg)	160 (72.6)
Flat Plate Crush	lb/in. (kg/mm)	40 (0.71)

Electrical Specifications		
Performance Property	Units	US (metric)
Velocity of Propagation	%	84
Dielectric Constant	NA	1.38
Time Delay	nS/ft (nS/m)	1.20 (3.92)
Impedance	ohms	50
Capacitance	pF/ft (pF/m)	23.9 (78.4)
Inductance	uH/ft (uH/m)	0.060 (0.20)
Shielding Effectiveness	dB	>90
DC Resistance		
Inner Conductor	ohms/1000ft (Ω/km)	1.39 (4.6)
Outer Conductor	ohms/1000ft (Ω/km)	1.65 (5.4)
Voltage Withstand	Volts DC	2500
Jacket Spark	Volts RMS	8000
Peak Power	kW	16

Visual part#: CA01-0N0N-9xxx ("CA01-0N0N-9100" 100 ft cable in Arena) https://app.bom.com/items/detail-spec?item_id=1247526868&version_id=10984681528

RoHS statement for Times Microwave cable

Note: The RoHS statement for Times Microwave cable is at: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\Antenna cables](#)

CA01-0N0N-9xxx specs

Flame retardancy/toxicity

Water-rating (LMR-400-DB)

Part Description					Stock
Part Number	Application	Jacket	Color		Code
LMR-400	Outdoor	PE	Black		54001
LMR-400-DB	Outdoor/Watertight	PE	Black		54091
LMR-400-FR	Indoor/Outdoor Riser CMR	FRPE	Black		54030
LMR-400-FR-PVC	Indoor/Outdoor Riser CMR	FRPVC	Black		54073
LMR-400-PVC	General Purpose	PVC	Black		54218
LMR-400-PVC-W	General Purpose	PVC	White		54204

Temperature ratings

Environmental Specifications		
Performance Property	°F	°C
Installation Temperature Range	+23/+167	-5/+75
Storage Temperature Range	+23/+167	-5/+75
Operating Temperature Range	+23/+167	-5/+75

Electrical specs

Electrical Specifications			
Performance Property	Units	US	(metric)
Velocity of Propagation	%	76	
Dielectric Constant	NA	1.73	
Time Delay	nS/ft (nS/m)	1.34	(4.40)
Impedance	ohms	50	
Capacitance	pF/ft (pF/m)	26.7	(87.6)
Inductance	uH/ft (uH/m)	0.067	(0.22)
Shielding Effectiveness	dB	>90	
DC Resistance			
Inner Conductor	ohms/1000ft (/km)	1.8	(5.9)
Outer Conductor	ohms/1000ft (/km)	1.65	(5.4)
Voltage Withstand	Volts DC	2500	
Jacket Spark	Volts RMS	8000	
Peak Power	kW	16	

Other cable types

*Times Microwave LMR-600 cable


- Refer to <http://www.timesmicrowave.com/documents/resources/LMR-600.pdf>

LMR-600

TIMES MICROWAVE SYSTEMS
LMR®-600
Flexible Low Loss Communications Coax

Ideal for...

- Jumper Assemblies in Wireless Communications Systems
- Short Antenna Feeder runs
- Any application (e.g. WLL, GPS, LMR, WLAN, WISP, WiMax, SCADA, Mobile Antennas) requiring an easily routed, low loss RF cable



Part Description

Part Number	Application	Jacket Color	Stock Code
LMR-600	Outdoor	PE Black	54003
LMR-600-DB	Outdoor/Waterlight	PE Black	54003
LMR-600-FR	Indoor/Outdoor Riser CMR	FRPE Black	54032
LMR-600-FR-PVC	Indoor/Outdoor Riser CMR	FRPVC Black	54074
LMR-600-PVC	General Purpose	PVC Black	54219
LMR-600-PVC-W	General Purpose	PVC White	54205

Construction Specifications

Description	Material	In. (mm)
Inner Conductor	Solid BCCAI	0.176 (4.47)
Dielectric	Foam PE	0.455 (11.59)
Outer Conductor	Aluminum Tape	0.491 (11.71)
Overall Braid	Tinned Copper	0.490 (12.45)
Jacket	(see table)	0.590 (14.99)

Mechanical Specifications

Performance Property	Units	US	(metric)
Bend Radius: Installation	in. (mm)	1.50	(38.1)
Bend Radius: repeated	in. (mm)	8.0	(152.4)
Bending Moment	ft-lb (N-m)	2.75	(3.73)
Weight	lb/ft (kg/m)	0.131	(0.20)
Tensile Strength	lb (kg)	350	(158.9)
Flat Plate Crush	lb/in. (kg/mm)	60	(1.07)

Environmental Specifications

Performance Property	Units	°C
Installation Temperature Range		-40/+185 -40/+85
Storage Temperature Range		-94/+185 -70/+85
Operating Temperature Range		-40/+185 -40/+85

Electrical Specifications


Performance Property	Units	US	(metric)
Velocity of Propagation	%	85	
Dielectric Constant	NA	1.32	
Time Delay	nS/ft (nS/m)	1.17	(3.83)
Impedance	ohms	50	
Capacitance	pF/ft (pF/m)	22.4	(76.6)
Inductance	uH/ft (uH/m)	0.058	(0.19)
Shielding Effectiveness	dB	>90	
DC Resistance	ohms/1000ft (ohms/km)	0.53	(1.7)
Inner Conductor	ohms/1000ft (ohms/km)	1.2	(3.9)
Voltage Withstand	Volts DC	4000	
Jacket Spark	Volts RMS	8000	
Peak Power	kW	40	

Q. Customer has asked me if he can use a LMR-600 cable instead of LMR-400 for the connection of GPS antenna to the SecureSync.

A (reply from Keith Wing) I would have to say "Absolutely" to this question. This cable is even better than the LMR-400 cable we offer. This cable can even run further than the 300 feet we spec (without a preamplifier being installed).

LMR-400 has a cable loss of about 5db/100 feet of cable at 1.5GHz. The specs on LMR-600 at the same frequency is about 3 to 3.5dB /100 feet of cable (it's a lower-loss cable). So it can run longer than 300 feet. Just note that this cable has a different diameter than LMR-400 cable. The connectors we send with the Model 8226 won't likely work with this cable. So type N Male connectors for LMR-600 should be purchased/installed on the cable.





Description
Specs
Reviews
All Lengths
Q & A
Accessories


[Click Here to Download the Spec Sheet](#)

Features & Specs

Cable Type	?	LMR-600
Impedance	?	50 ohms
Center Conductor	?	Bare Copper Covered Aluminum (BCCA)
Center Conductor Diameter	?	.179 inch
Dielectric	?	Foam PE (Polyethylene)
Jacket Material	?	Polyethylene (PE) (Indoor/Outdoor)
Cable Diameter	?	.59 inch
Minimum Bend Radius	?	1.5 inch
Operating Temperature Range	?	-40/+185°F
Attenuation 900 MHz/100 ft	?	2.5dB/100ft
Attenuation 2.4 GHz/100 ft	?	4.3dB/100ft
Attenuation 5.8 GHz/100 ft	?	7.3dB/100ft

You Might Also Like

*Times Microwave LMR-240 (“ultra-flex”)

- Refer to: <http://www.impulseelectronics.com/times-microwave-lmr-240-ultra-flex-coax-cable/>
- **Cable loss at 1.5GHz:** 11.85 dB/100 feet (32.4 dB/100 meters)

*Times Microwave LMR-195 cable

- Refer to: <http://www.danets.com/download/lmr-195%20spec.pdf>
- **Cable loss at 1.5GHz:** 14.5dB/100 feet

	10		100		1,000		10,000				
	Frequency (MHz)										
Frequency (MHz)	30	50	150	220	450	900	1500	1800	2000	2500	5800
Attenuation dB/100 ft	2.0	2.5	4.4	5.4	7.8	11.1	14.5	16.0	16.9	19.0	29.9
Attenuation dB/100 m	6.5	8.4	14.6	17.7	25.5	36.5	47.7	52.5	55.4	62.4	98.1
Avg. Power kW	0.89	0.68	0.39	0.32	0.22	0.16	0.12	0.11	0.10	0.09	0.06

Calculate Attenuation = $(0.366869) \cdot \sqrt{\text{FMHz}} + (0.000470) \cdot \text{FMHz}$ (interactive calculator available at <http://www.timesmicrowave.com>)
Attenuation: VSWR=1.0, Ambient = +25°C (77°F) Power: VSWR=1.0, Ambient = +40°C, Inner Conductor = 100°C (212°F),
Sea Level, dry air; atmospheric pressure; no solar loading

Environmental Specifications		
Performance Property	°F	°C
Installation Temperature Range	-40/+185	-40/+85
Storage Temperature Range	-94/+185	-70/+85
Operating Temperature Range	-40/+185	-40/+85

Mechanical Specifications			
Performance Property	Units	US	(metric)
Bend Radius: installation	in. (mm)	0.5	(12.7)
Bend Radius: repeated	in. (mm)	2	(50.8)
Bending Moment	ft-lb (N-m)	0.2	(0.27)
Weight	lb/ft (kg/m)	0.021	(0.03)
Tensile Strength	lb (kg)	40	(18.2)
Flat Plate Crush	lb/in. (kg/mm)	15	(0.27)



Construction Specifications			
Description	Material	In.	(mm)
Inner Conductor	Solid BC	0.037	(0.94)
Dielectric	Foam PE	0.110	(2.79)
Outer Conductor	Aluminum Tape	0.116	(2.95)
Overall Braid	Tinned Copper	0.139	(3.53)
Jacket	(see table above)	0.195	(4.95)

Flexibility and Bendability are hallmarks of the LMR-95 cable design. The flexible outer conductor enables the tightest bend radius available for any cable of similar size and performance.

Low Loss is another hallmark feature of LMR-195. Size for size LMR has the lowest loss of any flexible cable and comparable loss to semirigid hard-line cables.

RF Shielding is 50dB greater than typical single shield coax (40dB). The multi-ply bonded foil outer conductor is rated conservatively at >90dB (i.e. >180 dB between two adjacent cables).

Weatherability: LMR-100A cables designed for outdoor exposure incorporate the best materials for UV resistance and have life expectancy in excess of 20 years.

Electrical Specifications			
Performance Property	Units	US	(metric)
Cutoff Frequency	GHz	41	
Velocity of Propagation	%	80	
Dielectric Constant	NA	1.56	
Time Delay	nS/ft (nS/m)	1.27	(4.17)
Impedance	ohms	50	
Capacitance	pF/ft (pF/m)	25.4	(83.3)
Inductance	uH/ft (uH/m)	0.064	(0.21)
Shielding Effectiveness	dB	>90	
DC Resistance			
Inner Conductor	ohms/1000ft (lkm)	7.6	(24.9)
Outer Conductor	ohms/1000ft (lkm)	4.9	(16.1)
Voltage Withstand	Volts DC	1000	
Jacket Spark	Volts RMS	3000	
Peak Power	kW	2.5	

*Belden 9914 RG8-U cable

Email from Dave L to a customer (9/17/12)

The 9914 RG8-U type cable will work. It has a spec of **5.5 db loss per 100 feet** which is comparable to LMR400. There are a few varieties of RG8-U type cables with different specs, so the customer must make sure the cable loss does not exceed acceptable levels.

A) CA01-0N0N-XXX (RG-213 plenum cable we used to offer)

- Our P/N: CA01-0N0N cable:
- Refer to both <I:\Engineering\Engineering Shared\Spectracom parts\CA01-0000-1000> and <http://www.timesmicrowave.com/content/pdf/lmr/82-85.pdf>
- We ship the Times Microwave LMR-400-LLPL cable
- Minimum bend radius is 1 inch
- Cable loss at 1.5GHz: about 5.2 dB/100 feet

Info about using alternate coax cable types for GPS input

- Link to coax cable loss calculator: <I:\Customer Service\Cable loss calculator>

Receiver signal level requirements for “optimum operation”:

- **Trimble Res-T GPS receiver:** desires input of 20dB to 30dB.
- **Trimble Res-SMT-GG receiver:** desires input of 22dB to 30dB
- **Ublox M8T receiver:** desires input of 5dB to 20dB

Alternate cable types (RG-59, RG-59, RG-8/RF400, etc)

D) Single-shield cables

Reasons it's not recommended to use inexpensive cables (such as RG-58 or RG-59) with GPS

Email from Tom Richardson (8 Jan 2016) Not just the loss in the cable but also shielding effectiveness can come into this. If they get a less expensive RG-58 type cable, there can be poor shielding and possibility of interference or jamming. Also, I talked with an engineer at tallysman and a leaky cable can feed back into the antenna. With 40 dB of gain it doesn't take much to set up a feedback path and there is a possibility of jamming itself.

C) RG-174 (not recommended to run from the breakout to equipment)

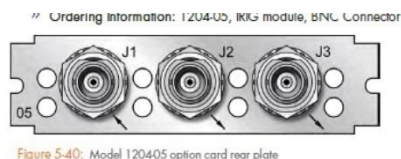
- Refer to Salesforce case 174338
- this cable is not recommended for distribution to equipment

Emails from Dave Lorah (24 Sept 2018)

I have researched the RG-174U cable you said was being used for the IRIG transmission. This may be the problem.

We usually specify an RG58 type cable for IRIG. The RG174U cable has roughly ten times the DC resistance of the RG-58 which might be attenuating the signal to the point the IRIG Slave will not recognize the waveform data. The Input will allow a wide range of signal from 500mV to 10Vp-p. If the IRIG Input signal level is below 500mV it will not recognize the signal.

The IRIG Slave SecureSync has one 1204-05 Option card installed. This card is different than the other 1204-15 IRIG Output cards as it has one IRIG Input and two outputs. This is what the card face looks like.



We use the RG-174 for this cable but it is limited to a maximum length of 15 Meters. Your RG-174 cable is approximately four times this length and would have a lot of signal attenuation. This is due to the electrical resistance of the 26 AWG wire in the RG-174 vs the 20 AWG in the RG-58 cable.

Tam is going to move the IRIG Slave unit close to the IRIG Master and check if it syncs with a shorter cable. This will prove the configuration is correct and the two units are working properly.

The RG-58 cable has about 1/10 the resistance of RG-174 and should be fine for 400 feet.

D) RG-59 cable (such as Belden 8241 or Belden 9104) or any other 75 ohm cable

Email from Tom Richardson (15 Feb 2013) RG-59 low loss will work, and I see it recommended over regular RG-58. This is same as yesterday's question. I assume it is the same customer with the pre-existing antenna feed. There is always a big discussion about the different impedances, but I think it came down to <1 or 2 dB.

Email from Matt Loomis (15 Feb 2013) The Belden (9104) RG-59 cable is Symmetricom's standard GPS cable for their timeservers (S200, S350, Xli, etc.). They recommend up to 150ft without a preamp. Adding an inline preamp for 150 – 300ft lengths.

E) RG-58 cable (such as Belden 8219, Belden 9104, Belden 8259)

- This is a 50 ohm cable (OK for GPS) but with very high cable loss at GPS Frequency (1.5GHz)
 - We recommend cable runs less than 100 feet total length.
 - We don't recommend combining this type cable with other cables, due to:
 - the high cable loss
 - Due to single shield (See email from Tom Richardson further above).
 - When used with the Model 8225(or comparable) antenna, cable loss is very high!
-

F) RG-58A (Belden 8219)

- 24dB/100 feet
-

G) RG-58C (Belden 8259) 32dB/100 feet

Note: If it's desired to use RG-58 cable for extended distance GPS cable runs, the customer can use our DUC Up/Down converter (instead of using an 8225 antenna/8226 surge suppressor). Because of the much lower frequency transmitted by the down converter antenna, the DUC kit allows for up to 1500 feet (457 meters) of RG-58 cable for GPS cable runs.

Refer to: [Raven Down-Up coax cable converters for GPS](#)

H) RG-8 cable (Belden RF400, Belden 7810A)

- This is 50 ohm (OK for GPS) double-shielded cable
 - **RG-8/U (Belden 8237)** 10 dB/100 feet cable loss
 - **RG-8/U (Belden 9913)** 6 dB/100 feet cable loss
 - **RG-8X (Belden 9258)** 20 dB/100 feet cable loss
-

I) Heliax/Superflex cables

- EXCELLENT very low loss cables for GPS
- Uses specialized connectors
- Very Low loss cable

- **1/2" SuperFlex** 4.6 dB/100 feet
- **3/8" SuperFlex** 4.5 dB/100 feet
- **Heliax:** 3 dB/100 feet

****Bent center plate on Type N connector (due to cross-threaded connector)**

One or more bent center plates has resulted in RF signal still getting to the receiver, but Antenna Problem alarm being asserted

- The condition of one of the four plates being spread out too far has resulted in at least one instance where the GPS RF signal was still getting in (receiver was tracking satellites) but the antenna problem alarm was still asserted.

Email Keith sent to a customer (2 Aug 16) regarding an RMA with internal coax cable replaced due to a bent plate- receiver still tracking satellites but Antenna Problem alarm was asserted

The picture below from the cable that was replaced shows exactly what the condition was and allows me to be able to easily explain what inadvertently happened to this connector after it was shipped from the factory.

The center of this rear panel connector that makes contact with the center pin of the building cable is formed by four small plates. The tech found that one of these plates had been pushed apart from the other three plates, affecting the shape of the center connection (the plate to the upper-left in the picture below):



When the building cable is attached to the back of the time server on this threaded connector, if this cable connector starts off as being cross-threaded (before being backed-off and reconnected), the center pin of the cable can go into these plates at an angle, causing one or more of the plates to be pushed apart from the others.

This picture above was a very peculiar incident in where there was just enough contact with the center pin that the GPS signal was still able to reach the GNSS receiver (it was still able to track satellites). But the 5vdc that is outputted from the receiver to power the antenna had less current than expected. The receiver was sensing this as an open in the antenna cable and therefore was asserting the Antenna Problem alarm (this alarm indicates the receiver is detecting either an open or short in the antenna cable). Normally if the receiver is able to track satellites, the 5vdc is fine so the antenna problem alarm wouldn't be asserted.

I have seen this condition with a bent plate happen before, where the cross-threaded connector has pushed the plates apart. But it usually causes a complete loss of RF and the antenna problem alarm to be asserted. This is the first I've seen where the plate being bent out still allowed RF to get through to the receiver, but also caused an issue with the 5vdc current draw.

Conduit interference (other cables run in same conduit as the antenna cable)

Q. We need to know if it would be ok to run a GPS antenna cable inside a conduit with electrical and radio circuits. Will the EMI or RFI cause a problem with the GPS signal?

A Email from Tom Richardson to Will Hickey (8 Feb 2013) Depends on a bunch of stuff. What are the frequencies of the signals in the conduit? What kind of cables are being used? What are the signal strengths of the signals in the cables? What are the shielding characteristics of the cables? Are all the cables bundled together? Etc...

GPS signals are at 1.575 GHz, signal levels -160 dBm let them know.

We run our cables in trays from the roof and I haven't seen any issues, but we separated the GPS lines from the other lines.

Adapters/Coax cable connectors

****Type N barrel connector (P/N 067022)**



- **Our P/N: 067022** (in Arena as an **obsolete** part): https://app.bom.com/items/detail-sourcing?item_id=1203165679&version_id=10294592738
- **Amphenol P/N:** 82-101-RFX
- Looks like we no longer offer this part. Salesforce doesn't list it as a product and Arena shows it being obsolete.
- Can be purchased elsewhere from places such as Mouser (the Mouser P/N is 523-82-101-RFX): <http://www.mouser.com/ProductDetail/Amphenol-RF/82-101-RFX/?qs=qhgJLQbFbXINLec6%2FCWtaQ%3D%3D>

****SMA to Type N adapter**



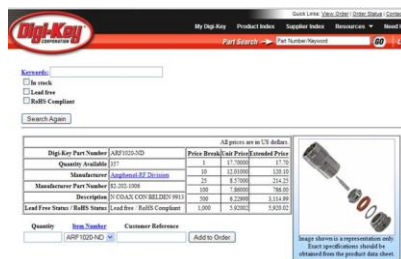
- **Our P/N:** ACC 325 (**PEN5-9350-0015** in Arena) https://app.bom.com/items/detail-spec?item_id=1202834983&version_id=10221283248
- **In SalesForce:** https://na28.salesforce.com/_ui/search/ui/UnifiedSearchResults?searchType=2&sen=00a&sen=0F9&sen=a04&sen=02i&sen=ka&sen=00O&sen=00Q&sen=001&sen=003&sen=a0A&sen=01t&sen=005&sen=500&sen=006&sen=810&str=+ACC+325+#!/fen=01t&initialViewMode=detail&str=ACC%20325
- **Fairview P/N:** SM4263
- **Microwave Dist P/N:** XNM-SF

Email from Tony Diflorio to a customer (18 Aug 15) I just confirmed that the connector on the receiver cable end is only available with an "N" connector. We no longer offer this antenna with SMA on the receiver cable end. However, we do offer an SMA Male to N Male adapter # ACC325. Price: \$120 each. See below: Will this work for you?

Type N connectors for cable termination

A) Field installable (no crimping) type N clamp connectors

- Two are supplied with each Model 8226 and 8227
- **Spectracom P/N:** P051-0001-0100 (in Arena): https://app.bom.com/items/detail-spec?item_id=1202844970&version_id=10221293598&orb_msg_single_search_p=1&redirect_segno=7712967562
- In SalesForce: <https://na28.salesforce.com/01tC00000039zC2?srPos=0&srKp=01t>
- **Mfg:** Amphenol
- **Amphenol P/N:** 82-202-1006
- **Digikey P/N:** ARF1020-ND
- **Link to Digikey:** (<http://www.digikey.com/classic/Ordering/AddPart.aspx>)



Cable preparation/cut dimensions

These field-installable connectors provided with the Model 8226 surge suppressor are Amphenol P/N 82-202-1006.

The following link provides the dimensions for prepping the end of the cable to install the connector:
<https://www.amphenolrf.com/media/downloads/60/280.pdf>

B) Type N crimp-style connectors we use to pre-terminate CA01(CAL7) cables at the factory

- Shortcut to information on this part: <I:\\Engineering\\Engineering Shared\\Spectracom parts\\P050-0010-xxxx>

The crimp-style connector we use to pre-terminate the CALXXX cables:

Our P/N: P050-0010-0100

Mfg P/Ns:

- AMPHENOL 82-340-1052
- RF Industries RFN-1006-3I
- Times Microwave Systems TC-400-NM
- Amphenol Connector 172102H243

Type N connector dimensions for cable/conduit recommendations

Our type N Connector outside dimension (across from side to side) .8 inches (just under 1 inch)
<http://www.jameco.com/wcsstore/Jameco/Products/ProdDS/567736.pdf> (connector datasheet)

Based on size of the connectors, the minimum recommended diameter for conduit would be 1 ½ inches for each cable to be run through the conduit to ensure ample space for connectors. So for two cables, we would recommend a 3 inch conduit. However, if it's desired to use smaller conduit, they can cut the connectors off the cables and then re-install the connectors after the cable has been run through the conduit.

LMR-400 specs/ Connector specs

<http://www.timesmicrowave.com/content/pdf/lmr/22-25.pdf>

For Sales and technical information on LMR 400, contact Times Microwave Systems at 203-949-8400. They are located in Wallingford, CT. The specs are as follows:

Cable loss:	5dB/100Feet	LMR-400	Standard outdoor
inner conductor:	0.108 in		-DB Watertight
Dielectric:	0.285 in		-FR Fire Retardant
Outer conductor:	0.291 in		-PVC indoor cable
Overall braid:	0.320 in		-ULTRAFLEX
Standard jacket:	0.405 in		-LLPL Plenum fire rated,

Min bend radius: 1 in (**Note:** The Belden cable we sell is 4 inch minimum)

Temp range: -40 F to +185 F

Formula for calculating allowable cable length/configurations

Link to the auto-cable loss calculator: [cable loss calculator.xls](#)

8225= 30dB (antenna) – (cable loss) + 20dB (Preamp if used) – (.5dB/connector) = XXdB
ANT35= 35dB (antenna) – (cable loss) + 20dB (Preamp if used) – (.5dB/connector) = XXdB

918X/TTSxxx/8195B= XX dB should be between 18 dB to 36dB

818x/8195/8195A = XX dB should be between 10 dB to 33dB

Cable loss (Place preamp at 10dB loss location)

- **Andrews Heliax ½ in:** 2.7dB/100 (Requires special connectors and training to install).
- **Andrews Heliax 5/8 in:** 2.07dB/100 (Requires special connectors and training to install).
- **LMR-400:** 5.5dB/100
- Belden 8267 (RG-213): 10db/100

Maximum cable distances with LMR-400 (RF400):

- **918x products:** Up to 200 feet without Preamp. Up to 600 feet with preamp
- **8183- 819X products:** Up to 350 without a preamp. Up to 600 feet with a preamp.

- **928X products:** Up to 150 feet without preamplifier. Up to 500 feet with a preamp.
- **938x products:** Up to 300 without a preamp. Up to 600 feet with a preamp.
- **SecureSync/9400s with Res-T GPS receivers** (prior to ~Oct 2013): Up to 300 without a preamp. Up to 600 feet with a preamp.
- **SecureSync/9400 with Res-SMT GPS receivers and 8230 GPS antenna** (prior to ~Oct 2013): Up to 300 without a preamp. Up to 600 feet with a preamp.

Note: The Trimble GPS Receiver will handle two 8227 preamps to extend the cable length. (55mA max) (Bear Sterns used it.)

Maximum cable distances with RG-213 (Belden 8267) cable

- **8183- 819X products** - Up to 200 feet without a preamp. Up to 400 feet with a preamp.
- **918x products** -Up to 120 feet without a preamp.

Minimum Cable distances (818x series only)

Due to unique system dynamics of the antenna, amplifier and receiver, a minimum of cable length of 450 feet (24 dB cable loss) is required to prevent overloading the GPS receiver used in the Models 8183, 8183ES and 8189. The GPS receiver used in all other Spectracom products do not require a minimum cable length.

5VDC voltage drop through long antenna cable runs

- Refer to sites such as: <http://www.calculator.net/voltage-drop-calculator.html>
- Minimum DC voltage to power the Timing 1000 GPS antenna is 4.5vdc.
- Timing 1000 antenna current draw is 27ma
- Model 8227 preamp current draw is 15ma

Example below is based on 1500 feet (457 meters) of Belden RF400/RG-8 (10 AWG wire) with 27ma for the antenna and 15ma for Model 8227 also installed inline (42 ma total)

Voltage Drop Calculator

Results:

Voltage drop: **0.13**

Voltage drop percentage: **2.71%**

Voltage at the end: **4.67**

Please note that the result is an estimation based on normal condition. The actual voltage drop can vary depend on the condition of the wire, the conduit being used, the temperature, the connector, the frequency etc. But, in most cases, it will be very close.

Wire Material	Copper
Wire Size	10 AWG (10.4 kcmil)
Voltage	4.8
Phase	AC single phase
Number of conductors	single set of conductors
Distance	1500 feet
Load current	.042 Amps
Calculate	

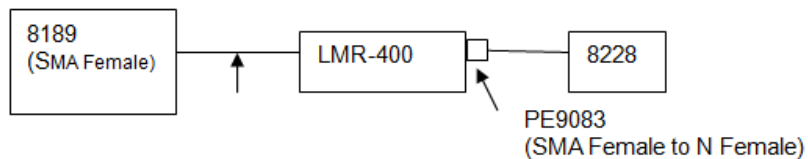
Desire to use different antenna cable with GPS products

Note: The CA11001 and A-001-001-0000 adapters have been discontinued. They are no longer available from us. The adapters can be purchased through Pasternack at toll free 866-727-8376 or www.pasternack.com.

For the Model 8189 to adapt to N Cable: Order from Pasternack their P/N PE9082 (SMA Male to N Female).

For the Model 8228 to adapt to N cable: Order from Pasternack their P/N PE9083 (SMA Female to N Female).

8189 to RG-213 or LMR-400 (outdoor cable) to 8228 (indoor antenna)



*8183 or 918x to 8228 (indoor antenna)

Order the following additional components:

A001-0001-0000 (N to SMA connector) to connect 8183/918x to SMA cable of the indoor antenna

Or order both the A001-0001-0000 and 067022 N to N barrel connector if replacing the LMR-195 cable with LMR-400 and will be putting the 8228 at the end of the LMR-400 cable.

***8183 or 918x to 8228 (indoor antenna) But using LMR-400 cable to extend distance to greater than 50 feet.**

Note: If increasing distance over 50 feet-Due to increased cable loss and attenuation through a window, we recommend running the entire distance with LMR-400 to antenna and placing the adapter onto the antenna (Don't use the 50 ft cable). Follow the normal distance limitations of LMR-400 with this scenario. Order A001-0001-0000 and a 067022 to connect the antenna side of the LMR-400 cable to the SMA connector on the Model 8228.

No adapter is required between the Model 8183/918x and the antenna cable (cable goes right onto the unit).

8225 outdoor antenna to SMA/SMA cable to 8189.

8225 antenna to CA11001 (With barrel connector removed) to SMA/SMA cable to 8189.

Order: CA11001 (comes with Barrel connector but they can remove).

Need to run Greater than 50 feet with cable thinner than RG-213/LMR-400

Recommend using LMR-195 with a preamp. Place preamp at the 75 foot area from the antenna and then run the rest of the distance to the unit.

Black box-ordering: 877-877-2269

Black Box tech support: 724-746-5500

CW04-FLFL-xxxx RS-485 twisted-pair cable

- Refer to (in Salesforce)
https://na8.salesforce.com/_ui/search/ui/UnifiedSearchResults?searchType=2&sen=a0A&sen=01t&sen=005&sen=00Q&sen=001&sen=00T&sen=810&sen=500&sen=003&sen=00U&sen=02i&sen=00O&sen=a04&sen=ka&sen=00a&sen=0F9&str=cw04*#!/fen=01t&initialViewMode=detail&str=cw04*
- Refer to (in Arena) <https://app.bom.com/items/list-main>
- P/N: CW04-FLFL-xxxx (where xxxx is the length of cable) (such as CW04-0100 for example)
- Also referred to as “RS-485 Station cable”
- Twisted-pair cable, with a white and blue wire.
- This cable is a shielded cable (so it can be run up to 4000 ft.)
- Standard length cables are (in feet) 10, 25, 50, 200, 400 and 500 ft.

General info on Fiber cable/SFP Modules

A) Fiber cable info

B) SFP module info

- Refer also to info in: <I:\Customer Service\1- Cust Assist documents\SecureSync Option Card information.pdf>

SFP module color scheme



C) BX10 SFPs with Monitoring interface

- Cut-in to our system to sell: Refer to **ECO-003070** (in Arena at: https://app.bom.com/changes/detail-summary?change_id=2414570401&orb_msg_single_search_p=1)
- In our system to be able to resell (also search Salesforce for our P/N)

Our P/Ns:

- **MP40R-0009-0001** BX10 ONU Fiber Optic SFP Module, Monitoring Interface

- In Arena at https://app.bom.com/items/detail-spec?item_id=1317574012&version_id=12362188398&orb_msg_single_search_p=1

SFP Module for 1000BASE-BX10 fiber optic interface (LC Simplex for 9/125 um cable) with 1Gb networks. ONU transceiver (1310nm Tx, 1490nm Rx)

Pair with SFP-FIBER-BX10-OLT Primarily used with White Rabbit products, supports typical 10 km point to point link. Corresponds to Axcen AXGD-1254-0531

- **MP40R-0010-0001** BX10 OLT Fiber Optic SFP Module, Monitoring Interface

- In Arena at https://app.bom.com/items/detail-spec?item_id=1317574029&version_id=12362188648&orb_msg_single_search_p=1

SFP Module for 1000BASE-BX10 fiber optic interface (LC Simplex for 9/125 um cable) with 1Gb networks. OLT transceiver (1490nm Tx, 1310nm Rx)

Pair with SFP-FIBER-BX10-ONU Primarily used with White Rabbit products. Supports typically 10 km point to point link. Corresponds to Axcen AXGD-3454-0531

- **MP40R-0011-0001** C21 DWDM SFP Module, Monitoring Interface

- In Arena at https://app.bom.com/items/detail-spec?item_id=1317574040&version_id=12362189078&orb_msg_single_search_p=1

SFP Module for 1000BASE-DWDM fiber optic interface with 1Gb networks. LC Duplex, 1560.61 nm, Monitoring interface

To be selected for long distance (up to 100 km on 9/125 um Single Mode Fiber) point to point WR link. Requires calibration: a calibration service shall be offered along with this item.

- **MP40R-0012-0001** C22 DWDM SFP Module, Monitoring Interface

- In Arena at https://app.bom.com/items/detail-spec?item_id=1317574152&version_id=12362190478&orb_msg_single_search_p=1

SFP Module for 1000BASE-DWDM fiber optic interface with 1Gb networks. LC Duplex, 1559.79 nm, Monitoring interface

To be selected for long distance (up to 100 km on 9/125 um Single Mode Fiber) point to point WR link. Requires calibration : a calibration service shall be offered along with this item.

D) eLoran/eLoran antenna

eLoran h-Field Antenna (includes 10 meter cable)

- Refer to (in Arena) https://app.bom.com/items/detail-spec?item_id=1215163767&version_id=10416552018&

Mount for ELoran Antenna

P/N MP10R-0000-0005

ELORAN

eLoran basics

- eLoran System requirements – Maritime, Aviation, Land-mobile, Timing
- eLoran System Overview – Core eLoran service provider – Application service provider
- eLoran Signal in Space – Loran pulse shape – Timing control – Loran Data Channel (LDC)
- eLoran vs. Loran-C
- Maritime Harbor Entrance and Approach

Enhanced Loran is an internationally-standardized positioning, navigation, and timing (PNT) service for use by many modes of transport and in other applications. It is the latest in the longstanding and proven series of low-frequency, Long-Range Navigation (LORAN) systems, one that takes full advantage of 21st century technology. • eLoran meets the accuracy, availability, integrity, and continuity performance requirements for aviation non-precision instrument approaches, maritime harbor entrance and approach maneuvers, land-mobile vehicle navigation, and location-based services, and is a precise source of time and frequency for applications such as telecommunications. • eLoran is an independent, dissimilar, complement to Global Navigation Satellite Systems (GNSS). It allows GNSS users to retain the safety, security, and economic benefits of GNSS, even when their satellite services are disrupted. From

ELORAN

eLoran technology is built upon the foundation of Loran-C

- eLoran has been developed over the past decade as a response to the recognized vulnerability of GNSS, by international government agencies, industry and academia
- eLoran transmitter and receiving equipment makes full use of 21st century technology
- eLoran is recognized and recommended by the International Association of Lighthouse Authorities (IALA)
- eLoran receiver Minimum Performance Standards are being developed by the Radio Technical Commission of Maritime services (RTCM) Special Committee 127

Satelles STL (iridium) antenna

*Available outdoor/rooftop STL antenna (E050-0006-0001)



- Refer to ECO-002645 (Oct 2020) in Arena at https://app.bom.com/items/detail-sourcing?item_id=1290400154&version_id=11795833158
- **Our P/N:** E050-0006-0001
 - In Salesforce: <https://orolia.lightning.force.com/lightning/r/Product2/01t0h000005oo9EAAQ/view>
- **MFG/Model:** Tallysman Model TW3600 P/N 33-3600-14-01 (Datasheet: <https://www.digikey.com/en/products/detail/tallysman-wireless-inc/33-3600-01-11/4862790>)
- STL signal only
- Type N female connector

*Active STL antenna (E050-0004-0001)

- **Refer to** “E050-0004-0001” in the SecureSync assist doc for more info: <..\SecureSync-VersaSyncCustAssist.pdf>
- Our P/N for Active Antenna: E050-0004-0001
- Attached 96 inch (8ft) RG-174 cable

*Passive STL antenna (E050-0001-0001)

- **Our P/N:** E050-0001-0001 in Arena: https://app.bom.com/items/detail-spec?item_id=1230586692&version_id=10696861268
- Includes 96 inch (8ft) cable
- **Refer to** “E050-0001-0001” in the SecureSync assist doc for more info: <..\SecureSync-VersaSyncCustAssist.pdf>

GNSS Satellite constellations (GPS/Glonass/Galileo/Beidou/QZSS/NavIC)



GNSS Status

Constellations	Nominal number of satellites and type of orbits	Operational satellites	Number of signals	Number of frequencies
GPS	24	31	8	3
GLONASS	24	24	5	3
BeiDou	27-MEO, 3-IGSO, 5-GEO	3-MEO, 6-IGSO, 6-GEO	6	4
Galileo	30	17	6	4
QZSS	3-IGSO, 1-GEO	3-IGSO, 1-GEO	5	4
IRNSS/NavIC	4-IGSO, 3-GEO	4-IGSO, 3-GEO	2	1

Mid-2020s

GPS

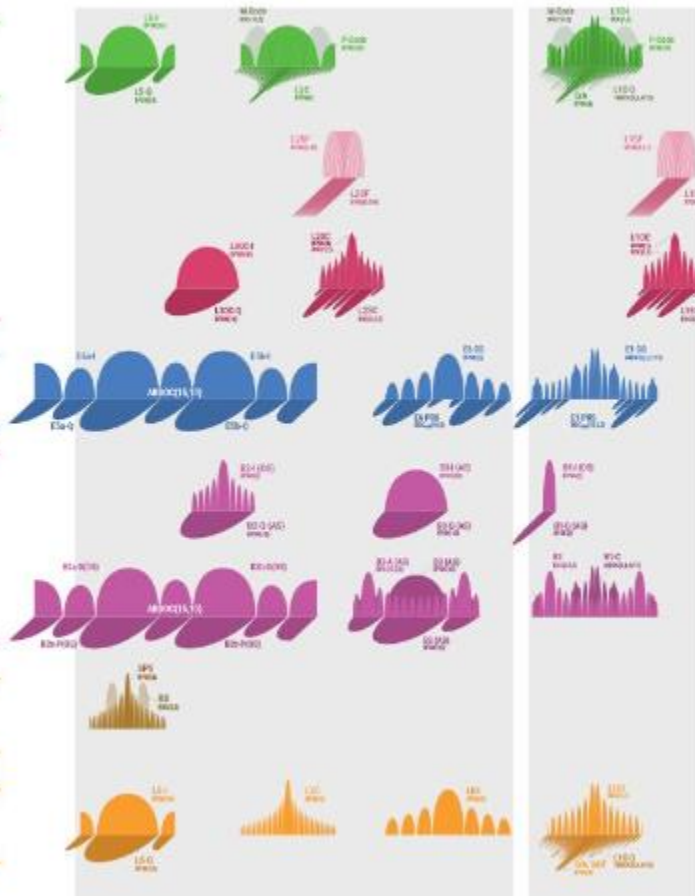
GLONASS

Galileo

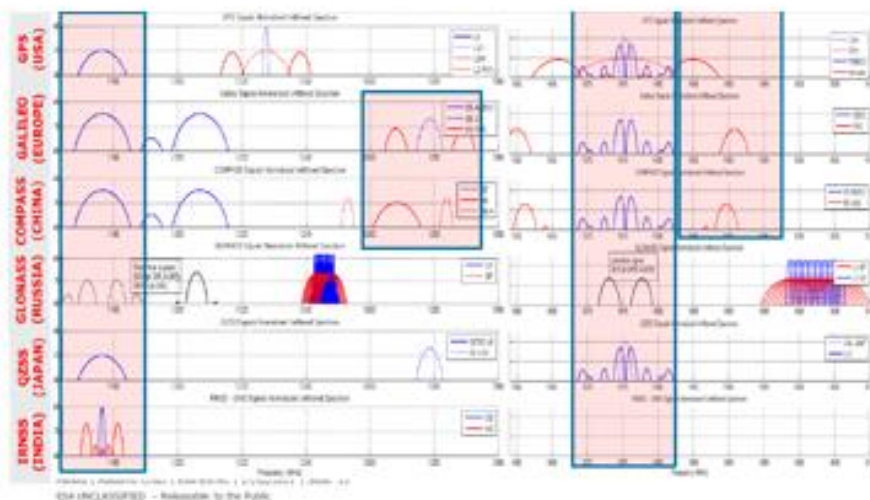
BeiDou

NavIC

QZSS



GNSS SIGNALS



GNSS (GPS, Glonass, etc) INFO, GPS ANTENNAS AND GPS RECEIVER INFORMATION

GNSS Constellation Status info

- good site for GPS + Glonass + Beidou status info: <https://www.glonass-iac.ru/>

A) GPS Constellation status info

GPS: USCG NAVIGATION CENTER: NANUs/ GPS SERVICE INTERRUPTIONS-OUTAGES / GPS TESTING NOTICES/ REPORT STATUS

- The main page for USCG Navigation Center GPS Technical info: <https://navcen.uscg.gov/?pageName=gpsTechnicalReferences>
 - GPS Problem Reports Status: <https://www.navcen.uscg.gov/?Do=GPSReportStatus>
 - GPS TESTING NOTIFICATIONS (which may affect GPS): https://www.navcen.uscg.gov/pdf/gps/gpsnotices/GPS_Interference.pdf
 - NANUs: (scheduled/unscheduled outages): <https://www.navcen.uscg.gov/?Do=constellationStatus>

B) European Galileo Constellation status info/NAGUs

- <https://www.gsc-europa.eu/system-status/Constellation-Information>

C) Russian GLONASS Constellation status info

Main page for Glonass status: <https://glonass-iac.ru/en/GLONASS>

- *Glonass Status info*: <https://glonass-iac.ru/en/CUSGLONASS/index.php>
- Status/monitoring of Glonass satellites: <https://glonass-iac.ru/en/GLONASS/>

*GPS INFO

GLOBAL POSITIONING SYSTEM (GPS)

- Operated by the U.S. Department of Defense
Minimum 24 satellites in orbit: MEO = 20,000 Km high
31 satellites operating today
- Consists of three segments
 1. Space Segment- SV SVN
 2. Control Segment- stations worldwide
 3. User Segment - receivers
- Triangulation for position
Requires 3 satellites to obtain a 2-D fix (lat and long)
Requires 4 satellites to obtain a 3-D fix (lat, long, and altitude)
- Timing
Uses the received signal to calculate its own inaccuracy and adjust
- US Naval Observatory monitors the SV clocks and sends corrections to the USAF
- The USAF uploads corrections via Schriever AFB
- **GPS can therefore be traceable to UTC(USNO)**

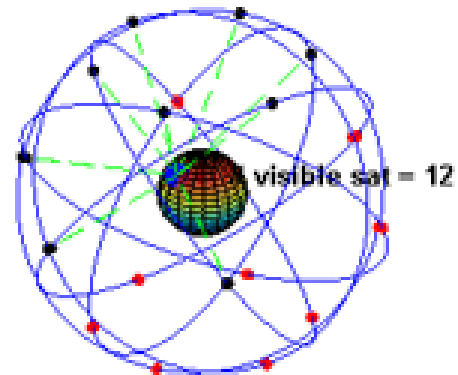


PNT Principles | 6/6/2010 46 orolli

GPS Signal Structure

SIGNAL STRUCTURE

- Dual Frequency: L1 (1575 MHz) and L2 (1227 MHz)
- CDMA: each satellite has its own PRN (pseudo-random noise) code 1024 chips long
C/A - Coarse/Acquisition code - 1M chip/sec
P - Precision code - 10 M chip/sec
- Modulated Data - 50 bps
- Almanac
- Contains orbit and status for EVERY satellite
 - Each satellite transmits the entire almanac
 - Ionospheric model
 - Leap second information
 - 1/25 of the Almanac is transmitted in nav message
 - Takes 25 complete navigation messages to receive entire almanac
 - 12.5 minutes
 - Considered valid for 180 days
- Ephemeris
- Orbital information for each satellite
 - Each satellite only transmits its own data
 - Considered valid for about 4 hours



PNT Principles | 6/6/2010

48 orolli

WAAS/EGNOS/GAGAN/MSAS (Systems that Aid GPS)

SYSTEMS THAT AID GPS

Satellite Based Augmentation System (SBAS)

- Additional satellites in orbit to transmit correction messages
 - Geostationary orbit
 - Receive corrections from ground stations
 - Re-transmits to GPS users
 - Improve reliability and accuracy
- Current SBAS systems
 - EGNOS - Europe
 - WAAS - North America
 - MSAS - Japan
 - GAGAN - India

Assisted GPS (A-GPS)

- Consists of a server in conjunction with the receiver
- Eliminates need of decoding navigation message from satellite = easier signal acq
- Used extensively in mobile phones

Differential GPS (DGPS)

- Uses 2 receivers - one reference at a known position
- Cancels common mode errors



PNT Principles | 4/6/2010

49 orolla

- **EGNOS:** European Geostationary Navigation Overlay Service
- **WAAS:** Wide Area Augmentation System developed by the FAA to aid in air navigation and augment GPS.
- **MSAS:** Multi-functional Satellite System
- **GAGAN** GPS-Aided Geo Augmented Navigation
- Commercial systems include StarFire, and OmniStar

Controlling agencies/controlling documents for GPS (ICD-GPS-200, IS-GPS-200)

- GPS is controlled by the GPS Wing of the US Air Force
- Controlling document / Specs: ICD-GPS-200, IS-GPS-200
- Refer to: [:\Engineering\Specs and Standards\GPS](#)
 - **ICDs (Interface Control Document)** are the formal means of establishing defining and controlling interfaces and documenting detailed interface designs.
 - **IS (Interface Specifications)** are specific types of ICDs.

ICD-GPS-200: Defines the requirements related to the interface between the Space Segment (SS) of the Global Positioning System (GPS) and the Navigation User Segment (US) of the GPS. It describes the GPS signals, atmospheric models, etc

- Refer to: <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB8QFjAAahUKEwj4nZC-m5TGAhXCO6wKHY2KAL0&url=http%3A%2F%2Fwww.gps.gov%2Ftechnical%2Ficwg%2FICD-GPS-200C.pdf&ei=hxaAVbi-GsL3sAWNiYLoCw&usq=AFQjCNFhIkBe4HUdT-1dBYYSZZXn9AMxg&bvm=bv.96041959,d.b2w>
- **IS-GPS-200:** Defines the requirements related to the interface between GPS space and user segments of both L1 and L2 (such as leap second, UTC offsets, GPS week number, signal data, atmospheric models. etc)
- Refer to: <http://www.gps.gov/technical/icwg/>

GPS time traceability to UTC

Thanks for your email and question about the GPS satellites (which are owned and controlled by the GPS Wing of the US Air Force). To answer your question, the GPS constellation's controlling document is IS-GPS-200. From this document:

GPS Time and SV Z-Count.

GPS time is established by the Control Segment and is referenced to Coordinated Universal Time (UTC) as maintained by **the U.S. Naval Observatory (UTC (USNO))** zero time-point defined as midnight on the night of January 5, 1980/morning of January 6, 1980. The largest unit used in stating GPS time is one week defined as 604,800 seconds. GPS time may differ from UTC because GPS time shall be a continuous time scale, while UTC is corrected periodically with an integer number of leap seconds. There also is an inherent but bounded drift rate between the UTC and GPS time scales. The OCS shall control the GPS time scale to be within one microsecond of UTC (modulo one second).

The NAV data contains the requisite data for relating GPS time to UTC. The accuracy of this data during the transmission interval shall be such that it relates GPS time (maintained by the MCS of the CS) to UTC (USNO) within 90 nanoseconds (one sigma). This data is generated by the CS; therefore, the accuracy of this relationship may degrade if for some reason the CS is unable to upload data to a SV. At this point, it is assumed that alternate sources of UTC are no longer available, and the relative accuracy of the GPS/UTC relationship will be sufficient for users. Range error components (e.g. SV clock and position) contribute to the GPS time transfer error, and under normal operating circumstances (two frequency time transfers from SV(s) whose navigation message indicates a URA of eight meters or less), this corresponds to a 97 nanosecond (one sigma) apparent uncertainty at the SV. Propagation delay errors and receiver equipment biases unique to the user add to this time transfer uncertainty.

As eluded to above, GPS time scale that the satellites transmit is not the same time as UTC timescale, as UTC time has periodic leap seconds asserted (GPS does not assert leap seconds). But GPS knows how many leap seconds have been asserted since GPS went online and transmits this number to the GPS receivers. This number of leap seconds allows the SecureSync to calculate UTC from the GPS time by accounting for the leap seconds.

ICD-GPS-153/ ICD-GPS-153c (documentation for the DAGR receiver)

- Refer to the "ICD-GPS-153" section of the SecureSyncCustAssist document: <..\SecureSync-VersaSyncCustAssist.pdf>

GPS satellite Navigation Message format and protocol details:

- A good tutorial with details about the GPS signal (by Ed Weston): <http://gpsinformation.net/gpssignal.htm>

GPS leap second insertion

- Apparently, GPS will announce leap seconds **no less than 30 days** prior and **no sooner than 6 months** prior. However, I couldn't find any spec/notes on this, including in the ICD control documentations

****LEAP SMEAR (SMEARING THE LEAP SECOND INSTEAD OF JUMPING ONE SECOND)**

Email from Denis Reilly (1 Dec 16) We have a whole section on leap smearing in the NTP BCP, and why it is bad for public servers. Here is our guidance:

Leap Smearing must not be used for public-facing NTP servers, as they will disagree with non-smearing servers (as well as UTC) during the leap smear interval. However, be aware that some public-facing servers might be configured this way anyway in spite of this guidance.

System Administrators are advised to be aware of impending leap seconds and how the servers (inside and outside their organization) they are using deal with them. Individual clients must not be configured to use a mixture of smeared and non-smeared servers. If a client uses "smeared servers", the servers it uses must all have the same leap smear configuration.

The NTP guys insisted on the "Must" in that first sentence. I added the second sentence, because I suspected Google would keep doing this in spite of a stern finger-wagging from the IETF. I am glad to see that Google added the caution to mix smeared and non-smeared time servers in their blog post, though.

Keith: I'm not sure if any of our customers are using Google's NTP servers, but please be aware that if customers are mixing smeared servers and non-smeared servers at the same time, Bad Things can happen. And if they are using Smearing servers like Google's, they will be off from UTC for 20 hours....

Solar flares and effects on GPS

- Nice website for showing activity that occurred on a specified date: http://www.thesis.lebedev.ru/en/sun_flares.html?m=7&d=7&y=2013

Using a smart phone/cell phone to test for GPS/GNSS reception

- androids are MUCH better for this function than iPhones are
 - iPhones have limited API calls to the receiver, so they can only obtain position data (not raw satellite data)

Q Which app do you recommend on iOS and Android to track satellites?

A Reply from Keith (5 Oct 2018) Thanks for your great question about recommended phone apps to check for localize GPS reception...

Starting with iPhones: These are definitely not ideal cell phones to use for this function. Unlike with Androids, the communications between the iPhone and its GPS receiver is very limited, to primarily obtaining just location data (such as latitude and longitude positional data only).

Another problem with iPhones is they use GPS combined with other signals to help find locations even faster than if it was only using GPS reception.

However, I figured out one very rudimentary “work-around” that seems to indicate if the phone is receiving a GPS signal, using Google map’s “saved parking” function. After turning on Airplane mode (to turn off wi-fi and other non-GPS signals), go to the location of the GPS antenna.

Open “Google Maps” and click the blue dot indicating your position. This should open a selection on the bottom allowing you to “share your location” with “set as parking location” listed below that. Click “set as parking location” to mark this location. Then start walking away from this location.

If there is no GPS reception available, the blue dot and the Parking indicator will stay right next to each other, as you continue walking away from the starting position. But if there is GPS reception available, the blue dot indicating where you are should continue to move away from the marked parking position. Try this test first indoors, away from windows. Then repeat the same test near the location of the antenna. If you see the same effect happening, there is likely a source of nearby local interference to the GPS signal.

Don’t forget to turn back off Airplane mode after performing this test 😊!

If you, or someone else has an Android phone, this is a MUCH better phone to use. There are many apps available for reporting the satellite data of its GPS receiver. A very good example app to use is “GPS test” (a free download, or a “Plus” version for purchase): <http://appcrawlr.com/android/gps-test>

Below are some example screenshots from the GPS Test app:



Please let me know if you are able to use one of these apps (especially the one for Android) and how the test goes!

Security considerations/PCI audits

A) SecureSyncs

- Refer to “PCI-DSS / PCI compliance/PCI Audits (Payment Card Industry) Security Assessments/audits”:[..\SecureSync CustAssist.pdf](#)

B) NetClock Models 9300/9200

- Refer to: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\9283-9288-9289-9383-9389-9388\network and GPS security](#)

GPS/Glonass Signals, Frequencies/Bands

**GPS Signal Modernization

GPS SIGNAL MODERNIZATION

M-CODE – NEXT GEN SAASM

- MUE Military User Equipment

L2C – PRECISE CIVILIAN CODE

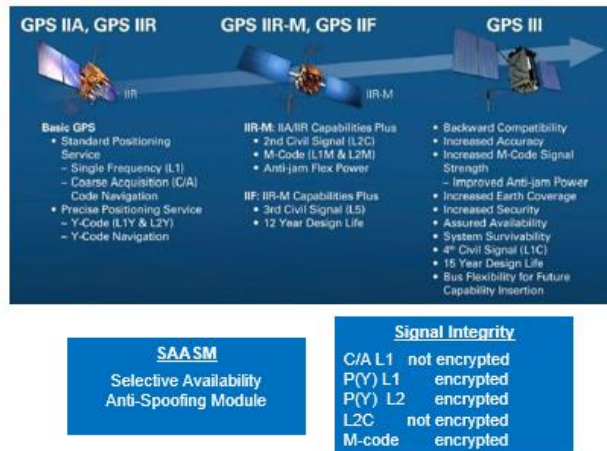
- No military encryption
- Modern modulation
- Obviates need for “semi-codeless” techniques

L5 – NEW CIVILIAN – SAFETY OF LIFE

- Compatible with Galileo E5;
- More powerful; less interference (protected band)
- More frequency separation

L1C – SAME CAPABILITY AS L1

- Compatible with Galileo
- First satellite not yet launched (GPS Block III)
- Full by 2026



PNT Principles | 6/6/2018

88 orolida

GPS

- **Commercial: L1 band** (1575.42 ±15) MHz (1560.42 - 1590.42 MHz)
- **SAASM: L2 band** (1227.60 ±15) MHz (1212.60 – 1242.60 MHz)
- **M-Code**
- **L1C** same capability of L1
- **L2C** (precise Civilian Code)
- **L5** (new Civilian- Safety of Life)

Glonass

- Glonass uses Frequency Division Multiple Access (FDMA)
 - **L1 band:** 1602 MHz
 - **L2 band:** 1246 MHz

Galileo

GPS week numbers (date/time info GPS transmits)

Date/Time GPS satellites transmit

From: https://en.wikipedia.org/wiki/Global_Positioning_System#Message_format

As opposed to the year, month, and day format of the [Gregorian calendar](#), the GPS date is expressed as a week number and a seconds-into-week number. The week number is transmitted as a ten-bit field in the C/A and P(Y) navigation messages, and so it becomes zero again every 1,024 weeks (19.6 years). GPS week zero started at 00:00:00 UTC

(00:00:19 TAI) on January 6, 1980, and the week number became zero again for the first time at 23:59:47 UTC on August 21, 1999 (00:00:19 TAI on August 22, 1999). To determine the current Gregorian date, a GPS receiver must be provided with the approximate date (to within 3,584 days) to correctly translate the GPS date signal. To address this concern the modernized GPS navigation message uses a 13-bit field that only repeats every 8,192 weeks (157 years), thus lasting until the year 2137 (157 years after GPS week zero).

GPS Week Numbers

- Link to a calendar showing GPS week numbers: <http://adn.agi.com/GNSSWeb/>

April 2019: 20 year GPS Week roll-over issue due to number of bits in the message (2019, 2036, etc..)

- GPS epoch condition occurring every 20 years (2019, 2036, etc)
- General info about GPS week rollover/how to test for it: refer to (on our website): <https://spectracom.com/resources/blog/lisa-perdue/2018/gps-2019-week-rollover-what-you-need-know>
- For more info, refer to sites such as: <http://www.colorado.edu/geography/gcraft/notes/gps/gpseow.htm>

Thank you for the case. The links below should help with your questions about the 2019 Week Rollover:

<https://spectracom.com/resources/blog/lisa-perdue/2018/gps-2019-week-rollover-what-you-need-know>

<https://spectracom.com/gps-week-rollover>

https://spectracom.com/sites/default/files/document-files/GPS%20Week%20Number%20Rollover%20Issues_v4_2_Short_0.pdf

Refer to: <I:\Customer Service\GPS\GPS week rollover-2019>

Note: the next 1024 week rollover occurs on **7 April, 2019**

Q I have been made aware of an issue with another manufacturer of GPS Clocks and although not one we use it prompts me to ask the same question to all our clock suppliers.

Apparently, there are several scenarios when a GPS clock can roll over due to “a limited number of bits in the satellite message”. A roll over in a Gorky unit is believed to have failed in the past and there will be a major roll over in 2019.

Could you confirm that a limited number of bits in the satellite message will not cause the Spectracom 9383 units we have in service to fail in any way?

A. Email from Paul Myers (22 Jul 16) “This is an end of epoch issue a 20 year period of GPS weeks which rolls over in a counter which can’t go beyond the number 1024.”

Testing/certification of our GPS receivers

A) SecureSynchs, NetClock 9400s and TSynch boards

YEAR 2036

uBlox

- Based on firmware version. Refer to: <https://www.u-blox.com/en/docs/UBX-19039990>

In a continuous effort to offer excellent technical support to the customers, u-blox has evaluated all u-blox 5, 6, 7, 8 and M8 receivers and listed the GPS week number roll-over compensation value for each u-blox GNSS receiver firmware version as shown in **Table 1**.

Generation	Firmware	Week number	Start date	End date
u-blox 5	5.x	1460	2007-12-30	2027-08-14
	6.x	1528	2009-04-19	2028-12-02
u-blox 6	6.x	1528	2009-04-19	2028-12-02
	7.x	1603	2010-09-26	2030-05-11
	1.x	1691	2012-06-03	2032-01-17
u-blox 7	7.x	1603	2010-09-26	2030-05-11
	1.x	1691	2012-06-03	2032-01-17
u-blox 8/M8	2.0x	1756	2013-09-01	2033-04-16
	3.0x	1867	2015-10-18	2035-06-02
	3.5x	1936	2017-02-12	2036-09-27

Table 1: Default GPS week number roll-over compensation values of u-blox GNSS receivers

Trimble Res-T and RES-SMT-GG

~~~~~ YEAR 2016

Email Dave L sent to a customer (2 Dec 16) I have confirmed that none of the receivers used in the SecureSync product are affected by the year 2019 GPS week rollover issue.

Earlier email (don't recall from whom or when): Our Engineering department had done a quick test with a Rollover scenario and our SecureSync continued to function normally and without any problems.

As such, we are able to inform you with a high level of confidence that our SecureSync shall NOT be affected by the Rollover problem.

However, as informed earlier – we shall still be doing a more elaborate series of tests the first week of March 2015 after which we shall send you our test reports for onward submission to OKI for their records.

We hope the above confirmation is to your satisfaction.

Resolution-T GPS receivers (9183, 9283, 9383, earlier 9400s and earlier SecureSyncs)

Q. From Dick Fox to Dave Sohn: Do you know what is meant by GPS week counter roll over problem? Is this a known issue with other GPS receiver? Does the Res-T receiver have this issue?

A From Dave Sohn (2/21/13 KW) The GPS week rollover issue would be caused as the GPS week counter rolls over back to zero, indicating another GPS epoch. Some receivers may have issues responding to this, causing errant behavior on the year, day of year reported. The receiver we utilize in SecureSync does not have a GPS week rollover issue

Note about Dave's response above: Dave asked Lisa Perdue to test a Res-T GPS receiver for the week roll over issue, using a GSG Simulator. The testing worked just fine. She did not experience any roll over issues.

B) Acutime antennas

C) Legacy VelaSyncs (ublox receiver)

D) Legacy TSAT timing boards (Acutime antennas)

E) NetClock 9300s/9200s/9100s

Resolution-T GPS receivers (9183, 9283, 9383, earlier 9400s and earlier SecureSyncs)

2016

Q. From Dick Fox to Dave Sohn: Do you know what is meant by GPS week counter roll over problem? Is this a known issue with other GPS receiver? Does the Res-T receiver have this issue?

A From Dave Sohn (2/21/13 KW) The GPS week rollover issue would be caused as the GPS week counter rolls over back to zero, indicating another GPS epoch. Some receivers may have issues responding to this, causing errant behavior on the year, day of year reported. The receiver we utilize in SecureSync does not have a GPS week rollover issue

Note about Dave's response above: Dave asked Lisa Perdue to test a Res-T GPS receiver for the week roll over issue, using a GSG Simulator. The testing worked just fine. She did not experience any roll over issues.

F) FAA Model 8183A TOY Clocks/NetClock Model 8183

- all had a **Motorola Oncore GT or GT Plus** receiver installed (I believe)
- Refer to salesforce Cases such as **172829** (Aug 2018)
 - FAA tested 2019/2038 rollovers using GSG and reportedly found 2019 OK, but 2038 not OK???

G) Ageless oscillators Model 8195/8295 series

Q from Dave L I was wondering if we ever did test the 8195 series products for the April 2019 Rollover? I have customers asking about this now.

A Reply from Dave Sohn (7 Feb 2019) We did and did not find issues around the week rollover

GPS/UTC 1PPS timing error with several satellites (26 Jan 2016)

- **Details:** refer to the Tech Note Lisa Perdue authored ("Jan26-GPS-Timing-Event"): [I:\Customer Service\GPS\GPS timing glitch Jan 2016](#) (**Note: this document is for internal use only. Do not distribute**)
- Refer to sites such as the following"
 - <http://www.insidegnss.com/node/4831>
 - <http://www.insidegnss.com/node/4829>
 - <http://it.slashdot.org/story/16/01/26/1735223/discrepancy-detected-in-gps-time>
- On 26 Jan, 13.7 microsecond timing error to UTC 1PPS versus GPS 1PPS occurred (The GPS 1PPS and UTC 1PPS are supposed to always be less than 1 microsecond apart)
- Affected SecureSyncs with version 5.0.0 and above (4.8.9 and below uses GPS 1PPS while 5.0.0 and above now use UTC 1PPS – as it's a common 1PPS for multiple constellations)
- Problem remained in four affected satellites for 3.5 days (until almanac data was replaced with new data)
- Resulted in Frequency Error alarm being asserted on Tuesday, 26 Jan (which then cleared about 30 minutes or so thereafter). Our logs show first Frequency Error alarm was asserted at 03:31 UTC. We also saw another

****Change made to GPS signal January 11, 2010**

- Refer to NC3903.
- Right after the last ground station had a software update applied, the Trimble receivers and Acutime antennas started experiencing momentary loss of satellites every 12.5 minutes. The GPS Wing added a sequence of zeroes to a sub-frame which started causing the Trimble receivers to think the signal was being jammed. This caused the receiver to momentarily stop and then restart tracking satellites.
- Noticed on the GPS-based Models 9300, 9200 (Including SAASM receivers when keyed- unkeyed SAASM receivers were OK) TSYNC and KSI timing boards.
- Trimble incorporated a software change to the commercial receivers that we started receiving here on or about 2/5/10. The new receivers are not dropping to 0 satellites. The P/N of the receiver did not change because of the software version. Receivers can be updated outside of the unit if desired, but this is not a requirement for repairs.

GPSD (GPS service daemon)

- Refer to the online VersaSync user guide http://manuals.spectracom.com/VSS/Content/_Global/Topics/_GLOBAL/GPSD_Setup.htm
- As of at least Oct 2018: currently only supported in VersaSyncs/VersaPNTs (firmware versions 1.3.1 and above)
- Now also supported in Model 2400 SecureSyncs (not installed in 1200 SecureSyncs)

Description GPSD is a free, open-source package used worldwide to manage GNSS systems and devices. With GPSD support on a VersaSync, users can:

- connect to the unit over a network via TCP at the specified port using any GPSD-compatible software
- receive position and timing information from the GNSS receiver in a consistent format, and
- use the WebUI (or CLI) to configure the GPSD service and view status information.

Great info about GPSD: refer to <https://gpsd.gitlab.io/gpsd/#others>

“gpsd is a service daemon that monitors one or more GPSes or AIS receivers attached to a host computer through serial or USB ports, making all data on the location/course/velocity of the sensors available to be queried on TCP port 2947 of the host computer.

GPSD is everywhere in mobile embedded systems. It underlies the map service on Android phones. It's ubiquitous in drones, robot submarines, and driverless cars. It's increasingly common in recent generations of manned aircraft, marine navigation systems, and military vehicles.

Orolia Intelligent Repeater Systems / Zone Based Indoor Location Using GNSS Simulators

(Spectracom Intelligent Repeater Systems)

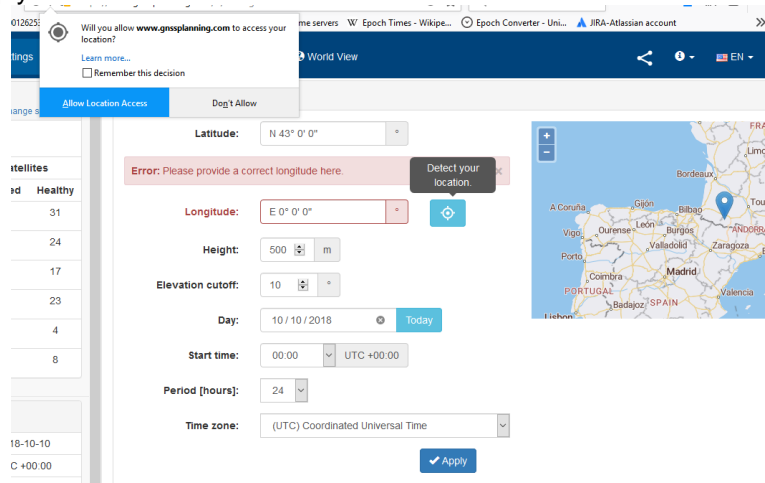
- Refer to “**Orolia Intelligent Repeater System**” in: <..\GSG Customer Service.pdf>

*“Trimble GNSS Planning tool” / GPS prediction software (freeware)

- The program can be utilized at: <https://www.gnssplanning.com/#/settings>
- We do not “support” this program

Steps

- 1) With the **Settings** tab selected on the top of the page. On the left side of the page, enter customer’s position (lat and long) as well as Date/UTC time of the event (note you can also drag the map to move to a desired location). Press Apply



- 2) To limit the view to just one or more satellite constellations (such as “GPS” satellites only), in the left side of the Settings tab, press the checkmark icon key next to all undesired constellations (to change it to an “X”)

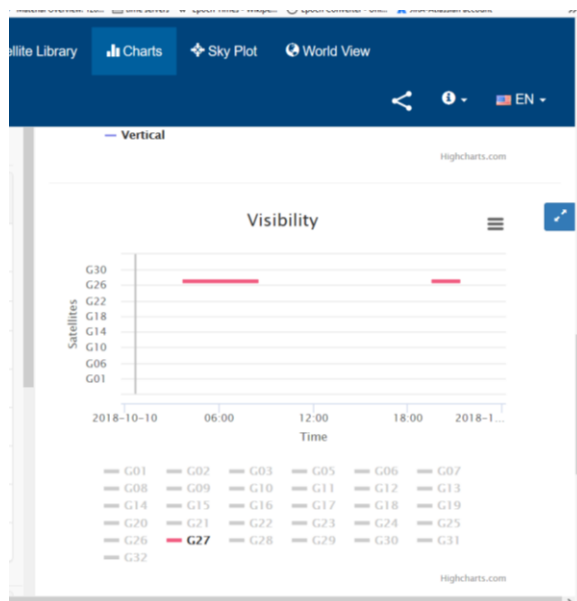
Satellite Selection			
Change selection			
Satellites: 1/110			
System: active		Satellites	
		Selected	Healthy
GPS	<input checked="" type="checkbox"/>	1	31
GLONASS	<input type="checkbox"/>	0	24
Galileo	<input type="checkbox"/>	0	17
BeiDou	<input type="checkbox"/>	0	23
QZSS	<input type="checkbox"/>	0	4
IRNSS	<input type="checkbox"/>	0	8

- 3) To limit the view to just one or more particular satellites in the enabled constellations, select the Satellite Library tab at top of the page. On the left, press the name (in blue) of the desired constellation to modify. On the top-right side, press “Invert” (to de-select all satellites in the selected constellation listed below this button). Then scroll down and select only the desired satellite(s) to view data on (such as “G27” for instance)

G01	Healthy	i
G02	Healthy	i
G03	Healthy	i
G05	Healthy	i
G06	Healthy	i
G07	Healthy	i
G13	Healthy	i
G14	Healthy	i
G15	Healthy	i
G16	Healthy	i
G17	Healthy	i
G18	Healthy	i
G24	Healthy	i
G25	Healthy	i
G26	Healthy	i
✓ G27	Healthy	i
G28	Healthy	i
G29	Healthy	i

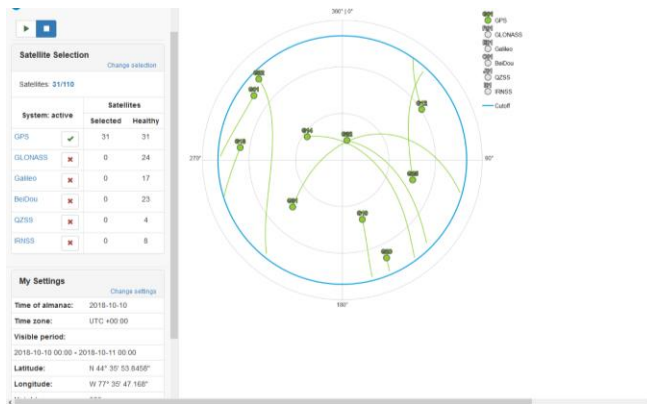
Viewing satellites which were in view

- There is an alternate/better way (besides the “**Sky Plot**” tab, described further below) to see which satellites were in view.
- After performing the other steps on the Settings tab, select the **Charts** tab. then scroll down the right side of the page to “Visibility”. This will display all GPS sats in various colors. Since some of the colors are similar, you can press each satellite ID under the chart (except G27) to de-select it from being displayed. If any lines are still present, G27 was in view at that time.



OR

Select “Sky Plot” tab at top of page



Zoom to see the various GPS satellites that were in view at the time entered in the Settings tab

Earlier, downloadable Trimble Prediction software (appears no longer available from Trimble directly??)

- This program shows items such as the number of satellites in view throughout the day, based on your geographical location (a GPS receiver is not required for use with this software).
- To run this program after its installed: Start -> All Programs -> Trimble Office -> Utilities -> Planning
- We do not support this program.

U.S. Coast Guard Navigation Center (NAVCEN): GPS Situational awareness (problem reports/outages/GPS Interference testing, etc)

- <https://navcen.uscg.gov/?Do=GPSReportStatus>

Satellite outages

- Refer to: <http://adn.agi.com/SatelliteOutageCalendar/SOFCalendar.aspx>

Scheduled GPS Interference testing

- Refer to: http://www.navcen.uscg.gov/pdf/gps/gpsnotices/GPS_Interference.pdf

the following is from:

https://orolia.my.salesforce.com/_ui/core/chatter/groups/GroupProfilePage?g=0F9C00000004KGd&fId=0D50h000055zTic&sIoid=00D80000000aMdF&sInid=0000000000000000&emkind=chatterUnifiedUserDigest&sIuid=00580000001p7IW&emtm=1536986372644&fromEmail=1&sIext=0

To provide better service and situational awareness to the public, the U.S. Coast Guard Navigation Center (NAVCEN) now publishing reports of GPS problems on its website. Any notes about problem resolution, if available, will also be listed. The website will be updated as new reports are received and processed. All reports made in 2018 are now available. Reports for prior years will be made available in the future.

Reports of GPS problems submitted to NAVCEN through the GPS Problem Reporting webpage will be posted to the GPS Problem Report Status webpage after review by NAVCEN staff. Reports will be anonymized to protect the submitter's personal information and any equipment manufacturer data. After user and interagency partner input has been collected, any findings will be added to the report along with the suspected cause and resolution, if available.

The webpage will include the following information for each report:

- **Date / Time of Disruption:** Date and time of the report as provided by the reporting source.
- **Date Submitted:** Date the report was submitted to NAVCEN.
- **Location:** The general location of the reported problem based on input from the reporting source. Latitude and longitude may be used for maritime reports.
- **Type:** Installation type as provided by the reporting source. Choices include: Agriculture, automobile, aviation, communications, first responder, marine, law enforcement, research, surveying, timing, transportation, and other (with a fillable field).
- **Description:** Description of the problem. This information from the reporting source is edited for clarity and to remove personal and equipment manufacturer identifying details. The description also provides GPS satellite constellation analysis information as provided by the GPS Operations Center, a determination if authorized GPS testing might have been a factor, and information on correlating reports from other users and interagency partners.
- **Cause:** The most likely cause of the report based on interagency input.
- **NAVCEN Closed Date:** NAVCEN collects interagency input and provides a detailed response to the reporting source for each report submitted. If there are no further questions from the reporting source, and NAVCEN has no other correlating information, NAVCEN will close the case. The results of interagency input will be included in the description field when the case is closed. This date may not correspond to the event end date.

Civil GPS users are encouraged to submit reports of GPS problems to the Coast Guard Navigation Center, civil aviation users are encouraged to report GPS anomalies to the Federal Aviation Administration, and military users should contact the GPS Operations Center.

Rick Hamilton

CGSIC Executive Secretariat

GPS Information Analysis Team Lead

U.S. Coast Guard Navigation Center

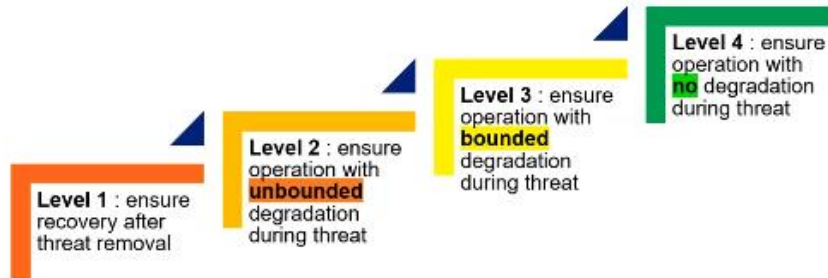
703-313-5930

GNSS Security framework (GNSS jamming/spoofing)

Dept Homeland Security Levels

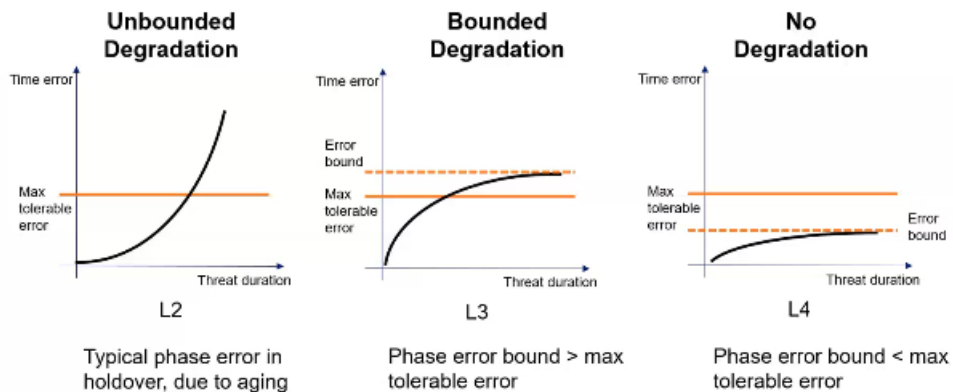
GNSS SECURITY FRAMEWORK – CRITICAL INFRASTRUCTURES

- (US) DHS conformance framework as a good, generic, approach to GNSS security
 - Conformance framework will be used as guidance for sector specific standards
 - PNT equipment manufacturers categorize their solutions based on resilience levels
 - Critical Infrastructure operators will incorporate resilience levels in their acquisition requirements



- Other frameworks are in preparation, in particular NIST PNT profile
- In Europe, several initiatives are expected (as part of the Cybersecurity act) to build a GNSS security framework

TIME ERROR PROFILES TO MEET RESILIENCE LEVELS

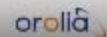


THREAT SCENARIOS

- Resilience levels actually need to refer to threats, which tend to be sector/application specific
- For critical infrastructures, we could imagine some generic threat scenarios, as below

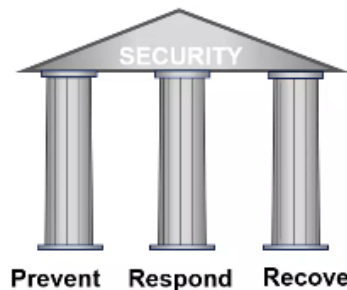
S#	Malicious / non malicious	Jamming /spoofing	Sophistication level	Event duration	Typical Scenario
S1	Non malicious	Jamming	Low	Short	In-vehicle privacy jammer, passing in vicinity
S2	Malicious	Jamming	Low	Medium	In-vehicle jammer, intentionally placed close to target
S3	Malicious	Jamming	High	Medium	Crafted / customized jamming device, high power, aiming at denying GNSS acquisition in a large area
S4	Malicious	Spoofing	Low	Medium to Long	Basic spoofing device, using SDR radio and unmodified open-source simulation SW
S5	Malicious	Spoofing	High	Medium to Long	Sophisticated spoofing device, using SDR radio and optimized/crafted simulation SW, placed close to the target

SECURESYNC 2400 TRAINING - OROLIA PROPRIETARY



THE GNSS SECURITY PILLARS – A SOLUTION APPROACH

- How can we map our offer to security requirements ?
- Prevent
 - Anti-Jam antenna
 - GPS Dome (can be combined with AJ ant.)
 - SAASM / M-Code (military only)
 - STL Option
- Respond
 - Detect
 - JADE – Jamming detection (free)
 - IDM Suite – including spoofing detection
 - Act upon threat detection – switch to
 - Internal oscillator (TCXO < OCXO < RUBIDIUM) – L2 type resilience
 - External "on site" reference (STL, eLORAN, ...) – L3 type resilience
 - Network PRC – L3 to L4 type resilience
- Recover
 - Automatic with all our solutions



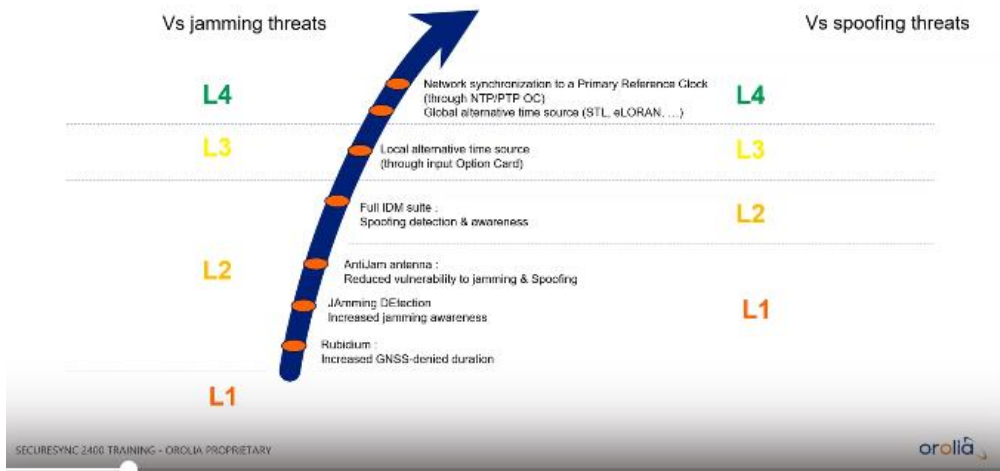
Meeting a L2 to L4 resiliency level is a system and architecture problem

JADE and IDM suite allow to address the "detection" portion required to Respond a GPS threat, enabling L2 to L4 resilience levels

SECURESYNC 2400 TRAINING - OROLIA PROPRIETARY



OROLIA SOLUTIONS MAPPING TO RESILIENCE LEVELS



KEY GNSS RESILIENCE QUALIFICATION QUESTIONS

- What are the threat scenarios you need to consider ?
 - Consider the 5 generic scenarios
- What is the duration of the GNSS threat duration for which you need to be protected ?
 - Can be associated with an "intervention notice duration", or time needed to access a site
- What is the maximum time and/or frequency error tolerated by your application ?
- What is the impact for your application if time and/or frequency error grows beyond your tolerance threshold ?

Broadshield software /Local interference/ GPS jamming (anti-jamming) and GPS spoofing (anti-spoofing)

GPS Jamming/Local interference:

Excellent Email from Dave L to a customer about jamming (16 Mar 16) One possibility for this problem is the signal is being jammed by an RF transmission in the area. If jamming is the problem, boosting the signal will not help. GPS Signal jamming is a difficult problem to resolve. Basically the antenna needs to be shielded from the jamming source or the source of interference discovered and removed.

There is specialized equipment made to help locate the source of jamming signals. Spectracom does not deal with or recommend any particular equipment to locate GPS Jamming but here is some information I found on Google:

<http://www.gps-world.biz/index.php/products/gps-jamming-detection>

http://www.chronos.co.uk/files/pdfs/cs-an/Detecting_Locating_GPS_Interference.pdf

***GPS Jammers/GPS transmitters/GPS spoofers



➤ Refer to sites such as:

- **Info about Jammers:** <https://www.foxnews.com/tech/gps-jammers-illegal-dangerous-and-very-easy-to-buy> and
- <https://www.nbcnews.com/news/us-news/gps-under-attack-crooks-rogue-workers-wage-electronic-war-n618761>
- **Article discussing the use of GPS jammers UK for car thefts** <http://www.tracker.co.uk/news/press-releases/rise-in-use-of-gps-jammers-no-threat-to-tracker/>
- **GPS jammers for sale:** https://www.chinaecarts.com/gps-jammers-c-42_44.html

general email Keith sent to a customer (11 Feb 2019) in case you are interested in more info the illegal/mobile GPS jammers/transmitters, here is an even better link than the one I provided earlier:
<https://www.foxnews.com/tech/gps-jammers-illegal-dangerous-and-very-easy-to-buy>

Note these devices are illegal in the US, but they are becoming more and more prevalent (especially in commercial vehicles). They are readily (and inexpensively) available from overseas.

info below from: <https://www.foxnews.com/tech/gps-jammers-illegal-dangerous-and-very-easy-to-buy>

Jammers transmit a low-power signal that creates signal noise and fools a GPS receiver into thinking the satellites are not available. They can be used to confuse police and avoid toll charges, and some pranksters use them to nettle unsuspecting [iPhone](#) users.

But the real threat is the unknown. Criminals could use them to hide their whereabouts from law enforcement -- and some experts fear terrorists could use high-powered jammers to disrupt GPS reception on an airplane or in military operations.

The devices pose serious societal risks, and they're unquestionably illegal to buy and use in the United States. The FCC is bullish about pursuing anyone who buys a GPS jammer and will prosecute and jail anyone who uses one. Yet they're easily bought online, and their proponents say they should stay that way. Fox News was able to buy GPS jammers for as little as \$50 from numerous online sources.

Jamming detection/Mitigation

General overview of our jamming/spoofing IDM mitigation capabilities: refer to our website at: <https://www.orolia.com/solution/interference-detection-and-mitigation/>

***Opt-BSH: BroadShield IDM software option / Opt-JADE (Jamming detection)

- Third-party software from Talen-x
- OPT-BSH (or Opt-Jade) Optionally installed in 1200/2400 SecureSyncs and VersaSyncs/VersaPNTs for detecting GNSS jamming

BROADSHIELD – JAMMING AND SPOOFING DETECTION



Detects **Jamming**

Continuous Wave (CW)

Swept CW

Pulsed CW

AWGN

BPSK

...



Calibration not required

Dynamic range based on the receiver RF front end (AGC, LNA, etc.)

Detects **Spoofing**

GNSS simulators

Anomalies in the GPS data

Jumps in position and time

And everything in between

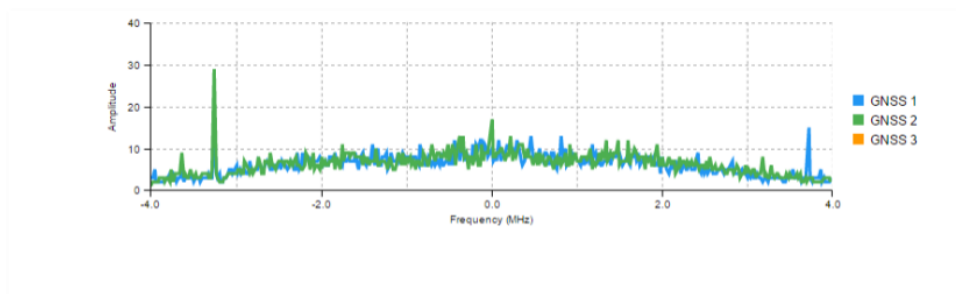
Alerts when jamming and/or spoofing is detected

SecureSync automatically implements user-defined counter measures

Allowing for continuous and reliable operation in adverse environments

JAMMING AND SPOOFING DETECTION

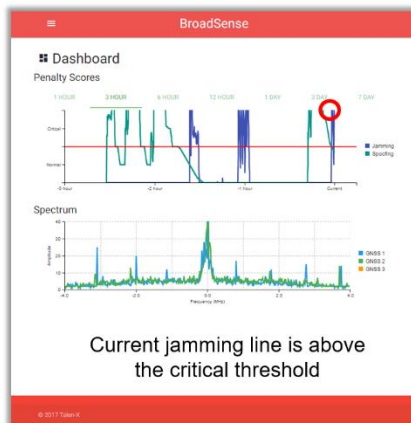
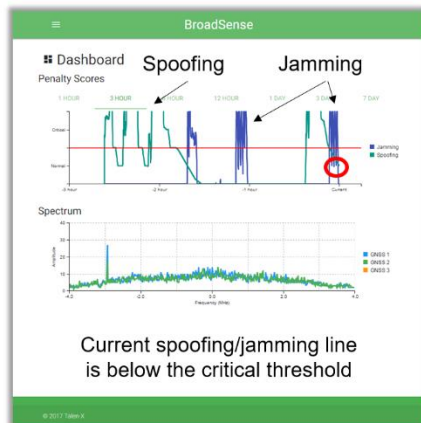
- *Detectable energy in the band*
- *Detecting movement or jumps in time or position*
- *Inconsistent / overly consistent power levels among the various satellites*
- *Examining data correctness*
- *Obtaining data messages from the GPS control segment*
- *Correlation among the reports from all the GNSS constellations*



- Refer to the BroadShield datasheet on our website: <https://www.rolia.com/product/broadshield/>
- Refer to Talen-X/Broadshield in the applicable assistance docs (especially 1200 SecureSync, as well as 2400 SecureSync or VersaSync at <I:\Customer Service\1- Cust Assist documents>) for Model-specific details on Opt-BSH/Opt-Jade.

Penalty Score

COMBINING ALL FACTORS INTO A PENALTY SCORE



***Talen-X BroadSense

BroadSense

- Refer to sites on our website:

<https://www.rolia.com/products/interference-detection-mitigation/broadsense>

https://www.rolia.com/sites/default/files/document-files/ods_broadsense_10-9-19.pdf

What is BroadSense?

BroadSense is a GPS jamming and spoofing detection sensor designed to provide real-time and historical situational awareness data. Utilizing sophisticated GNSS receivers and patented jamming and spoofing detection algorithms, BroadSense can detect when the GPS signal or GPS spectrum is compromised.

**Talen-X BroadSense Handheld (BSE-HH)

- **Talen-X P/N:** BSE-HH
- Rugged Windows 10 tablet with two internal u-blox M8 receivers running BroadShield software.
- **In Arena at:** https://app.bom.com/items/detail-spec?item_id=1254119523&version_id=11112285748
- **In Salesforce at:** <https://rolia.my.salesforce.com/01t0h000004kWhy?srPos=0&srKp=01t>
- Refer to ECO-1736 for our release of this product

***Talen-X BroadSense Micro (BSE-MICRO)

Talen-X P/N: BSE-MICRO

In Arena at: https://app.bom.com/items/detail-spec?item_id=1254119603&version_id=11112288518&

- **In Salesforce at:** <https://rolia.my.salesforce.com/01t0h000004kWh?srPos=0&srKp=01t>
- **Description:** Small form factor sensor with 2 internal GNSS receivers. Over 75 jamming and spoofing algorithms. Includes sensor, case, cables, GNSS antenna, and battery pack.
- Refer to ECO-1736 for our release of this product

***Talen-X BroadSense Nano (BSE-NANO-S)



- **Talen-x P/N:** BSE-NANO-S
- **Description:** Small size, weight, and power BroadSense with J/S display, spoofing detection, and USB interface.
- **In Salesforce at:** <https://rolia.lightning.force.com/lightning/r/Product2/01t0h000005yiuoAAA/view>

➤ **Shortcut to datasheet on our website** (excerpt below): <https://www.rolia.com/sites/default/files/document-files/BroadSense%2005-06-2020.pdf>

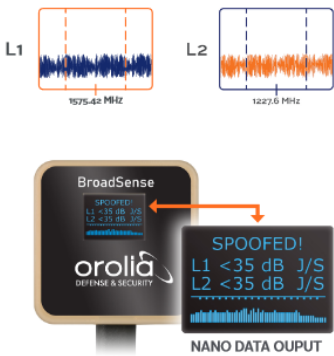
BroadSense Nano

BroadSense Nano is a low size, weight and power (SWaP) all in one jamming and spoofing detection sensor, making it extremely easy to integrate and operate. It utilizes a sophisticated multi-frequency GNSS receiver, an integrated antenna and advanced algorithms. This allows BroadSense Nano to detect GPS jamming on multiple frequency bands of the GPS spectrum and give accurate figures showing the jamming power level in the environment.

Low SWaP (Size, Weight, and Power) Specs	
Size: 41 x 41 x 19mm (LxWdH)	Weight: 46 grams
Power Consumption: 0.7 watts	Operating voltage: 5V

BroadSense Nano Key Features	
Integrated antenna	
Patented detection algorithms	
J/S measurements for L1 and L2	
Real-time visual data output (screen)	
Custom NMEA output message via USB or UART	

BroadSense Nano Recommended Applications			
UAV Platforms	Dismounted Warfighters	Cell Towers	
Situational awareness in GPS degraded or denied environments			



Added functionality with ThreatBlocker (ruggedized)

The ThreatBlocker ruggedized display shows a GPS status indicator with four green dots and the text 'GPS: OK'. Below this, it shows 'Signal Strength: 100%' and 'Signal Quality: 100%'. There are also red and yellow indicator lights on the right side of the display.

Threatblocker (sold thru OGSi)



- Refer to <https://www.orliads.com/threatblocker>
- GPS Jamming and Spoofing Data, Detection and Protection

Other suggestions to help potentially eliminate GPS jamming

Email from Dave Lorah (18 Mar 16) It's not possible to resolve a signal interference jamming problem easily. There are no controls in the SecureSync to eliminate interference.

There are two ways to resolve the problem.

1) Locate and eliminate the jamming signal.

2) Shield the antenna from the jamming signals. Since GPS is a line of sight transmission, it is possible to install a shield between the antenna and the jamming transmitter to shield the antenna from the signal. The hard part is finding out where the jamming signal is coming from. If there is a road or highway next to the building perhaps installing a shield to block the antennas view of the road may help??

Some experimentation may be needed to find the best spot to install a shield.

Local broadcast interference

Harmonics from local broadcasts may interfere with the GPS L1 carrier (1575.42 MHz). Certain television and FM radio broadcasts, while operating within their frequency allocations, can cause GPS jamming because of the harmonics of the carrier.

Table A-1 lists the potential problem television stations and their respective GPS harmonics.

TELEVISION STATIONS WITH GPS JAMMING POTENTIAL

CHANNEL	HARMONIC	Actual Frequency
66	2 nd	783.25 MHz
23	3 rd	525.25 MHz
10	8 th	193.25 MHz
7	9 th	175.25 MHz
6	18 th & 19 th	83.25 MHz
5	20 th	77.25 MHz

Note: TV 22 is close to TV 23 (3rd harmonic), so it could also affect GPS.

FM radio stations, while lower in radiated power, may cause GPS jamming also.

Table A-2 below lists the potential problem radio frequencies and their respective GPS harmonics.

FM RADIO FREQUENCIES WITH GPS JAMMING POTENTIAL

FREQUENCY	HARMONIC
104.8 - 105.2	15 th
98.3 - 98.7	16 th
92.5 - 92.9	17 th
87.3 - 87.7	18 th

****GPS filtering of local interference (such as LTE 3G/4G phone service)**

Email from Tom Richardson (2/10/11) (this is regarding Robert Houts from Harris in Irving, TX)

Reference:

081030 Antenna spec for out of band attenuation.

Out-of-Band Attenuation: 30 dB min. @ $F_o \pm 50$ MHz

Receiver spec for out of band attenuation.

RF Jamming Immunity Provide up to 10dBm of immunity, utilizing the Adaptive Tracking Loops algorithm built in the Firmware. I don't know if there is any filtering in front end.

I don't know if this is same guy as before but we have used the ANT-35, GPS ANTENNA W/35db GAIN, Spectracom part no. 236015, which has better filtering in antenna. Filtering • 60 dB minimum at ± 50 MHz

Elevation Masks

- Allows for portions of the sky to be blocked from satellite reception.
- Supported in our receivers but we there is no user-interface provided for customers to use this function.

Anti-spoof:

The SecureSync, unless purchased with a SAASM GPS receiver, has no anti-spoof capability (please note that the SAASM GPS receivers can only be purchased by qualified US Military or NATO organizations).

Anti-jam:

The GPS receivers do have some anti-jamming capabilities, though. If the GPS receiver detects its being jammed by a nearby transmitter at the same or harmonic frequency of GPS, the GPS receiver will internally reset, to try to eliminate the jamming.

GPS spoofing (anti-spoofing) versus GPS jamming

Note:

- 1) GPS Spoofing is the act of introducing bad/wrong timing (or other data) into a GPS receiver.
- 2) GPS jamming is the act of introducing a frequency that prohibits the GPS receiver from being able to track any satellites.

GPS spoofing (anti-spoofing)

Using a GSG GPS simulator to induce bad time into a SecureSync with a Rb oscillator installed.

Email from Jeremy Thomas to a customer (20 May 13)

To add to Keith's responses so far and with the assistance of our Chief Engineer John Westwood would like to provide some additional considerations for this proposal.

It is relatively easy to jam a receiver and difficult (but not impossible) to spoof. For both cases the Rx antenna must be visible to the false source which will likely present its own challenges for 'spoofers' where key often secure financial centres are involved.

For general jamming – the GPS rx will stop giving good results and the SecureSync (receiver) will enter oscillator holdover (or look at secondary inputs).

The GPS rx uses "overdetermined" mode when static is selected. After the initial position survey, the rx regards the position as fixed and then compares the timing results from each satellite – if any of these show a significant error (compared with the others) then it is ignored.

Again it is difficult to spoof once the GPS rx has the almanac as it will ignore satellites that it does not expect to see. This is why you have to do a cold start for receivers when simulating with a simulator such as our GSG. Cold starting the receiver would be out of 'spoofers' reach.

One additional security consideration is that as from June this year there will be a dual receiver GPS & GLONASS Securesync available. This will be an additional measure of protection as it is much more difficult to spoof both GPS & GLONASS at the same time . . . and in the right place as previously mentioned

Q (from Masataka 14 Nov 2012) And, they plan to implement to the system a mechanism for preventing the reception of invalid GPS signals (with incorrect time information) in a way described under [Process] at the bottom of this message when such a signal reaches SecureSync 1 ("SS1" hereafter) on the transmitting side.

In this connection, could you please answer the questions below:

When the GPS signal coming to SS1 recovers to the normal state (having the correct time information), is there any status item (e.g. "TFOM", "ETE") that tells the user the recovery? If yes, please let us know how the status changes when the signal recovers to the normal state.

As there is no way to know this recovery timing in Step 5 of the [Process] below at present, the customer cannot tell when they should enable GPS again. If there is any status item that tells the GPS signal recovery on SS1, they can manually set "GPS" back to "Enabled" on the Priority Reference Setup page at the right moment by monitoring the status.

[Process]

1. SS 1 on the transmitting side is receiving normal GPS signals (and TFOM is at <3 at this time).
2. SS1 detects an invalid GPS signal (with incorrect time information).
3. SS1's TFOM deteriorates to ">3" because SS1 detected invalid GPS signals.
4. The customer disabled "GPS" on the Priority Reference Setup page when TFOM becomes >3 to prevent the invalid GPS signal reception.
5. When the GPS signal recovers to the normal state, the customer enable "GPS" on the Priority Reference Setup page again to make it possible to receive normal GPS signals again.

A Email from Dave Sohn (14 Nov 2012) I'm not sure there is a good way of doing what they are asking unless there are some indicators from the GPS receiver itself. For steps 1 - 3 of their process, they can set a Max TFOM value, which would provide an indicator through the entering of the holdover state when TFOM rises above that. They could then disable the GPS reference based on that. Once they do that, we no longer track the TFOM value generated from trying to sync to the GPS, so you can't use that to determine when to go back into sync with the GPS receiver. If the receiver provides indication of the problem through loss of satellites or its DOP values, those are available to the user (satellites from web UI, SNMP, CLI... DOP from SNMP, CLI). They could enable the GPS reference once those were back at acceptable levels. I don't know that the timing problem they are hoping to avoid would be visible in either of those indicators.

A Email Keith sent to Masataka (14 Nov 2012) I have some information for your regarding the desire to prevent the reception of invalid GPS data signals by the SecureSync (or any other NTP server).

To begin, what you and your customer are referring to when discussing the presence of invalid GPS data is called "Spoofing" the GPS signal. The ability for a GPS receiver to be able to detect and reject invalid GPS signals is called "Anti-Spoofing".

Commercially available GPS receivers (such as the GPS receivers installed in most NTP time servers) do not have "Anti-Spoofing" capabilities. "Anti-Spoofing" capability is limited to only specific types of GPS receivers which are not commercially available. The distribution of these unique GPS receivers (known as SAASM GPS receivers) is highly controlled by the US Government and are only available to qualified US Military / Dept of Defense and NATO organizations.

Unless your customer happens to be a US-approved NATO organization, they will not be eligible to obtain a SAASM GPS receiver. Therefore, they will only be able to obtain the standard, commercially available GPS receiver.

As all commercially available GPS receiver won't have "Anti-Spoofing" capability, the GPS receivers used in the SecureSyncs (or any other NTP server with a commercially available GPS receiver) will have no dedicated protection against spoofing of the GPS signal. The commercially available GPS receivers we use in the NetClocks and SecureSyncs have some protection against spoofing, but have no dedicated anti-spoofing capabilities, how the GPS receiver operates in a spoofing attack is unpredictable, and affected by many different variables. In some cases, the GPS receiver may reject the spoofed signals, while in other cases it may accept the spoofed signals as being valid. In a "spoofing scenario", the GPS receiver may happen to drop to 0 satellites being tracked. Or, the 1PPS signal from the GPS receiver may become erratic. These are the only two conditions that might indicate the GPS receiver is actively being spoofed. If the GPS receiver happens to drop to 0 satellites while its being spoofed, the GPS receiver dropping to 0 satellites will cause GPS to become a "not valid" input reference. If there are any other lower-priority input references available, the SecureSync will switch to another reference. If there are no other input references available, the SecureSync will go into Holdover mode, until at least one GPS satellite is tracked again. If the 1PPS signal from the GPS receiver is affected by the spoofing signal, the TFOM value would potentially increase.

These potential conditions can provide indications that the GPS signal may be actively being spoofed. If the SecureSync goes into Holdover mode because GPS is the only valid input and it happens to drop to 0 satellites being tracked, the Holdover alarm will be asserted and an SNMP Holdover trap can be sent. There is also a user-defined alarm and SNMP trap available that can be generated/sent if the GPS receiver starts tracking less than a user-specified number of satellites (if this alarm is enabled and configured to alarm if the GPS receiver drops below 4 satellites, for example, and the GPS receiver drops to 0 satellites, the user-defined alarm is asserted and the associated SNMP trap can be sent).

If there are other lower-priority valid references available (such as IRIG or have quick for examples) and the GPS receiver happens to drop to 0 satellites, the SecureSync will switch to using the lower priority reference and the "Reference Change" will be logged (and email can be sent for this condition). Also, the Status -> Time and Frequency page of the browser will also indicate GPS is not valid, if the GPS receiver happens to drop to 0 satellites during a spoofing event.

If the GPS receiver happens to drop to satellites, when it is able to start tracking satellites again, it will become a valid input reference again. If it's the highest priority input that is valid, the SecureSync will switch back to using GPS as its reference again. GPS going back to being a valid reference again, (s indicated by the **Status -> Time and Frequency** page showing GPS is a valid reference again, and additional SNMP traps that can be sent, will indicate to your customer that they can then re-enable GPS input in the Reference Priority table.

Q. Email from Masataka with TOYO (9 Nov 2012)

Customer tried following procedure using GPS simulator and SecureSync to investigate how SecureSync behave when incorrect GPS signal (which has incorrect time information) is input suddenly.

<Procedure>

- (1).SecureSync is using GPS as reference. (At this time,TFOM is 4 and MAX TFOM is 3. So,Sync LED is orange.)
- (2).Slide "Time" value of all GPS signal output from GPS simulator.
- (3).TFOM value changed from "4" to "3" temporarily. So,"Sync" LED changed to Green.
- (4).TFOM changed from "3" to "5".
- (5).TFOM keeps "5" ever after.

In (1)-(5) step,TFOM value get lower and then higher.(4-3-5) Could you please let us know why it behave as above?

*We realize that TFOM value should get higher at first and then get lower.

In step (3), TFOM value should get higher because phase of 1PPS reference step away by step (2).

In step (5), TFOM value should get lower because phase of 1PPS output from oscillator get close to 1PPS reference.

A. Email reply from Dave Sohn: The phase error and TFOM values are based on unsigned phase error magnitudes. It is possible that the time change from the simulator crossed from positive to negative or vice versa, and the calculations and filtering initially indicated this as a smaller error magnitude value as it transitioned. In the end the error value increased as the calculations caught up to the time shift provided by the simulator. Since the TFOM values are in a logarithmic scale, sometimes it may appear that the algorithm is not synchronizing the reference because the phase alignment is occurring at a much smaller magnitude per second than the TFOM shows. It may be better to watch the phase error value to see it decreasing slowly over time, which will eventually bring down the TFOM value. Another note is that the Rubidium disciplining uses very long loop constants, so it may take some time for the alignment to

occur.

Using a STA-61 to help detect a spoof attack

Q. Email from Dick Fox to Dave Sohn (15 Nov 2012)

I wanted to get your perspective on what Google is doing to identify potential time discontinuities cause by a possible GPS issue including spoofing

They have purchased standalone Rubidium Oscillator – SS. They initially sync SS to GPS and then let the SS free run in hold over mode They compare the 1 PPS from our GPS based TSync boards with 1 PPS from the free running SS rubidium unit. And look for and major discontinuities that could be introduced by GPS

I am tempted to offer this approach as a way for them to look for a “disturbance in the force”

STA-61 could do this very nicely. This wouldn't be automatic, but could allow them to determine when a disturbance happened. Take some corrective action and disable the GPS reference

When the disturbance is over they can manually enable the GPS reference. Any thought on feasibility of the approach?

Dick

A Dave Sohn responded with: They would need to periodically resynchronize the unit with a rubidium oscillator to GPS, but otherwise that could work.

****Non-Spectracom ANTI-JAM GPS Antennas**

******Novatel Model GAJT antenna**

- **Refer to:** <http://www.novatel.com/products/gnss-antennas/gajt/>
- Pronounced “gadget”
- These antennas are NOT available from Spectracom
- Good for localized GPS jamming
- Very expensive antenna

Email from Lisa Perdue (1 Dec 14)

The GAJT is about 25k-27kUSD if I am remembering correctly.

Keith is right in that if the jamming is right on top of the antenna will not be able to block it, but normally the jammers are not that close and the antenna will work. It would probably work well for the type of jamming we suspect is happening at the Harris site.

Because of that jamming situation and the potential for others, Spectracom has been working on a lower cost solution for our customers. We are working with a partner company to develop an antenna using a similar approach to the GAJT antenna, at less than half of the cost of the GAJT and that would be directly compatible with our NetClock and SecureSync products (no additional integration work by the customer is needed).

If you would like to discuss this project further, I am copying our CTO, John Fischer, on this email. He would be the point of contact for discussion on our new product.

Link to VIC100 GPS antenna (our P/N 236015): <I:\Engineering\GPS Antennas> (Panasonic VIC 100)

Customer has to realize that the GPS signal is a very low level signal, -130 dBm, and can be swamped by a large signal no matter what the filtering. No transmission is perfect, all have skirts, yada yada...

P/N for the inline GPS filter

8225 “SA-300” (started shipping after about 5/1/08 with a Serial Number above about 9800): **62 ohms**

8225A (S/N 0840 and above) = **176 ohms**

8225 (S/N 0839 and below) = **377 ohms** or **70 ohms**

Square 8227 (shipped after around 5/1/08) = **91kohms**

Circular 8227 = (Shipped before about 5/1/08) = **152 ohms**

Newest style Rectangular 8227 (our P/N "AR02-1587-2002" from GPS Networking (their P/N MLA20RPDC-N) started shipping around Sept 2011= 9.3 kohms.

8225 and 8227 = 110 ohms

8225A and 8227 = 82 ohms

8228 - both mounting styles – (Motorola) **240 ohms** (8189 manual has typo of **140 ohms**). (Stopped selling 3/2003)
(Hawk antenna) (Cut-in ~Mar 2003). Reads about **4-5 megaohms**.

ANT35 (ANT-35) The Model ANT-35 GPS antenna impedance starts at 1,000,000 - 5,000,000 ohms reading, and then starts to decrease. After 10 seconds or so, it stabilizes at about 690,000 - 700,000 Ohms.

GPS/GNSS ANTENNAS

General Cabling/Antenna installation info provided to/available for customers

- Refer to online NetClock user guide:
http://manuals.spectracom.com/NC/Content/NC_and_SS/Com/Topics/CONFIG/Conn_Ref_Inputs.htm
- Refer to **Model 8230 user manual (1222-5000-0050)** in Arena: https://app.bom.com/items/detail-spec?item_id=1202835947&version_id=10498638648&orb_msg_single_search_p=1
- Refer to the available “**Outdoor GNSS Antenna Installation Considerations**” Tech Note on our website:
https://spectracom.com/sites/default/files/document-files/GPS-Antenna-Installation_TN07-101_D.pdf
- Refer to the “**GPS Survey**” (Model 8225 pre-install questionnaire Keith created back in 2006 to help installers before purchasing our equipment): <I:\Customer Service\GPS\spectracom GPS Survey Page.doc>
 - note this doc needs some updating

(As of at least April 2019) the NetClock and SecureSync user guides currently provide VERY little (like “connect the cable to the back panel”) info antenna installation (no details at all on cabling). They refer customers to the Model 8230 user manual (1222-5000-0050) included with the antenna. This very brief two-page document provides physical mounting/bracket info, but no details on cabling/media converters, etc.

The available “**Outdoor GNSS Antenna Installation Considerations**” Tech Note on our website (mentioned below) provides much more details on cabling/antenna install and media converters. But its not currently referenced in either the NetClock/SecureSync user guides or the Model 8230 user manual. Keith recommended (24 April 2019) that either a link to this Tech Note on our site is added to all three customer documents, if not adding the info from this tech note to the Model 8230 antenna user manual.

****Antenna installation Tech Note (“Outdoor GNSS Antenna Installation Considerations”) on our website**

- https://spectracom.com/sites/default/files/document-files/GPS-Antenna-Installation_TN07-101_D.pdf

email from Dave L (23 Apr 18) Here is a link to a Tech Note describing GNSS Antenna Installations. https://spectracom.com/sites/default/files/document-files/GPS-Antenna-Installation_TN07-101_D.pdf. Our antenna cables are a LMR400 type, which is what we recommend for antenna installations.

*** Corrosion on outdoor connectors/cleaning corrosion off connectors**

Email from Dave Lorah (9 July 2019) For cleaning the connections, **Isopropyl Alcohol** will work as a degreaser but to clean corrosion you may need some sort of chemical. Here is a short article I found on the web:
<http://www.madsci.org/posts/archives/2000-04/955052616.Eg.r.html>

We recommend using a weatherproof enclosure if the surge suppressors are installed outdoors to prevent any chance of moisture damage. The surge suppressors are not weatherproof devices.

Available weatherproofing kit for outdoor cable install

- Weatherproofing kit, with cable wrap, vinyl tape and instructions.
- **Spectracom P/N:** 1142-0000-5001 (in Arena) https://app.bom.com/items/detail-spec?item_id=1202838955&version_id=10489975928&subview_mode=0
- **Link to manual (documentation):** <I:\New Released\Manuals\1142-xxxx-xxxx> (1142-5000-0054)
On our website: https://spectracom.com/sites/default/files/document-files/1142-5000-0054_rev_b_weatherproofing_kit_inst_guide.pdf
- **Link to info in Salesforce:** <https://na8.salesforce.com/01t80000002Axan?srPos=0&srKp=01t>

The Weatherproofing Kit consists of the following:

- Weather Proofing Wrap
- Vinyl Electrical Tape

International shipping Regulations (HTS code, ECCN Number, EAR, CCATS, etc)

- For details refer to (in this document): [Export control \(HTS and ECCN numbers\) for all products](#)

Refer to Export Control matrix

- <I:\Trade Compliance\Export Control Matrix>
- <I:\Customer Service\Export Control-HTS and ECCN numbers>

For 8230s

US HTS code: 8543.70.9910

Europe HTS code: 8543.70.3000

ECCN number: EAR99

**GPS Antenna Height/Altitude/Elevation

- GPS specifies altitude as HAE (height above ellipsoid) referenced to the WGS84 ellipsoid.
- Many receivers specify height as relative to MSL (mean sea level).
- These are not the same!

The difference can typically be several tens of meters and can be up to 100 meters

Q. In the 9383 NetClock, it is reporting a -60 metres (negative height) antenna height.....at one particular. Other sites seem to be positive height e.g 30 metres.

A Email Dave Lorah sent to customer (28 Jul 2014)

The elevation is based on the "ellipsoid height" of the earth and can sometimes actually show the height as negative. This is normal.

Here is a very nice explanation of this:

<http://www.esri.com/news/arcuser/0703/geoid1of3.html>

Email from Paul Myers (4/12/11):

Keith,

The altitude a GPS receiver provides has to be based against some reference. Altitude can be referenced to Mean Sea-level (GEOID) or Height above a ellipsoid that modes the shape of the earth (Or other models).

The GPS receiver is configured to determine altitude against a selected model and the accuracy can vary from actual altitude surveyed against sea level.

The Resolution-T defaults to MSL (Mean Sea-Level using the WGS-84 Earth model ellipsoid. See GGA message of NMEA for example.

I believe the Polaris Link does also. (I don't remember the Force 22E...)

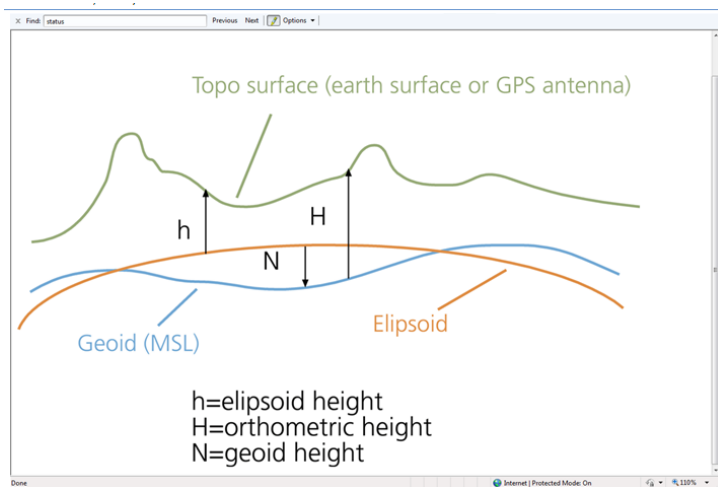
See http://trl.trimble.com/docushare/dsweb/Get/Document-221342/ResolutionT_UG_2B_54655-05-ENG.pdf

See page 79-81 for example of data in a message.

See the figure below- Altitude s based on a model close to the earth surface which can vary by 10's of meters.

http://www.esri.com/news/arcuser/0703/graphics/geoid2_lg.gif

<http://www.esri.com/news/arcuser/0703/geoid1of3.html>



*** Interference from other transmitters (near a GNSS antenna)

Note: Tom Richardson included the Tallysman TW3470_TW3472 data sheet with his response below.

Q, the radio antenna has not been installed yet. I want to find out if it will interfere once installed. Do you know if radio antennas will interfere with the GPS unit?

A Email from Tom Richardson (12 March 2020) Short answers;

GNSS signals are at 1.57542 GHz and -160 dBW at the earth's surface... Any harmonic falling on this frequency will interfere.

Anything transmitting close to the frequency can have noise skirts that will jam the GNSS signals. See LightSquared Inc. controversy

<https://www.novatel.com/tech-talk/thought-leadership-series/interference-and-jamming/#q-and-a>

An antenna at any frequency putting out a RF signal can overload (swamp) the low noise amplifier in the active antenna we sell. Like Keith said, it depends.

If possible, moving the antenna farther from the interfering source can be a solution.

Q Reply from customer Looking at that signal we have 850 Mhz at about 18 W (42.55 DBm) at the panel antennas a few meters away.

Depending on the amount of filtering from the antenna through the amplifier to the receiver it could be OK.

Here are the numbers:

850 Mhz Fire Department 3rd harmonic = 2.55 Ghz (We are 1G away from GPS).

A Reply from Tom Richardson (12 March 2020) The interference will depend on the signal and noise at the receiving antenna. GNSS L1 is a 1 MHz wide signal centered at 1575.42 MHz and a very low level signal at about -160 dBW at the surface of the earth.

Looking at your installation the second harmonic of 850 is 1700 MHz which is 125 MHz away from GNSS. The antenna is designed for 1574 to 1606 MHz with filtering of >50 dB@1500 MHz to >70 dB@1640 MHz. See attached data sheet. So the 1700 MHz signal should be attenuated by at least 70 dB by the filter. 18 W = 12.55 dBW. 12.55 dBW - 70 dB = -57 dBW. That would be with the antenna right next to the receiving antenna. 15 meters of separation can give another 60 dB attenuation.

Here is a calculator; <https://www.pasternack.com/t-calculator-fspl.aspx>

Get as much separation from the broadcasting antenna as you can. Unfortunately, You would probably have to install and then see.

****Cross-talk/ multiple GPS antennas installed near each other**

Minimum recommended separation

- **Operational perspective:** Tallysman recommends a minimum separation of **1.64 feet (0.5 meter)** between each antenna (this is a factor of the GPS wave-length)
- **Lightning /surge perspective/redundancy:** as far apart as possible (to help prevent multiple antennas being damaged/destroyed)
- **Local Electrical codes:** local codes may have specific requirements that we aren't aware of.

Tallysman
Email Keith sent to the 8230 manufacturer
Hi Tallysman team,
Good day to you!

My name is Keith and I am with Spectracom Tech Support in Rochester, NY. I was referred to you by Tom Richardson, with our Engineering team.

As a reseller of your TW3472 GPS/Glonass antennas for use with our products, we are periodically asked what the minimum recommended physical separation is between more than one antenna being co-installed.

In the past, we have used a "general" recommended minimum horizontal separation of a "few meters". But I would like to be able to provide a more specific response, if possible. I started searching online for this recommendation and was finding quite a bit of variance, from a couple of inches of separation ("NEMA recommends at least six inches of separation") to a calculator recommending 20 ft. horizontal separation and 150 ft. vertical separation.

So I was wondering if you have any recommendations for what the actual minimum separation between the antennas should be, in order to prevent potential interference between them?

Reply from Gyles Panther gyles.panther@tallysman.com

Keith,

That's a good question. The GPS carrier wavelength is about 19cm and with two antennas a wavelength apart, interaction will be minimal. At a spacing of 3 wavelengths, effectively there will be no interaction. Simulation would be required for a more quantified answer, but probably 0.5meter separation would be a reasonable call. You could also try this using the reported C/No value in the \$GPGSV NEMA sentence if you would like a bit more confidence in the number. Let me know if you would like to discuss this further.

Even though GPS antennas are receive-only (do not transmit), they do contain active components. Placing the Model 8225 GPS antenna or any other manufacturer' GPS antennas too close together can affect their search pattern. To prevent the search pattern from being affected, the antennas should be installed at least a couple of meters apart from one another as well as the same distances away from any metal, if at all possible. Putting GPS antennas too close to each other can affect the input sensitivity of the received signal, resulting in lower signal strengths. After "installing" the antennas, you can use the GPS Signal Status page in the web browser of the Spectracom NTP server to ensure you are tracking several satellites and the received signal strengths are in the 40s and 50's for the satellites being tracked. If you see strengths lower than this, move the antennas further apart from one another to minimize the effect on the search pattern.

From Tom Richardson: Do not have them put antennas within inches of each other. There will be interaction between the antennas and a loss of sensitivity will result. A few meters separation should be sufficient to isolate the antennas from each other. If a noticeable decrease in sensitivity is noted they should try repositioning the antennas to improve reception.

Antennas need to be separated from surrounding metallic materials also. Any metal in the area changes the shape of the reception pattern of the antenna. Any buildings or metallic materials close to the antenna can create shadows also which will shield the antenna from receiving in that direction.

For best reception, I recommend an installation with a clear view of the sky down to the horizon in all directions).

Email Jodi sent to customer (7 Oct 2019)

We recommend that the antennas are installed at least 2 meters apart.

Even though GPS antennas are receive only (do not transmit), they do contain active components. Placing the Model 8225 GPS antenna, Model 8230 GNSS antenna, or any other manufacturer's GPS antennas too close together can affect their signal search patterns. To prevent the search pattern from being affected, the antennas should be installed at least two meters apart from one another as well as any metal, if at all possible. Putting GPS antennas too close to each other can affect the input sensitivity of the received signal, resulting in lower signal strengths.

If a noticeable decrease in sensitivity is noted, try repositioning the antennas to improve reception. Additional separation that creates a minimum space of two meters between antennas should be sufficient to isolate them from each other. Antennas also need to be separated from metallic materials in the installation area, which change the shape of the reception pattern of the antenna. Any buildings or metallic materials close to the antenna can create shadows which will shield the antenna from receiving in that direction. For the best reception, Orolia recommends an installation with a clear view of the sky to the horizon in all directions

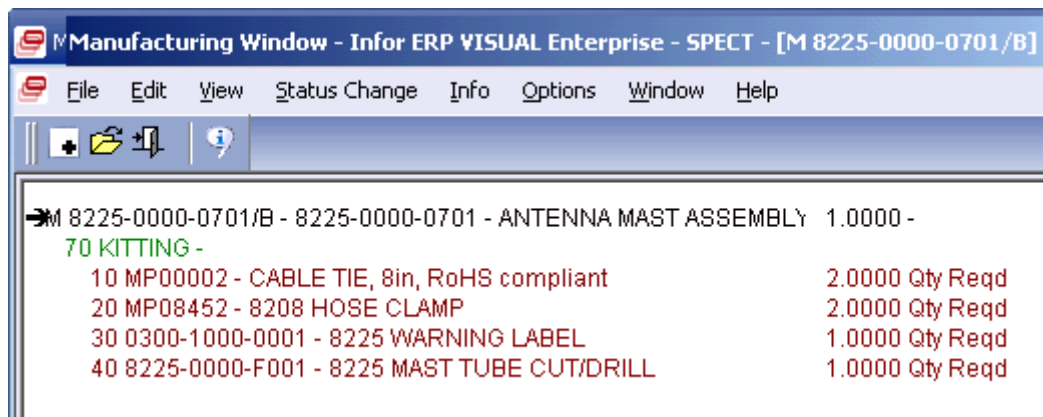
Email Keith sent to a customer (23 Apr 15) fortunately, the GPS antennas are receive-only antennas which do not intentionally transmit any signals. This significantly helps reduce the amount of separation needed between multiple antennas. The only concerns about separation are regarding EMI interference, which is limited to the active components inside of the antennas. More than one GPS antenna can be installed near each other with minimal separation required.

If the antennas are installed too close together there could potentially be interaction between the antennas and a loss of sensitivity can result. This could also adversely affect the search pattern of the antennas, resulting in fewer satellites being tracked. Just a few meters or separation should be sufficient to isolate the antennas from each other. If a noticeable decrease in sensitivity (resulting in weak signal strengths) and/or very few satellites being tracked is noted, you can then try repositioning the antennas to improve the satellite reception.

Also note that the antennas need to be separated from surrounding metallic materials. Any metal in the area changes the shape of the reception pattern of the antenna. Any buildings or metallic materials close to the antenna can create shadows which can shield the antenna from receiving in that particular direction. For the most optimal satellite reception, we recommend an installation with a clear view of the sky down to the horizon in all directions.

From strictly a redundancy factor, the antenna should be separated as much as physically possible, just to help isolate the antennas from being simultaneously affected by the same anomaly (such as a nearby lightning strike or a falling object, for examples).

****PVC mast assembly for the Model 8225/8230 antenna /included items



- Our P/N for the mast assembly: 8225-0000-0701
- The raw PVC pipe P/N is 067013.

- **Link to drawing for the mast assembly (8225-0000-F001):** <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\8225, 8225S, 8226, 8227 and grounding kit>
- **Link to process detail for mast assembly (8225-0000-0701):** <I:\New Released\Process Details\8225-xxxx-xxxx Process Details\8225-0000-0701>
- **Our P/N for the two provided metal hose clamps:** MP08452.
- **PVC pipe diameter:** Standard 1 inch “Schedule 40 PVC” (1 5/16 inch outside diameter).

Pipe length: 48.9 cm / 19.25 inches long

Threaded connector we place on end of mast assembly (mates with antenna collar): It is a union that we used one of the three pieces to attach to the PVC pipe. Our P/N for the union is 038009 Manufacturer is Colonial Engineering. Their P/N is C10286 <http://www.colonialengineering.com/html/unions.html>

*****Model 8213 / Antenna mounting for Models 8230 and 8225:**



*Model 8230 GPS/GNSS
Outdoor Antenna with optional
PVC Pipe (Model 8235) and
optional Flat Roof Mount
(Model 8213)*

Model 8213 Declaration of Conformity

- Refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Declaration of Conformity>

Note: The Declaration of Conformity for the Model 8213 is included in the SecureSync's Declaration of Conformity Certificate.

Per Dave Sohn (15 Jun 15): it includes EN 60950-1:2006/A11:2009 for safety. We don't test to EN61000-6-1:2007 or EN 61000-6-3:2007, instead testing against EN 55022:2006/A1:2007 for Class A emissions, and EN55024:1998/A2:2003 for immunity.

(From Model 8230 data sheet)

Flat Roof Mount Specifications (sold separately)

Mechanical

Material: Aluminum Base

Height: 6" (15.24 cm)

Diameter: 15.625" (39.7 cm)

Weight: 17 lbs. (7.7 kg) when filled with ballast (included) for stability

Antenna mounting

- (2) Hose clamps supplied with mast assembly



- **MFG and their P/N:** McMaster Carr P/N 5322K22 <http://www.mcmaster.com/#catalog/120/295/=q9e4nc>
- **Spectracom P/N** MP08452
- (2 inch to 6 inch clamp diameter)
- They are about 21 inches long

Quick-Opening Worm-Drive Hose and Tube Clamps



The slotted hex-head screw flips up to release the band for quick opening. Clamps are reusable. All have a Type 201 stainless steel band and housing, which offers good corrosion resistance. The band is 9/16" wide and 0.022" thick. Not recommended for use with silicone hose and tube.

Clamps with Zinc-Plated Steel Screw—Screws have a clear coating and offer fair corrosion resistance. Tighten with a wrench, slotted screwdriver, or 5/16" hex nutdriver. Torque is 35 in.-lbs. Temperature range is -40° to +375° F.

Clamps with Type 410 Stainless Steel Screw—Screws have good corrosion resistance. Tighten screw with a wrench, slotted screwdriver, or 3/8" hex nutdriver. Torque is 35 in.-lbs. Temperature range is -40° to +800° F.

Note: When choosing a clamp, measure the outside diameter of your hose or tube with the fitting installed.



Clamp ID Range		With Zinc-Plated Steel Screw				With Type 410 Stainless Steel Screw			
Inch	mm	SAE No.	Pkg. Qty.	Pkg.		Pkg. Qty.	Pkg.		
1/2"-1 1/4"	13-32	12	10	5322K14	\$8.31	10	5322K53	\$13.00	
3/4"-1 3/4"	19-44	20	10	5322K15	8.21	10	5322K54	13.80	
1"-2 1/4"	25-57	28	10	5322K16	8.73	10	5322K56	14.39	
1"-2 3/4"	25-70	36	10	5322K17	9.04	10	5322K57	15.23	
1"-4"	25-101	56	10	5322K19	12.06	5	5322K59	9.97	
1 1/2"-3 1/2"	38-89	48	10	5322K18	11.15	5	5322K58	9.56	
1 3/4"-7"	44-178	104	5	5322K23	9.52	5	5322K63	14.35	
1 3/4"-7 3/4"	44-197	116	5	5322K34	9.94	1	5322K64	3.01	
1 13/16"-15"	46-381	232	1	5322K37	2.55				
1 13/16"-18 1/2"	45-470	288	1	5322K41	3.05				
1 15/16"-16 1/4"	49-413	258	1	5322K38	2.93				
2"-5"	51-127	72	10	5322K21	14.06	5	5322K61	11.89	
2"-6"	51-152	88	10	5322K22	14.60	5	5322K62	13.12	
Product Detail									
Quick-Opening Worm-Drive Hose and Tube Clamp, 2" to 6" Clamp Diameter Range, Zinc-Plated Steel Screw									
Packs of 10									
ADD TO ORDER									
In stock									
2"-10"	51-254	152	5	5322K36	12.53	1	5322K66	3.37	
2"-12 1/4"	51-311	188	5	5322K24	9.55	1	5322K67	3.73	
2 1/16"-17"	52-432	272	1	5322K39	2.92				
2 1/16"-21 1/4"	52-540	332	1	5322K42	4.99	1	5322K68	5.06	
2 1/4"-8 1/2"	57-216	128	5	5322K35	10.05	1	5322K65	3.12	

Mounting antenna to a vertical surface

The Model 8225 GPS antenna is attached to a Schedule 40 PVC mast with a 1 5/16 inch outside diameter. The top of the mast assembly has a threaded mating connector which screws into a mating connector at the bottom of the antenna. The mast assembly has a groove in it so the antenna cable can be threaded up the inside of the mast assembly to the top of this connector. The mast is approximately 20 inches long.

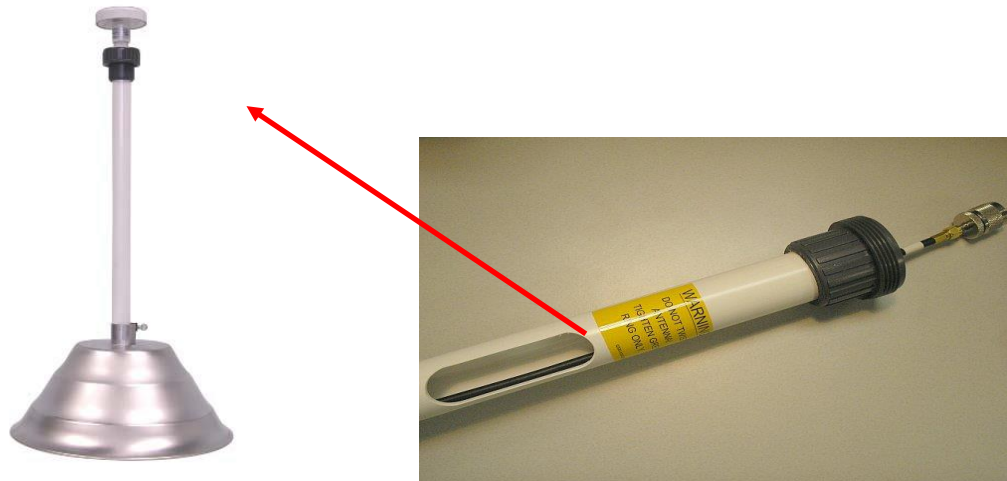
The mast assembly includes two metal hose clamps (approximately 18 inches long) that can be wrapped around the mast assembly to attach it to a station on the roof *such as a metal railing, vent duct, etc) for vertical mounting of the mast assembly. Spectracom also offers the Model 8213 flat-roof mount which is a weighted-base/stand (like the umbrella stands used with for tables) that the mast assembly can slide into to keep it standing straight-up. The Figure below shows the Model 8213 at the bottom of the mast assembly (this picture shows the Model 8225 GPS antenna attached to the top of the mast, instead of the TSAT dome antenna, but the TSAT dome antenna is mounted in the same fashion).

We've also had some customers procure a locally manufactured mount for the side of the building (preferably near the roof for a better view of the sky).

Antenna cable through the mast assembly (such as when using the Model 8213 base)

Q. When it is mounted on the PVC mast, I assume that the coax cable is running down the PVC mast. Where does the cable exit when you are using the 8213 flat roof antenna mount?

A. Keith's response: There is a large slot in the PVC mast, just below the connector that allows the antenna cable to pass through the mast assembly.



Custom brackets/Mounting



Mounting antenna to a horizontal surface (instead of to a vertical surface)

Email from Jeremy to a customer

I'm sorry but I guess we don't offer a horizontal mounting kit. Below is the thread from our support guys. I think however a good option would be to use a "T" style saddle clamp such as this one: <http://www.directindustry.com/prod/coraplast/service-saddle-clamps-89105-853503.html>

The specific one on the link may not be the correct diameter and such, but the style would work perfect I think. And I would actually drill 4 holes in it and include bolts which would help secure it further from falling over such as seen here:



Depending on the saddle clamp, the additional bolts may be over kill...but then again it's probably worthwhile to save the potential headache of having to deal with the techs there to fix anything if something happens.

******Wind resistance for the Models 8230, 8225 and 8213 (flat roof-mount base)**

“The Spectracom model 8213 flat surface antenna base mount will withstand up to 150 mph winds when the base mount has the full 12 lbs of sand (provided). This also assumes the full antenna mast length provided with the 8225 GPS antenna is used with the mount.”

Email from Scott Holmes (3/22/11) (as applicable to the Synergy Timing 1000 antennas)

Hi Keith,

I noticed that the current antenna has twice the side surface area as the older 8225 so I re-figured the side force at 150MPH with the new antenna size and, as expected the force was doubled. However, we are still under anything that would damage the mast so the 150 MPH limit is still OK.

If they are using the umbrella stand to mount their antenna they just need to make sure it is well weighted (15 lbs minimum) and the mast is secured in the stand with the thumb screw. Attached is a worksheet.

(Note: for the “**8225 Wind Loading Calculation**” worksheet referenced in Scott’s email above, refer to: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8225](#)

Note (Regarding the newer 8230 antenna): This info above was originally written for the Model 8225 antenna. On 29 Apr, 2015- Scott Holmes emailed me “**You’re correct, the wind load will also be 150MPH for this antenna.**”

Model 8235 / Model 8238 antenna mounting kits



Model 8230 GPS antenna purchase (P/N 1222-0001-0600) includes:

Note: Antenna purchase does not include mast assembly (refer to optional Model 8235 antenna mounting kit further below)

- Model 8230 Antenna
- (2) cable ties
- (2) metal hose clamps (our P/N
- (1) L bracket (Our P/N: MP10R-0000-0004)

Link to drawing of Tallysman L bracket (MP10R-0000-0006) in Arena: https://app.bom.com/items/detail-spec?item_id=1247634827&version_id=11001598408&

Models 8235 and 8238 Antenna mounting kits

A) Model 8235 antenna kit

- Refer to ECN 3243
- Shipping since Sept 2013

Visual P/N: 1222-0002-0600 (in Arena at: https://app.bom.com/items/detail-spec?item_id=1202847122&version_id=10221325668&orb_msg_single_search_p=1)

Links

- **Model 8235 in Arena:** https://app.bom.com/items/detail-spec?item_id=1202847122&version_id=10221325668&orb_msg_single_search_p=1
- **Model 8235 in Salesforce:** <https://orolia.my.salesforce.com/01tC00000003m4N9?srPos=1&srKp=01t>

This kit consists of:

- **PVC pipe Mast Assembly and hose clamps:** our P/N 1222-1000-0700 (length is 489 mm)

1. PVC pipe

Note this is the same schedule 40 post that's used with the Model 8225 antenna

- **P/N for just the PVC mast itself:** 1222-1000-0700
- **PVC Pipe length:** 33.4 mm dia. x 489 mm long

2. (2) Two Hose clamps:

our P/N MP08452 (2 **inch to 6 inch**) (see detailed info on brackets further above with antenna mounting info)

B) Model 8238 Antenna Mounting

- Refer to ECN 324

Visual P/N: 1222-0003-0600 (in Arena at: https://app.bom.com/items/detail-spec?item_id=1230481023&version_id=10696169258&orb_msg_single_search_p=1)

This kit consists of:

- A) Model 8230 antenna, cable ties, hose clamps
- B) L bracket (Our P/N: MP10R-0000-0004)

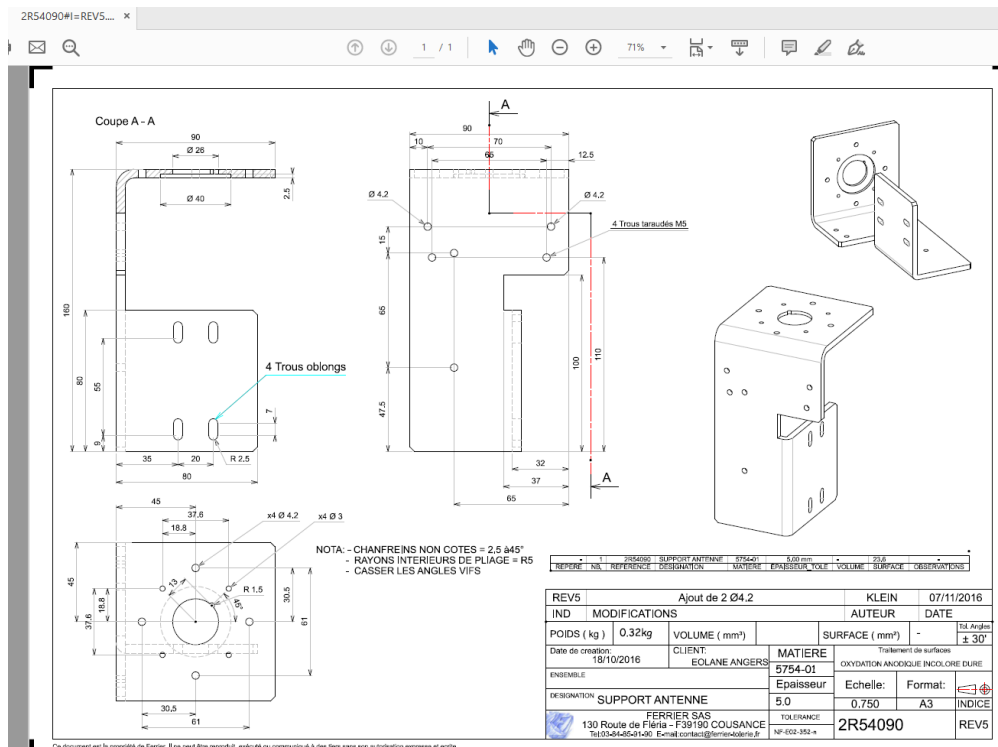
Optional Model ANT-KT “Rugged Post Mount Kit” for 8230 or ANT-35 antenna onto a vertical or horizontal post

- Link to ANT-KT data sheet: [I:\Marketing\ Product Data Sheets \(archive\)\GPS Antennas & Accessories](I:\Marketing\ Product Data Sheets (archive)\GPS Antennas & Accessories)
 - Data sheet on our website: <https://www.orolia.com/products/product-index/documents/mount>
- Spectracom P/N: 235846 (in Arena at: https://app.bom.com/items/detail-spec?item_id=1202847124&version_id=10212764838&orb_msg_single_search_p=1)

Drawings for ANT-KT

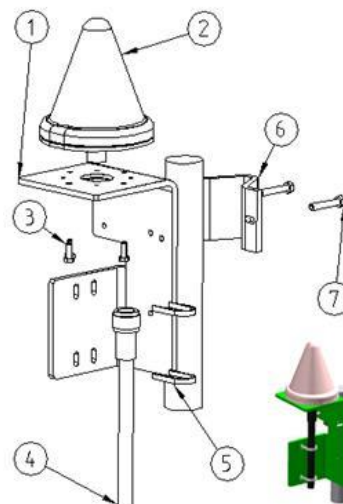
- Refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\ANT-KT rugged post-mount>

Drawing file 2R54090#1 (Created in Les Ulis, in French)



The optional Model ANT-KT post mounting kit allows you to mount the Epsilon GPS Antenna onto a vertical or horizontal pole. Kit includes:

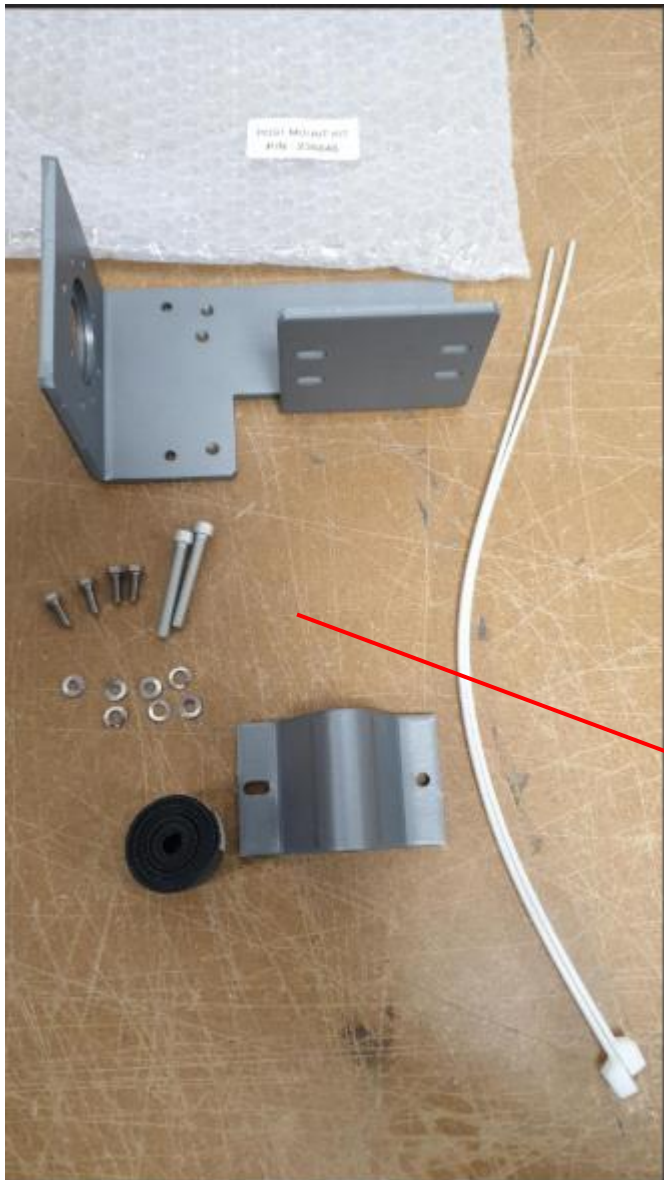
1. Post bracket
2. GPS antenna (purchased separately)
3. Screws
4. GPS cable (purchased separately)
5. Plastic cable tie
6. Post clamp
7. Screws & washers



See note below for specs on these screws

Metal that the bracket is made of: Aluminum
Contents of the kit (screws and such)

picture was supplied by Les Ulis



Sizes of the pipe that are supported by the Post Clamps: Post diameter 25 to 50 millimeters



Specs on the long screw for the post mount (Number 7 in diagram above)

Q What are the specs for the screws that are packaged with the rugged Post Mount kit?

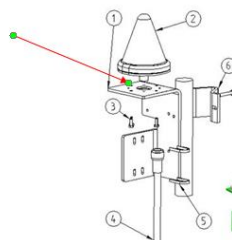
A reply from Joffrey Tuyant w/Spec France (15 Sep 17) The long screw in the post mount kit is a M5, 40 mm Aluminum hex head cap screw. See attached picture. This is the only information I have. This product is not in Arena but supported by Les Ulis.



A Earlier from Pierre (just before the one above) It seems that there are no specific recommendations about the screw dimensions. They just need to select the correct screw according to the wall or the way they want to fix it.

Compatibility of ANT-KT with the Raven/Forsberg DUC down-up converter's antenna

- (9 Jan 17) Dave L and Sadie confirmed the DUC converter antenna is not compatible with this bracket. Without modification of the bracket. There is no way to attach the DUC antenna to the bracket, because the hole at the top of the bracket is too small for the antenna to go through, and there is no way to fasten the antenna to this bracket.



HTS and ECCN codes for this bracket for international shipping

- Refer to (in this document): [Export control \(HTS and ECCN numbers\) for all products](#)
- Info below provided by Mary Slack to Jodi (4/26)

HTS: 8529.10.4080 **ECCN:** EAR99

Country of Origin/Manufacture: France

The part number for the post is either 235846 or ant-kt

Weight of just the kit by itself (as weighed by Keith, in the shipping area): 0.8 pounds

InfiniDome's GPSDome (inline add-on Anti-jammer from InfiniDome in Israel)

(GPS Dome)

IMPORTANT NOTE: GPSDOME REQUIRES TWO GNSS Antennas (such as 8230s and/or 8230AJ antennas be connected, in order for it to work!!!

Introducing GPSdome



Only Commercial (non-ITAR) GPS Anti-Jammer / Anti-Spoofers

- Revolutionary cyber product
- Retrofit protection of all GPS receivers
- Wields military tech in a minimal package
- Protects against both jamming and spoofing of GPS signals
- Uses a "front-end" approach which rejects high-powered interferences before they reach the receiver



11/15/2019

5

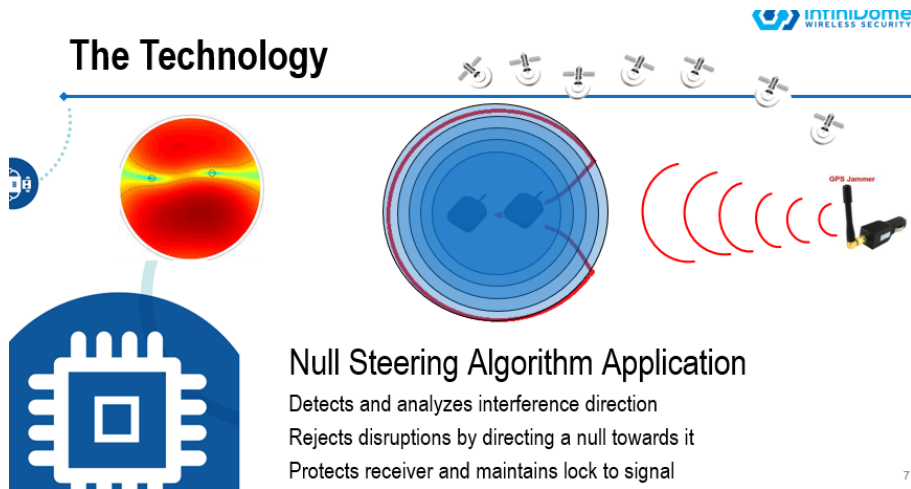
Links to:

- **GPSdome's Home page:** <https://www.gpsdome.com/>
- **Datasheet on our website:** https://www.rolia.com/sites/default/files/document-files/gpsdome_1.02b_-_military_systems_-_rolia_cobranded_-_8.5x11_2019-09-16.pdf
- **in Salesforce (for pricing/quoting):**
<https://rolia.my.salesforce.com/ui/search/ui/UnifiedSearchResults?searchType=2&sen=00a&sen=0F9&sen=a04&sen=02i&sen=0TO&sen=ka&sen=00O&sen=00Q&sen=001&sen=068&sen=003&sen=01t&sen=a0A&sen=00T&sen=005&sen=500&sen=00U&sen=006&sen=810&sen=a0E&sen=811&sen=a1N&str=gpsdome#!/fen=01t&initialViewMode=detail&str=gpsdome>

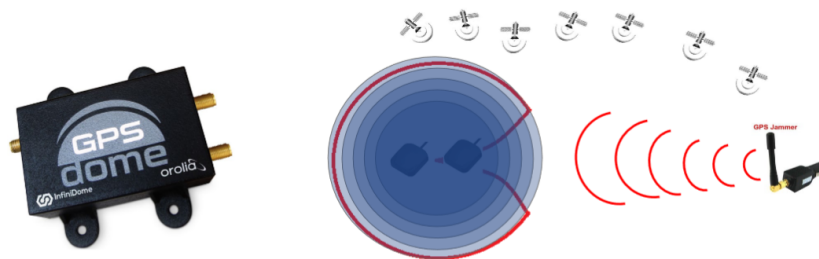
in Customer Service folder: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\GPSDome antenna](#)

Warranty length: One year (per Salesforce, at link above).

Description GPSdome is a small-sized, add-on device that provides protection against GPS jamming, ensuring continuity of autonomous navigation and operation during jamming conditions. No other solution that offers such protection is as small, light, affordable or as easily installed as GPSdome.



TWO ELEMENT CRPA ANTENNA

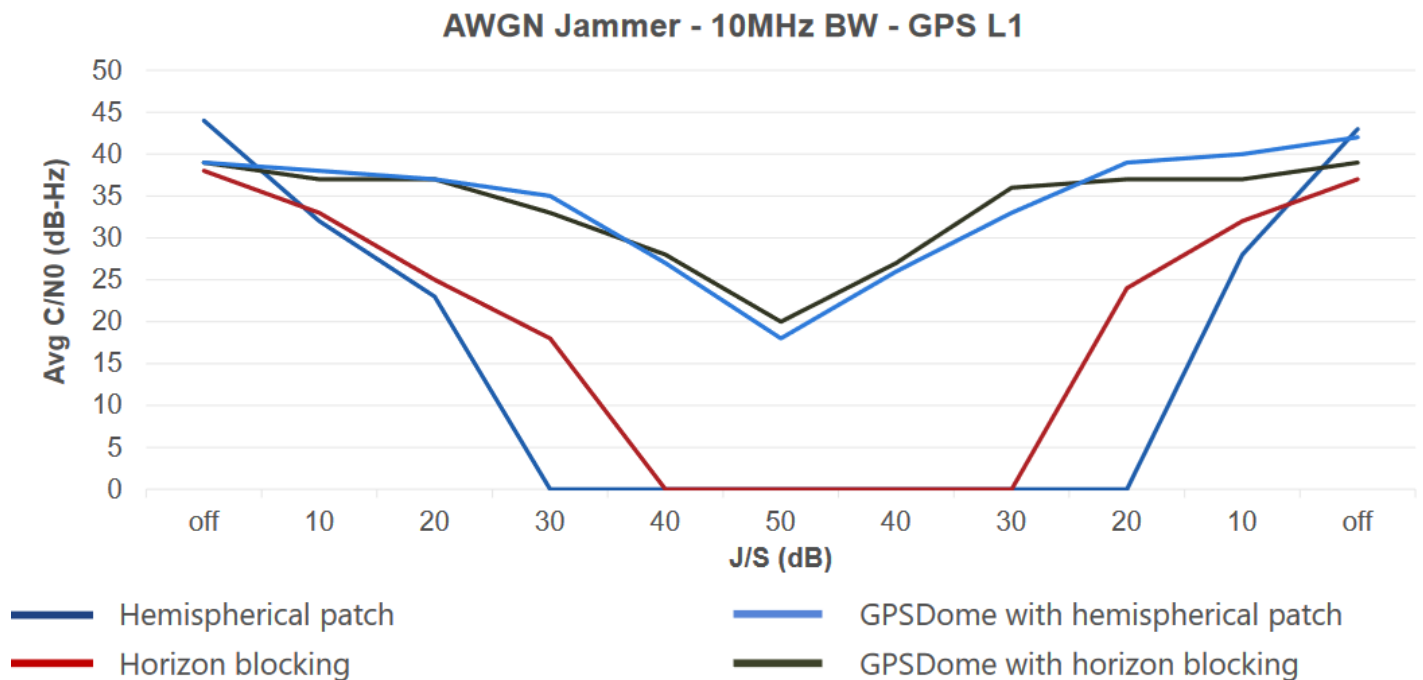


Single null is steered in the direction of the incoming interference

Internal comparison Testing results

- Refer to the PowerPoint training presentation in Customer Service folder: <..\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\GPSDome antenna>

NULL STEERER PERFORMANCE VS. BROADBAND JAMMER



Resilient Timekeeping for Critical Infrastructure | 2020

22

orolid

Applications

With GPS as the cornerstone of navigation, military systems can be completely disabled by simple GPS jammers available online today for less than \$50. GPSdome is suitable for a wide variety of GPS-dependent applications. GPSdome is a small sized, light weight, low powered solution suitable to be retrofitted to protect any navigation system. With GPSdome's protection, any military system immediately becomes more robust and protected against wireless attacks.

Features

- Null steering technology
- Small form factor: 70 x 48 x 24mm, 150 g
- Minimal power consumption: <0.75W• IP67, -40°C to +85°C

How GPSdome Works

GPS Vulnerabilities Are Well Known: Orbiting at 20,000KM above sea level, the GPS satellites emit a signal which is incredibly weak when received by GPS receivers (~-125dBm). To jam this signal, all one has to do is overpower it, either with a simple jammer bought online, which blocks it completely, or with slightly more sophisticated hardware that can trick it with erroneous data.

The Null Steering Algorithm was originally developed for military applications to protect wireless signals. GPS-dome adds our own sophisticated algorithms and proprietary RFIC to detect suspicious signals, combine antenna patterns and precisely target a null in the direction of the hostile signal.

Installation Couldn't Be Easier: After mounting both antennas on a flat, sky facing base at least half a wave-length apart (10cm minimum, 20cm is optimal), connect antennas to GPSdome, connect it to the antenna input on your GPS receiver, feed it with power and you're set to go.

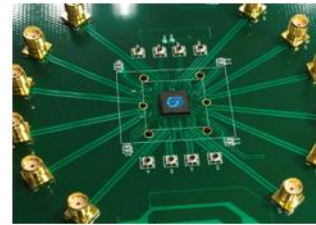
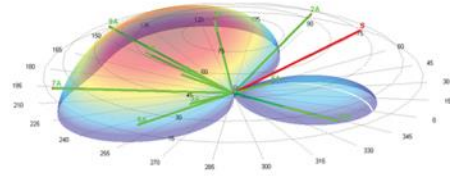
Jamming Detection is available from an LED on the GPSdome itself or via an external wire that could be integrated into any system computer



Our Solution: Military Tech – Reinvented

Low-Cost, Minimal SWaP, ITAR-Free

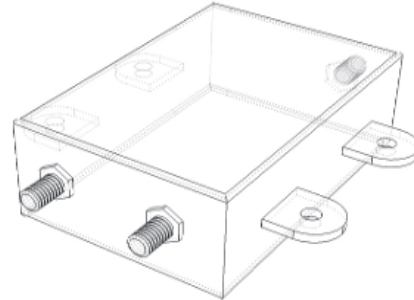
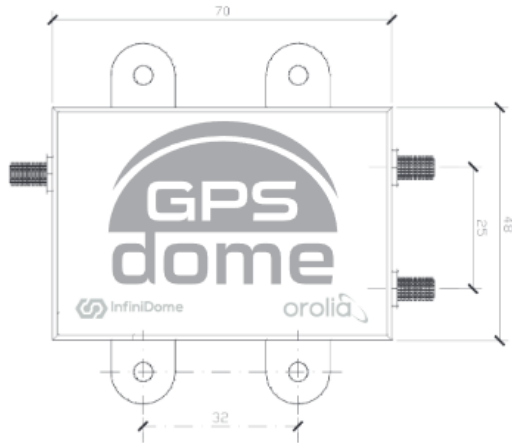
- Merges patterns from 2 antennas which enables real-time nullification of an interference from 1 direction
- infiniDome's patented architecture supports RF manipulation in real time introducing a small (100ns) constant delay in the RF chain



G.E. EHRLICH (1995) LTD. 11 Menachem Begin Road, 5268104 Ramat Gan, Israel	
to represent the undersigned before	<input checked="" type="checkbox"/> all the competent International Authorities <input type="checkbox"/> the International Searching Authority only <input type="checkbox"/> the International Preliminary Examining Authority only
In connection with the international application identified below:	
Title of the invention: PHASED-ARRAY ANTI-JAMMING DEVICE AND METHOD	
Applicant's or agent's file reference: 75947	
International application number: PCT/IL2019/050980	
filed by the undersigned with the following Office: ISRAELI PATENT OFFICE - Receiving Office, and to make or receive payment on behalf of the undersigned.	

Specification Summary

Dimensions



Physical	
Enclosure	70mm x 48 mm x 24mm (excluding mounting lugs)
Weight	150g
Mounting	4 x M3 bolts (not supplied)
Environmental	
Operating Temperature Range	-40°C to 85°C
Protection	IP67
Interfaces	
Primary Antenna Input (P)	50Ω SMA 2.75VDC designed for 26dB ±2dB gain
Auxiliary Antenna Input (A)	50Ω SMA 2.75VDC designed for 26dB ±2dB gain
Power Input	50Ω SMA *3.3VDC – 32VDC 0.75W *not for DF option

Performance	
Protected Signal	1575.42 MHz (GPS L1 C/A Code)
Latency	100ns ±15ns (fixed)
Compression Point	25dBm
Safety & Compliance	
R&TTE 1999/5/EC : EN60950-1 EN301 489-1 EN301 489-3 EN300 440-2	1575.42 MHz (GPS L1 C/A Code)
RoHS compliant	
WEEE registration number WEE/GK2929WW	
DF Wire Connection	
Red: 3.3VDC – 32VDC	
Black: GND	
Brown: Interference Indication	

Ordering Information

CAT NO	DESCRIPTION
Gpsdome 1.02B	Standard Product – VDC is supplied from the (R) connector
Gpsdome 1.02B DF	Additional 3 wire cable for 3.3VDC – 32VDC feed and Interference Indication

GPSDome P/Ns

- Infidome's Home page: <https://www.gpsdome.com/>
- Refer to ECO-2316 (Oct 2019) in Arena: https://app.bom.com/changes/detail-summary?change_id=2398970015&orb_msg_single_search_p=1
- Refer to ECO-2543 (Oct 2020) in Arena at: https://app.bom.com/changes/detail-affected?change_id=2403206828

Infinidome P/Ns:

Infinidome P/N	Our P/N	Power source
GPSdome 1.02B DF	GPSdome-1.02EPS-OS	Additional 3 wire cable for 3.3VDC – 32VDC feed and Interference Indication (<i>Powered by an External Power Supply</i>)
GPSdome 1.02B	GPSdome-1.02PPS-OS	Standard Product – VDC is supplied from the (R) connector (<i>Powered by the GNSS receiver</i>)
GPSdome 1.03 EPS	GPSdome 1.03 EPS	GPSdome unit - version 1.03 - unit is powered from receiver. Power input required: 3.3-32VDC 0.75W. Antennas purchased separately. Compatible with Active GNSS antennas with gain of 26dB +/- 2dB. Protects against jamming of the GPS L1 C/A signal and passes through GPS L2 signals.
GPSdome 1.03 PPS	GPSdome 1.03 PPS	GPSdome unit - version 1.03 - unit is powered from receiver. Power input required: 3.3-32VDC 0.75W. Antennas purchased separately. Compatible with Active GNSS antennas with gain of 26dB +/- 2dB. Protects against jamming of the GPS L1 C/A signal and passes through GPS L2 signals.
GPSdome 1.03 Unit Evaluation Kit	GPSDOME-1.03-EVKIT	GPSdome 1.03 Unit Evaluation Kit Evaluation Kit for GPSdome - version 1.03. Incorporates GPSdome unit - version 1.03 - External Power Supply variant, two u-blox receivers, and cabling. Includes three patch GPS patch antennas. USB connection for receiver communication and overall kit power.

A) GPSdome-1.0.2EPS-OS (external power supply)

- **EPS** = external power supply
 - This version of the GPSdome is powered by an external source using the provided wiring
 - Part number includes application of dual branded labeling
- In Salesforce at: <https://orolia.my.salesforce.com/01t0h000005ykFH?srPos=1&srKp=01t>
(**EPS** = external power supply)

Part number includes application of dual branded labeling

B) GPSdome-1.02PPS-OS (powered by receiver)

- **EPS** = external power supply
 - This version of the GPSdome is powered by an external source using the provided wiring
 - Part number includes application of dual branded labeling
 - **In Salesforce at:** <https://orolia.my.salesforce.com/01t0h000005ykFC?srPos=0&srKp=01t>
-

C) GPSdome 1.03 EPS (external power supply)

- **EPS** = external power supply
 - This version of the GPSdome is powered by an external source using the provided wiring
 - Part number includes application of dual branded labeling

GPSdome unit - version 1.03 - External Power Supply. Power input required: 3.3-32VDC 0.75W via 3 wire cable attached. External cable can also provide jamming indication to remote equipment. Antennas purchased separately. Compatible with Active GNSS antennas with gain of 26dB +/- 2dB. Protects against jamming of the GPS L1 C/A signal and passes through GPS L2 signals.

- **In Salesforce at:** <https://orolia.lightning.force.com/lightning/r/Product2/01t0h000005onRzAAI/view>
-

D) GPSdome 1.03 PPS-OS (powered by receiver)

- **PPS** = phantom power supply
 - This version of the GPSdome is powered by the receiver via the R connector.
 - Part number includes application of dual branded labeling

GPSdome unit - version 1.03 - unit is powered from receiver. Power input required: 3.3-32VDC 0.75W. Antennas purchased separately. Compatible with Active GNSS antennas with gain of 26dB +/- 2dB. Protects against jamming of the GPS L1 C/A signal and passes through GPS L2 signals.

- **In Salesforce at:** <https://orolia.lightning.force.com/lightning/r/Product2/01t0h000005onRuAAI/view>
-

Additional GPSdome Accessories

GPSdome install kit

- P/N: GPSdome-INST-KT
- In Salesforce: <https://orolia.lightning.force.com/lightning/r/Product2/01t0h000006BiGAAA0/view>

Kit includes: 6dB attenuator - Qty 2; Bias-T w/power supply - Qty 1; Cable - 5ft LMR 195 - Qty 1; Cable - 10ft LMR400 - Qty 2; Adapters - N-SMA 1ft cable - Qty 3; Weatherproofing kit - Qty 1

GPSdome-PoRF (GPSdome PoRF Bias Tee)

- GPSdome PoRF (Power over RF) is an add on module to GPSdome PPS unit
- In Arena at https://app.bom.com/items/detail-spec?item_id=1290383727&version_id=11795507918&

- PoRF (Power over RF) – provide Phantom Power Supply.

This unit gives power to the GPSdome PPS, in case the server cannot provide the required power.

Interfaces:

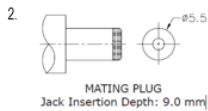
RF in – BNC connector, connect between the time server and the PoRF unit

RF out + DC – BNC connector, connect between the PoRF and the GPSdome

Power supply to the PoRF unit:

There are 2 options to connect the PoRF unit to power:

1. Micro USB



- LNA - Inline amplifier which allows for longer cable deployments

GPSdome Ordering

- GPSdome 1.02B PPS – List \$2150
- GPSdome 1.02B EPS – List \$2150
- GPSdome Installation Kit – List \$875
- Antennas
 - 8230 (x2)
 - 8230AJ (x2)
 - Customer Provided

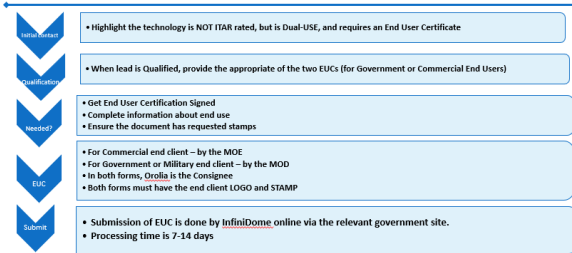
ITAR/Export/Shipping of GPSDome

- **NOT ITAR** controlled.
- Has to be exported out of Israel

Export Control – Dual use product (SUBJECT TO CHANGE)

- Worldwide export control distinguishes between government end users i.e. police, military and other official branches of the government and “civil” end users like Apple or BMW. This is also true for the Israeli export control.
- GPSDOME is a dual-use product. It can be used for civil and military applications.
- We must apply for an export license from the relevant office in Israel
 - Civil end users from the Ministry of Economics
 - Government end users From Israeli Ministry of Defense.
- **Export approval process is expedited by Infinidome**
- Note – in the process of a distribution approval for Spectracom Orolia

Export control – in practice



Availability of GPSDome

- P/Ns for GPSDome were released in October 2019

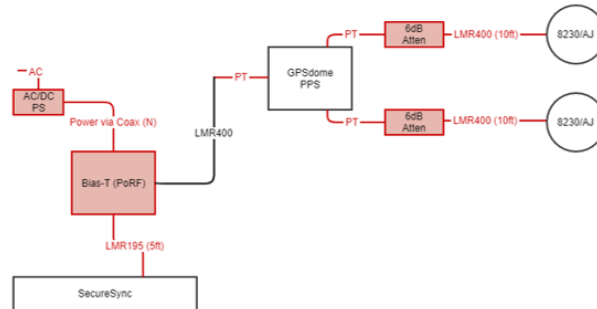
GPSdome Installation

- **Refer to GPSdome install guide:** [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\GPSDome antenna](#)

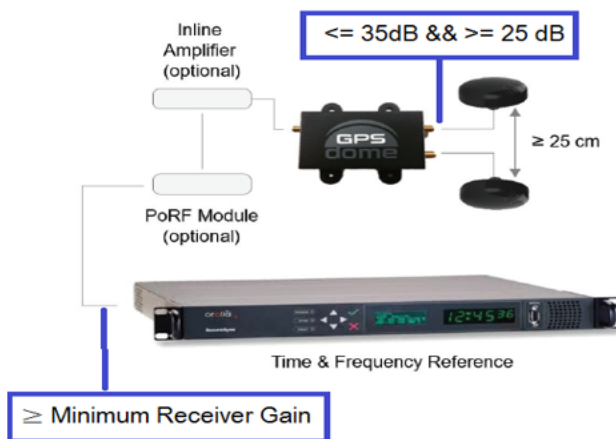
GPSdome Installation Kit

Contents:

- 6 dB attenuator (x2)
- Bias-T (PoRF)
 - Includes AC/DC PS
- Cables
 - 5ft LMR195
 - 10ft LMR400 (x2)
- Adapters
 - N-SMA 1 ft cable – PT (x3)
- Weatherproofing kit
- Installation Instructions



Installation



- Compatible with any **active** L1 GNSS antenna, with gain > 27 dB
- Both antennas must be similar
- Antennas are DC powered by GPSdome

5/2019

IMPORTANT NOTE: GPSDOME REQUIRES **TWO** GNSS Antennas (such as 8230s and/or 8230AJ antennas be connected, in order for it to work!!!

Both antennas are powered by the GPSDome.

Typical installation on time server

• PPS vs. EPS – Phantom Power Supply Vs External Power Supply

PPS receives power from the RF cable by PoRF (power over radio frequency). The EPS is fed by external power.

The operation voltage in both versions in 3.3VDC to 32 VDC

• GPSdome PPS

- GPSdome can accept max gain of 35 dB
- If using 40 dB gain antennas, you must add 5/6 dB attenuator after the antennas
- Insertion loss of GPSdome unit 6.5dB +/- 2dB. (This feature is corrected in the upcoming 1.03 product)
- Cable length + connectors
- If needed need to add inline amplifier after the GPSdome to be above the minimum receiver gain
- **PoRF – is needed with any installation, to provide the GPSdome required power.**
- Antenna Gain – Cable Loss – 1 db/ Surge Suppressor – 0.5 db/ Connector – 6dB attenuator (optional) <= 35dB && >= 25 dB – (6.5dB + 2db GPSDome) + 20 db/ Inline Amplifier ≥ Minimum Receiver Gain

• GPSDome EPS

- Same as GPSdome PPS apart from the power supply
- Need to provide the GPSdome external power between 3.3VDC to 32 VDC.

1/15/2019

Interfaces

(R) output to the GPS receiver SMA.

Primary Antenna Input (P) - 50Ω SMA 2.75VDC designed for 26dB ±2dB gain.

Auxiliary Antenna Input (A) - 50Ω SMA 2.75VDC designed for 26dB ±2dB gain.

Power Input:

Red: 3.3VDC – 32VDC (0.75W)

Black: GND

Brown: Open drain interference indication. (This wire sends an indication when the unit is detecting and protecting against a hostile signal).

GPS dome 1.02b -EPS – General view



General Operation of GPSdome/TWO status LEDs (power and interference detection indicator)

The GPS DOME module operates without manual intervention.

Two LEDs located on the GPS DOME module, provide the following indications:

- **LED 1 (Green):** When the module is powered ON and operating correctly, a green LED is steady on.
- **LED 2 (Red):** When the presence of a jamming event is detected, a red LED is steady on.

**Model 8230 and Model 8230-00 (TW3740/TW3742) GNSS Antennas



Model 8230
(Tallysman 3742-14-00)



Model 8230-00
(Tallysman 3742-14-01)



*Model 8230 GPS/GNSS
Outdoor Antenna with optional
PVC Pipe (Model 8235) and
optional Rugged Post Mount
(Model ANT-KT)*

Note: PVC pipe mast assembly is not included with Model 8230. Needs to be purchased separately (Model 8235)

Note: Initial following info is applicable to both the white and black variants of the 8230 antennas. Further below, there are two additional sections, one for each of the two variants.




Shortcuts/links

- **Shortcut to our datasheet (in SharePoint):**
<https://oroliagroup.sharepoint.com/sites/oroliasalesmarketing/Shared%20Documents/Forms/AllItems.aspx?viewpath=%2Fsites%2Foroliasalesmarketing%2FShared%20Documents%2FForms%2FAllItems%2Easpx&id=%2Fsites%2Foroliasalesmarketing%2FShared%20Documents%2FCollateral%2C%20Leaflets%20%26%20Brochures%2FSpectracom%20Datasheets%2FGPS%20Antennas%20%26%20Accessories>
- **Shortcut to Model 8230 manual (1222-5000-0050) in Arena:** https://app.bom.com/files/detail-summary?file_master_id=1235173111&file_id=1746857983
- **Shortcut to 8230 in cust service folder:** <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8230>
- **Shortcut to a document that discusses differences between Models 8230 and 8225 (on our website)**
<http://www.spectracomcorp.com/Desktopmodules/Bring2Mind/DMX/Download.aspx?EntryId=1422&PortalId=0>

Link to MFG. datasheet (TW3740/3742)

- **Models 8230 (white antenna) and 8230-00 (available black/dark gray antenna)**
Online: <https://www.tallysman.com/product/tw3742-single-band-gnss-antenna-pre-filtered/> (scroll down and select “Download datasheet”)

Comparison of Model 8230 to other Model Antennas

Model	8230	8225	ANT-35
Physical			
Frequency	1574-1606 MHz	1575.42 +/- 15 MHz	1575.42 +/- 1.023 MHz
Gain	40 dB	30 dB	35 dB typ
Out of band rejection	<1550 MHz: >50 dB >1640 MHz: >70 dB	Not specified	+/- 50 MHz: 60 dB typ
Op Temp	-40 to 85 C	-30 to 85 C	-40 to 85 C
Size	66.5 mm dia x 47.5 mm h	89 mm dia x 70mm h	90 mm dia x 98.4 mm h
Weight	140 g	191 g	285 g typ
Mounting	Through hole clamped to included L-bracket compatible with post mount and ANT-KT mount	Threaded rod with flange mounted to included post	M4 screws, compatible with ANT-KT mount

Tallysman 3742 antenna drawing

Excerpt below from: <https://www.tallysman.com/product/tw3742-single-band-gnss-antenna-pre-filtered/>

Details

Ideal for professional precision timing applications, TW3742 provides excellent circular polarized signal reception, great multi-path and out-of-band signal rejection.

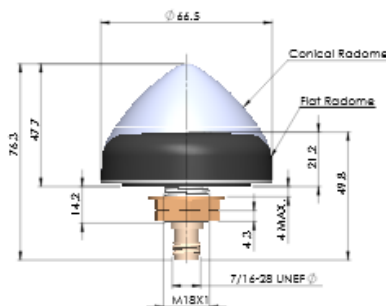
The TW3742 features a customizable dual-feed, wide-band patch element, and a 40 dB gain Low Noise Amplifier (LNA) with a high rejection out-of-band SAW filter, providing an excellent axial ratio that is constant across the full frequency, superb phase linear response and tight phase centre variation.

The TW3742 also includes an LNA pre-filter, providing enhanced protection against high level sub-harmonic signals like LTE and near frequency signals such as WiFi.

To minimize performance impact from signal jamming threats, the TW3142 is compatible with Tallysman's Anti-Jamming add-on, which modifies the radiation pattern of the GNSS antenna to eliminate signals arriving from -10° to +15° from horizon, while slightly increasing the gain of the antenna at zenith.

The TW3742 is housed in a permanent mount industrial grade weather-proof enclosure, available in conical or flat radome styles and in grey or white colours. Two options for pole mounting are available an [L-Bracket](#) or a [Pipe Mount](#).

Drawings



Model 8230/8230AJ Antenna/Cable installation information

- Refer to (earlier in this same document): [General Cabling/Antenna installation info provided to/available for customers](#)
- Refer to the **8230/8230AJ antenna installion Guide** (our P/N 1222-5000-0050) on our website at: <https://www.rolia.com/sites/default/files/document-files/8230%20GPS%20Antenna%20Install%20Guide%201222-5000-0050Rev3.pdf>

Customer inquiry about info in the Antenna install guide

Q Forwarded from Matt Mang (7 Oct 2020) what is meant by (under “**Installing the Antenna**”) the following bold “**The GPS/GNSS antenna must be installed outdoors with an unobstructed view of the sky (to 20° elevation from the horizon).**” An unobstructed line of sight to the sky allows the antenna to locate and track the maximum number of satellites throughout the day. Installations with obstructed views may still prove functional, but the equipment may experience reduced reception quality or be unable to simultaneously track the maximum number of satellites.

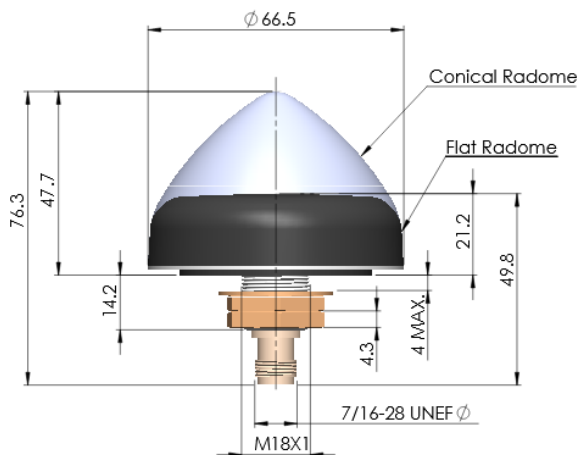
A Reply from Keith As for the elevation question, I believe this is referring to having a recommended clear view of the sky (preferably 360 degrees around it) from straight up, down to 20 degrees above the horizon. If there is a physical obstruction to one side, and the obstruction stops before getting to 20 degrees above the Horizon, it shouldn't have any impact whatsoever on the antenna being able to track the most satellites possible. The antennas/receivers don't care about GPS satellites at the horizon-level. So, a horizon-level satellite being physically blocked makes no difference. They would rather track satellites that are higher in elevation (more than 20 degrees above the horizon).

Pole Mounting of antenna (L-bracket or Pipe mount option)

Excerptst below from: <https://www.tallysman.com/product/tw3742-single-band-gnss-antenna-pre-filtered/>

The TW3742 is housed in a permanent mount industrial grade weather-proof enclosure, available in conical or flat radome styles and in grey or white colours. Two options for pole mounting are available an L-Bracket or a Pipe Mount.

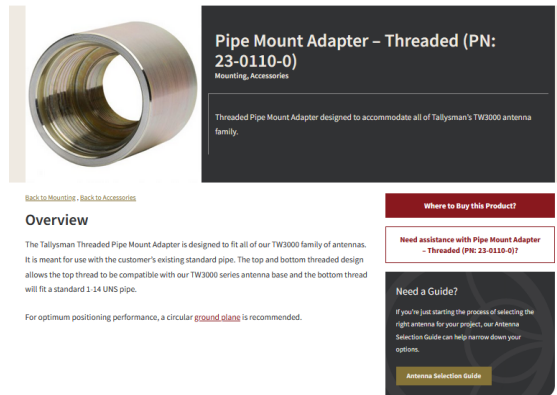
Drawings



“Pipe Mount Adapter – Threaded (PN: 23-0110-0)”



- Available from Tallysman directly (we don't currently offer it)
- top thread is compatible with TW3000 series antenna base
- the bottom thread of adapter will fit a **standard 1-14 UNS pipe**.
- Excerpt below from <https://www.tallysman.com/product/pipe-mount-adapter-threaded/>



Replacing Model 8225 with a Model 8230 antenna

- Refer to 8225 to 8230 document in: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8230>

International shipping Regulations (HTS code, ECCN Number/EAR)

- For details refer to (in this document): [Export control \(HTS and ECCN numbers\) for all products](#)

Refer to the Export Control matrix at:

- [I:\Trade Compliance\Export Control Matrix](#)
- [I:\Customer Service\Export Control-HTS and ECCN numbers](#)

For 8230s

US HTS code: 8543.70.9910

Europe HTS code: 8543.70.3000

ECCN number: 7A994

Any inorganic phosphorus material in the Model 8230?

- Refer to SF case 124460
- Refer to letter from Manufacturer: [..\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8230\inorganic Phosphorus](#)

Email from Josh to TOYO (16 Jan 18) We are pleased to inform you that we have just received confirmation from the 8230 antenna supplier that this antenna DOES NOT contain any inorganic phosphorus material.

Bracket and Antenna Drawings/PVC Mast assembly

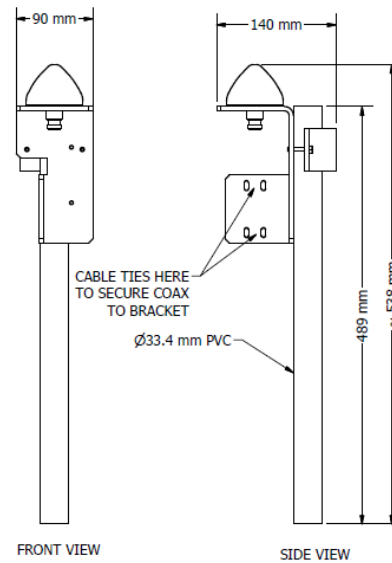
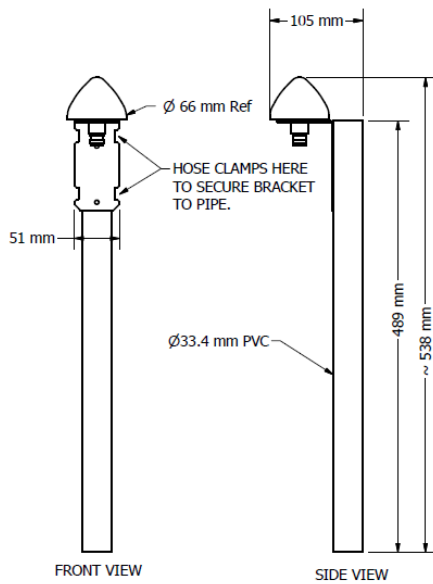
A) Antenna drawings

Refer to: [I:\Engineering\Mechanical\1222 \(GNSS Antenna\)](#) (or online at: <http://www.tallysman.com/index.php/gnss/products/antennas-gpsbeidougalileo/tw3740tw3742/> (select the "Drawings tab")

- **Model 8230 drawing** (our P/N: 1222-0001-0600):
- **L bracket** (our P/N: MP10R-0000-0004)

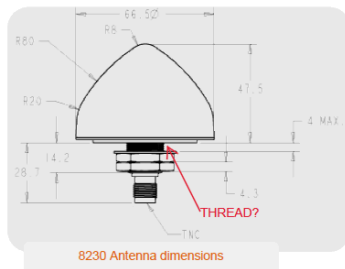
B) PVC Mast assembly/drawing

- **Mast assembly drawing** (our P/N: 1222-1000-0700): [I:\Engineering\Archive\New Released\Fabricated Part Drawings\1222-xxxx-xxxx](#)
 - Standard 1 inch "Schedule 40 PVC" (1 5/16 inch outside diameter).
 - **Pipe length:** 48.9 cm / 19.25 inches long



Thread sizes/specifications

Q Could you advise the thread specification please? I would like to thread the antenna directly into a housing with a tapped mounting hole.



A from the Tallysman datasheet: https://www.tallysman.com/wp-content/uploads/TW3470_TW3472_Datasheet_rev5_5.pdf **M18x1 thread**

Mechanicals & Environmental

Mechanical Size	66.5 mm dia. x 21 mm H
Operating Temp. Range	-40 to +85 °C
Enclosure	Radome: EXL9330, Base: Zamak White Metal (M18x1thread)

Model 8230 mounting bracket dimensions

- Refer to (excerpt below):
<https://files.bom.com/download/L1yTquFdbg2iMIFANtSgwUkGQgUIwkNY/sqvyafohozhmmjbvpvjutypoysgjrku/8230%20GPS%20Antenna%20Install%20Guide%201222-5000-0050Rev3.pdf>

Technical drawing of the L-Bracket showing three views: front, top, and side. The front view shows a bracket with a vertical leg of 50mm and a horizontal leg of 40.7mm. The top view shows a rectangular base with dimensions 110mm by 50mm, with four mounting holes. The side view shows the bracket's profile with a 90-degree bend. Dimensions are given in millimeters.

➤ Per the TW3740/TW3742 datasheet: “The TW3740 / TW3742 is a precision high gain GNSS antenna covering the BeiDou B1, Galileo E1, GPS L1, GLONASS L1 and SBAS (WAAS, EGNOS, QZSS & MSAS) frequency band (1557 to 1606 MHz).”

- GPS L1
- GLONASS L1
- BeiDou B1
- Galileo E1
- QZSS L1

<http://www.tallysman.com/gnss-antennas.php>

Gyles Panther
gyles.panther@tallysman.com

GPS antennas are Receive-only (they do not transmit any info)

- For documentation of this fact, refer to "SecureSync_onclassifiednetwork"
doc: <..\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\GPS\GPS is receive-only>

Q We currently have a 8230 Outdoor antenna installed and connected to a Spectracom SecureSync time receiver. Our client is concerned about information being transmitted over the antenna. I see plenty of information on the receiving specifications of the antenna, but I cannot find anything in the data sheet that actually states the antenna is receive only and does not transmit. Is this a correct statement and if so where could I find it in writing to show the client?

A: **Reply from Jodi:** The answer is No, the antenna does not transmit. I've attached a PDF for your reference, which shows that the antenna is Receive-Only.

Response from Keith to a customer (Case **284720**)

I can confirm for you that the SecureSync's Model 8230 GNSS antenna DOES NOT transmit ANY data!! The Model 8230 is a receive-only antenna with no capabilities to transmit any signals.

Your understanding is completely correct! The Model 8230 sends one-way raw GNSS satellite frequencies down to a GNSS receiver board installed inside the SecureSync. The GNSS receiver ONLY outputs to its antenna 5vdc, which is used to power the amplifier in its antenna. Besides this 5vdc operating voltage, the receiver sends nothing else (such as position data) up to its Model 8230 antenna. The internal GNSS receiver obtains /processes the raw GNSS signals from its antenna to calculate position and timing for use within the SecureSync.

Position data from the receiver can optionally be obtained from the SecureSync itself, via its front panel LCD and/or available ethernet connections. But as mentioned above, none of this information is even able to be passed back up its antenna cable to the Model 8230 antenna. And even if the receiver board in the SecureSync could send data back up to its antenna, the antenna itself still couldn't transmit it out, since the Model 8230 is a receive-only antenna (it doesn't have any transmit capabilities).

MTBF for Model 8230

- Refer to (in this doc): [MTBF/MTTR \(for all products\)](#)

A) Model 8230 (standard/white antenna) and accessories (our P/N 1222-0001-0600)



Model 8230
(Tallysman P/N: 3742-14-01)

- White GNSS replacement of the Model 8225 GPS antenna
- Model 8230 antenna started shipping 27 Sept 2013 (cut-in ECN 3243)
- Operates with GPS (L1 Band only) and Glonass (L1 band)

Part Numbers for 8230 antennas

- **P/N for just the raw antenna head (no manual, tie wraps or L bracket):** **E025R-0001-0011**
(in Arena) https://app.bom.com/items/detail-spec-redline?item_id=1218841868&version_id=10498638628&&redirect_seqno=11303803830
- **P/N for complete Model 8230 antenna (includes manual / cable ties / L bracket):** **1222-0001-0600**
(in Arena): https://app.bom.com/items/detail-spec?item_id=1202847121&version_id=10498638618&orb_msg_single_search_p=1
(in Salesforce): <https://orolia.my.salesforce.com/01tC00000003loQo?srPos=0&srKp=01t>

Tallysman MFG. Model Number: TW3742

MFG. P/N: 33-3742-14-01

Per Dave Lorah (Oct, 2017) We order the part number **33-3742-14-01** from Tallysman

Model 8230 Antenna specs

TW3470/TW3472 GPS/GLONASS Timing Antenna Specifications

Antenna	
Architecture	Dual, Quadrature Feeds
1 dB Bandwidth	32 MHz
Antenna Gain (with 100mm ground plane)	4.25 dBi
Axial Ratio (over full bandwidth)	1 dB typ, 3 dB max.
Electrical	
Architecture	One LNA per feed line -> SAW filter -> 2-Stage LNA
Filtered LNA Frequency Bandwidth	1574 to 1606 MHz
Polarization	RHCP
LNA Gain	40 dB min., 1575.42 to 1606 MHz
Gain flatness	+/- 2 dB, 1575 to 1605 MHz
Out-of-Band Rejection	<1500 MHz: >32 dB (TW3470) >50dB (TW3472) <1550 MHz: >25 dB >1640 MHz: >35 dB >70dB
VSWR (at LNA output)	<1.5:1
Noise Figure	1 dB typ. TW3470 3.5dB typ. TW3472
Supply Voltage Range (over coaxial cable)	2.5 to 10 VDC nominal
Supply Current	21 mA typ.
ESD Circuit Protection	15 KV air discharge
Mechanicals & Environmental	
Mechanical Size	66.5 mm dia. x 47.5 mm H
Connectors	TNC Jack (female).
Operating Temp. Range	-40 to +85 °C
Enclosure	Radome: ASA Plastic, Base: Zamak White Metal
Weight	140 g
Attachment Method	Permanent 3/4" (19mm) through-hole mount
Environmental	IP67 and RoHS compliant
Shock	Vertical axis: 50 G, other axes: 30 G
Vibration	3 axis, sweep - 15 min, 10 to 200 Hz sweep: 3 G
Warranty	One year, parts and labour
Ordering Information	
TW3430 - Dark gray radome, TNC connector	32-3470-0-00
TW3430 - white radome, TNC connector	32-3470-0-01
TW3432 - Dark gray radome, TNC connector	32-3472-0-00
TW3432 - white radome, TNC connector	32-3472-0-01
Please contact Tallysman Wireless for additional information	
Tallysman Wireless Inc	

- Gain: **40dB gain typical**
- Power requirements: 5vdc antenna (**accepts 2.5 to 16vdc, 19ma typ**)
- power draw of 8230 antenna is **19 mA**
- Noise Figure of 8230 antenna is **1dB typical**
- **Max cable distance** (using RF400 / RG-8 cable)- **400** feet with no Model 8227. **800** ft with 8227 inline
- Recommend connector be weather-proofed (Our Weather-proofing kit P/N: 1142-0000-5001)
- **Mounting:** ¾ inch (19mm) though hole for (N connector) or L bracket.

Any inorganic phosphorus material in the Model 8230?

- Refer to SF case 124460
- Refer to letter from Manufacturer: <..\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8230\inorganic Phosphorus>

Email from Josh to TOYO (16 Jan 18) We are pleased to inform you that we have just received confirmation from the 8230 antenna supplier that this antenna DOES NOT contain any inorganic phosphorus material.

Plastic enclosure UV-light, water exposure/immersion

- Refer to Salesforce Case 243304

Reply from Dave L (10 Sept 2020) The antenna materials are designed to withstand the outdoor environment where the antennas are deployed.

According to the attached data sheet from Tallysman the manufacturer, the plastic used is a EXL9330 copolymer.

LEXAN™ Resin EXL9330 is an opaque, amorphous PC-Siloxane copolymer. Is a UV stabilized, non-bromine, non-chlorine flame retardant (UL94 f1/V-0/5VA) grade offering highly stable mechanical, electrical, optical and thermal properties. Exhibits good impact resistance, outstanding dimensional stability and clarity. Processed by injection molding and suitable for ECO conforming applications.

UV-light, water exposure/immersion F1 - UL 746C

According to this online data sheet from Sabc:

<https://www.picoplast.nl/uploads/77632630bebc2067456d3523346e26c8Lexan%20EXL9330%20-%20MDS%20-%20EN.pdf>

I am not a materials engineer either, but hopefully these specs will satisfy your requirements.

Follow-up question from same customer above (10 Sept 2020) One question to ask (because I'm sure the customer is going to ask me): The Spectracom data sheet for the antenna which we advertised to the customer for the antenna refers to the radome as "ASA plastic". Does that relate to the EXL9330 copolymer listed in the Tallysman datasheet? From what I've read, they are two different things.

My gut feeling is that the Spectracom datasheet was either inaccurate or simply outdated on referencing ASA.

If that is the case, I can work with that with my customer. Just want to see if you have any additional explanation on the discrepancy.

Shock/vibe specs

- Refer to "**Mechanicals & Environmental**" section of the Tallysman Data sheet (as excerpted below):
<I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8230>

Environmental	IP67 and RoHS compliant
Shock	Vertical axis: 50 G, other axes: 30 G
Vibration	3 axis, sweep = 15 min, 10 to 200 Hz sweep: 3 G

MIL-STD-810: IP rating (Humidity specs/water penetration)

- Data sheet indicates it meets milspec MIL-STD-810
 - This Standard is located in [I:\Engineering\Specs and Standards\MIL \(Military Specs\)\MIL-STD](I:\Engineering\Specs and Standards\MIL (Military Specs)\MIL-STD)
 - Info on this Standard: <https://en.wikipedia.org/wiki/MIL-STD-810>

Test Method 506.5: Rain

Acceptable water penetration: water penetration of not more than 4 cm³ per 28,000 cm³ (1 ft³) of test item enclosure provided the following conditions are met:

- (1) There is no immediate effect of the water on the operation of the materiel.
- (2) The test item in its operational configuration (transit/storage case open or removed) can successfully complete the aggravated temperature/humidity procedure of Method 507.5.

Test Method 507.5: Humidity

Test Method 520.3 Temperature, Humidity, Vibration, and Altitude

- IP Rating for 8230: **IP67**
 - Refer to (in this document for breakdown of IP values: [IP rating/Ingress rating \(for all products\)](#))
 - Refer to "**Mechanicals & Environmental**" section of the Tallysman Data sheet (as excerpted below):
<I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8230>

Environmental	IP67 and RoHS compliant
---------------	-------------------------

From Salesforce case 25024:

Q Which of the following requirements does the GPS antenna meet or doesn't meet?

- fully operational when relative humidity is from 20 percent to 100 percent non-condensing.
- fully operational when rainfall rates are 30 mm/h or less for over a period of one hour.
- perform optimally when dust and sand are present with a diameter of greater than 0.5 mm to a concentration of not less than 180 mg/m².

A (slightly modified) Reply from Tom Richardson (12 Apr 17) This has come up frequently lately.

There is no spec for humidity.

The antenna meets IP67 for Ingress Protection.

- The “6” in “IP67” is for solid particle protection and it means the antenna is dust tight, no ingress of dust; complete protection against contact (dust tight).
- The “7” in “IP67” is for liquid protection and it means the antenna can withstand immersion in water up to 1 meter in depth for at least ½ an hour. Since it is water tight, no humidity would get inside it.

From Allen Crawford at Tallysman,

The TW3742(8230) is operational around the World in a wide variety of climates, including harsh environments with wide fluctuations in temperature and humidity. We have not had any reports of failures due to the type of exposure described by your customer.

The antenna will not survive 100% humidity inside the enclosure (which means the antenna is full of water with no air inside). The only way the inside of the enclosure will encounter 100% humidity is if it is immersed in water to a depth greater than 1m for a period of time. In short, the antenna can and does survive extended periods of rainfall (such as has occurred recently in California) without any water intrusion.

The enclosure is designed and has been tested to meet IP67 standards which means the antenna can survive immersion in water to a depth of 1m for 30 minutes. The pressure at this depth is approximately 10% higher than normal air pressure. There is no reason to expect water intrusion in the antenna enclosure at normal air pressures and 100% humidity for extended periods of time.

I would say it would meet all the requirements listed below. (referring to the customer inquiry above)

BTW the warranty is 1 year.

Email Keith sent to Josh (28 Mar 17) Attached is a copy of the Manufacturers data sheet for the Model 8230 antenna.

This antenna is outdoor-rated and sealed to keep out moisture. So, though the data sheet (not unexpectedly) doesn't mention humidity, its assumed that it can be used in up to 100% humidity ☺!! (humidity specs normally apply to items not rated for outdoor use and aren't completely sealed ☺)

B) Model 8230-00 (black/dark grey antenna)



Model 8230-00 (Tallysman P/N 3742-14-01)

Info about the Model 8230-00 (available black/dark grey antenna) P/N: 1222-0003-0600

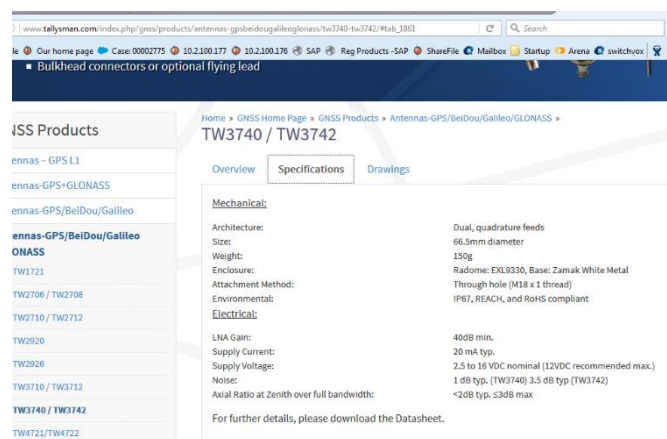
- Black (Dark Grey) GNSS replacement of the Model 8225 GPS antenna
- Model 8230-00 antenna was released on ECO 1161, Feb 2017 (in Arena): https://app.bom.com/changes/detail-summary?change_id=2387715485&
- Operates with GPS (L1 Band only) and Glonass (L1 band)
 - From the MFG data sheet: “covering BeiDou B1, Galileo E1, GPS L1, GLONASS L1 and SBAS (WAAS, EGNOS, QZSS & MSAS) frequency band (1557 to 1606 MHz)”

Associated Part Numbers/ Model Numbers for 8230-00 (black/dark grey antenna)

- **Spectracom P/N for the full kit** (black/grey antenna, bracket, two clamps and manual): 1222-0003-0600 (for comparison, the white Model 8230's P/N is 1222-0001-0600)
- **Spectracom P/N for just the black/grey antenna (no bracket, clamps. manual):** E025R-0001-0012 (In Arena) https://app.bom.com/items/detail-sourcing?item_id=1230481115&version_id=10694854138
- **Tallysman MFG. Model Number for just the black/grey antenna:** TW3742-14-01
MFG. P/N or just the black/grey antenna 32-3472-01-01

Model 8230-00 (Black/grey) Antenna specs

- Refer also to specs in 8230 (white antenna) further above.



- **Input DC voltage:** 2.5 to 16vdc (supply current 19mA typ)
- **Gain:** 40dB gain

- **Power requirements:** 5vdc antenna (accepts 2.5 to 16vdc w/12vdc recommended max, 19ma)
- Max cable distance (using RF400 / RG-8 cable)- **400** feet with no Model 8227. **800** ft with 8227 inline
- Recommend connector be weather-proofed (**Our Weather-proofing kit P/N: 1142-0000-5001**)
- **Mounting:** ¾ inch (19mm) though hole for (N connector) or L bracket.
- **IP Rating:** IP67 [IP rating/Ingress rating \(for all products\)](#)

IP67

Protected from total dust ingress.

Protected from immersion between 15 centimeters and 1 meter in depth.

Items included with purchase of either Model 8230 or 8230-00 antenna (P/N for the full kit: 1222-0001-0600)

Note: Kit does not include PVC mast assembly, which is purchased separately (Model 8235 Kit, P/N 1222-0002-0600)



1. (1) Model 8230 antenna (Our P/N: 1222-0001-0600)
2. (1) L bracket (Our P/N: MP10R-0000-0004)
3. (2) Hose clamps (Our P/N: MP05-0005-0036)
4. (2) Cable ties (Our P/N: MP00002)

Additional items that can be optionally purchased with Models 8230 and 8230-00 antenna (more info on these items further below)

Additional Accessories

2. Flat Roof Antenna Mount: Model 8213
3. GPS Antenna Splitter: Model 8224
4. Antenna Surge Suppressor: Model 8226
5. Surge Protector Grounding Kit: Part Number 8226-0002-0600
6. Inline Preamplifier: Model 8227
7. Low Loss Antenna Cable: Contact factory
8. Indoor Plenum-rated Antenna Cable, CMP equivalent: Contact factory
9. Connector Interface Weather-Proofing Kit: Part Number 1142-0000-5001
10. PVC Pipe with Hose Clamps: 33.4 mm dia. x 489 mm long (1.32" dia. x 19.25" long): Model 8235
11. Rugged Post Mount: Model ANT-KT

1. **Model 8213 flat-roof mount (weighted base/stand)**



2. Model 8235 Kit. P/N 1222-0002-0600 (optional PVC pipe and two hose clamps)

- **Our P/N for the two provided metal hose clamps in this kit:** MP08452.
- **PVC pipe diameter:** Standard 1 inch “Schedule 40 PVC” (1 5/16 inch outside diameter).
 - **Pipe length:** 48.9 cm / 19.25 inches long

3. Model Ant-KT (aluminum Rugged post-mount bracket)

Model 8230 Declaration of Conformity / Certificate of Compliance

- The Vendor’s (Tallysman) Certificate of Compliance: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8230\Rohs-Certificate of Conformity>
- Refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Declaration of Conformity>

Note: The Declaration of Conformity for the Model 8230 antenna is included in the SecureSync’s Declaration of Conformity Certificate.

Per Dave Sohn (15 Jun 15): it includes EN 60950-1:2006/A11:2009 for safety. We don’t test to EN61000-6-1:2007 or EN 61000-6-3:2007, instead testing against EN 55022:2006/A1:2007 for Class A emissions, and EN55024:1998/A2:2003 for immunity.

FCC Part 15 compliancy/certification

- Model 8230 has been tested / certified compliant with FCC part 15
- Refer to/send “Tallysman TW3470...” **Certificate of Compliance:** <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8230\Rohs-Certificate of Conformity>

Certificate of Compliance	
Customer :	Spectracom Corp.
Date:	2 Oct 13
Part Number :	32-3472-X
Applicable Specifications	
RoHS and REACH Compliant	
IPC-A-610 Class II Compliant	
32-3472-X Datasheet Rev 4.1	
FCC Part 15 Subpart B and ICE-003 for Radiated and Conducted Emissions	
CE Marked	

ESD sensitivity for the Model 8230 antennas

- Contains ESD circuit protection
- From page 2 of the Tallysman data sheet below (see yellow highlight)



Part Numbers for Models 8230 (white antenna) and 8230-00 (dark grey/black antenna)

Weather-proofing kit: 1142-0000-5001 (for either Model 8230 or 8230-00)

- Refer to: <https://na8.salesforce.com/01t800000002Axan?srPos=0&srKp=01t>

A) Model 8230 (white GNSS antenna)

1222-0001-0600 (Model 8230 antenna, bracket, etc)

Note: This is the P/N to sign-out for warranty replacement antennas. The included manual discusses how to attach the Model 8230 to the 8225/8230 mast assembly.

Note: PVC pipe mast assembly is not included with Model 8230. Needs to be purchased separately (Model 8235)

➔M 1222-0001-0600/A - 1222-0001-0600 - 8230 Antenna	1.0000 -
10 KITTING -	
10 1222-5000-0050 - 8230 Manual	1.0000 Qty Reqd
20 E025R-0001-0007 - Antenna, GPS-GLONASS, 40dB, 3 Filter	1.0000 Qty Reqd
30 MP00002 - CABLE TIE, 8in, RoHS compliant	2.0000 Qty Reqd
40 MP05R-0006-0036 - CLAMP, HOSE, SS, #36, 1.75in - 2.75in	2.0000 Qty Reqd
50 MP10R-0000-0004 - Bracket, L	1.0000 Qty Reqd

1222-0002-0600 Model 8235 Mounting kit (hose clamp and mast only- not the antenna)

➔M 1222-0002-0600/A - 1222-0002-0600 - 8235 Kit, Antenna, Mount	1.0000 -
10 KITTING -	
10 1222-1000-0700 - Mast, Antenna, 489 mm	1.0000 Qty Reqd
20 MP08452 - HOSE CLAMP, 2in to 6in	2.0000 Qty Reqd

1222-0003-0600 Model 8238 Antenna and mounting kit (includes Models 8230 and 8235) (**Note:** Model 8238 was intended and started to be released but was then cancelled)

➔M 1222-0003-0600/A - 1222-0003-0600 - 8238 Kit, Antenna and Mount	1.0000 -
10 KITTING -	
10 1222-1000-0700 - Mast, Antenna, 489 mm	1.0000 Qty Reqd
20 1222-5000-0050 - 8230 Manual	1.0000 Qty Reqd
30 E025R-0001-0007 - Antenna, GPS-GLONASS, 40dB, 3 Filter	1.0000 Qty Reqd
40 MP00002 - CABLE TIE, 8in, RoHS compliant	2.0000 Qty Reqd
50 MP05R-0006-0036 - CLAMP, HOSE, SS, #36, 1.75in - 2.75in	2.0000 Qty Reqd
60 MP08452 - HOSE CLAMP, 2in to 6in	2.0000 Qty Reqd
70 MP10R-0000-0004 - Bracket, L	1.0000 Qty Reqd

B) Model 8230-00 (dark grey/black GNSS antenna)

- Just the antenna by itself: **E025R-0001-0012** (In Arena) https://app.bom.com/items/detail-sourcing?item_id=1230481115&version_id=10694854138
- **1222-0003-0600** (Model 8230-00 antenna, bracket, etc) (in Arena) https://app.bom.com/items/detail-bom?item_id=1230481023&version_id=10694852168

Note: PVC pipe mast assembly is not included with Model 8230. Needs to be purchased separately (Model 8235)

Contains 6 first-level Items, 6 line Items, 6 unique Items, 0 of which are shared.		
#	Item Number	Item Name
1	1222-1006-0801 rev 1	8230 Kit, Dark Grey, Label
2	1222-5000-0050 rev 2	8230 Antenna Installation Guide
3	E025R-0001-0012 rev 1	Hi-Gain Multi-Constellation GNSS Antenna, Dark Grey
4	MP00002 rev 3	CABLE TIE, 8in, RoHS compliant, weather resistant
5	MP05R-0006-0036 rev 1	CLAMP, HOSE, SS, #36, 1.75in - 2.75in
6	MP10R-0000-0004 rev 1	Bracket, L

1222-0002-0600 Model 8235 Mounting kit (hose clamp and mast only- not the antenna)

M 1222-0002-0600/A - 1222-0002-0600 - 8235 Kit, Antenna, Mount	1.0000 -
10 KITTING -	
10 1222-1000-0700 - Mast, Antenna, 489 mm	1.0000 Qty Req'd
20 MP08452 - HOSE CLAMP, 2in to 6in	2.0000 Qty Req'd

Other Model 8230 antenna Specs

Note: The document referred to in the email from Tom R below is “**3845-Tallsman Wireless Inc REPORT.pdf**” located in: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8230>

Email from Tom Richardson to Spectracom France: Quite a while ago you guys asked about the compliance of the antenna with the following. For Aselsan I believe.

The attached and following is the response I finally got from the manufacturer. I hope it helps. I don't think it answers the question as to whether the antenna meets what I assume are MIL-STD requirements but it might meet something comparable...

STORAGE TEMPERATURE		OPERATING TEMPERATURE		MOISTURE	RAIN	COROSION
+ 60 °C Method 501.4 Procedure I	- 30°C Method 502.4 Procedure I	+ 50 °C Method 501.4 Procedure II	-30 °C Method 502.4 Procedure II	% 90 relative ATMOSPHERIC MOISTURE (noncondensing)	Rain Fall rate max 1.7mm/min Method 506.4 Procedure I	MIL-STD-1250A
SAND AND DUST		VIBRATION		MECHANICAL SHOCK	ICING	FUNGUS
MIL-STD-810f-Method 510.4 Procedure 1		Method 514.5 (non-functional) category 20		20G, 11ms	Ice thickness: 6mm Method 521.2 Procedure I	Method 508.5
						SOLAR RADIATION Method 505.4 (Procedure -I) 49°C, 1120W/m2

Wind resistance: Per Scott Holmes (29 Apr 15) wind load will also be 150MPH for this antenna.

Note: Additional info on wind resistance is in the “antenna install” section further above

Impedance of antenna by itself: 5.6Mohms: will look like an open on the cable

Comparison of a Model 8230 or 8225 antenna to a Model ANT-35 antenna (“Epsilon antenna”)

- Refer to: [Comparison of a Model ANT-35 to a Model 8230](#) (in the “ANT-35” section of this document)

Model 8230AJ (Anti-Jam GNSS antenna) (Horizon Blocking antenna)



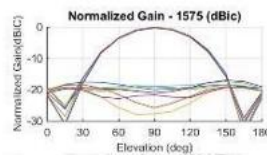
(Tallysman 3742AJ-14-G)

- Introduced with ECO 1430, 4 Dec 2017 (in Arena): https://app.bom.com/changes/detail-summary?change_id=2390440049
- Anti-Jam antenna
- 40 dB Gain GNSS antenna

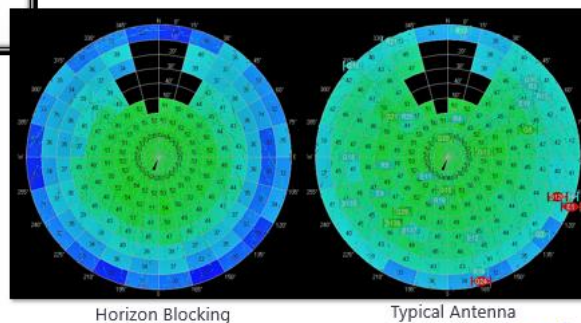
Shortcuts/links

- **Model 8230AJ and install items** (P/N 1222-0004-0600) in Salesforce: <https://orolia.my.salesforce.com/01t0h000004XLrC?srPos=0&srKp=01t>
- **8230AJ datasheet** (on our website): https://www.orolia.com/sites/default/files/document-files/Orolia_8230AJ_GPS-GNSS_Outdoor_Antenna_revC_0.pdf
- **Model 8230 Install Guide** (1222-5000-0050) in Arena (https://app.bom.com/items/detail-spec?item_id=1202835947&version_id=10221286288)
- **test data/cert of conformance/misc docs**: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8230AJ>

HORIZON BLOCKING ANTENNA



- Attenuation at the horizon where most interference comes from
- Low cost
- Suitable for timing and stationary applications

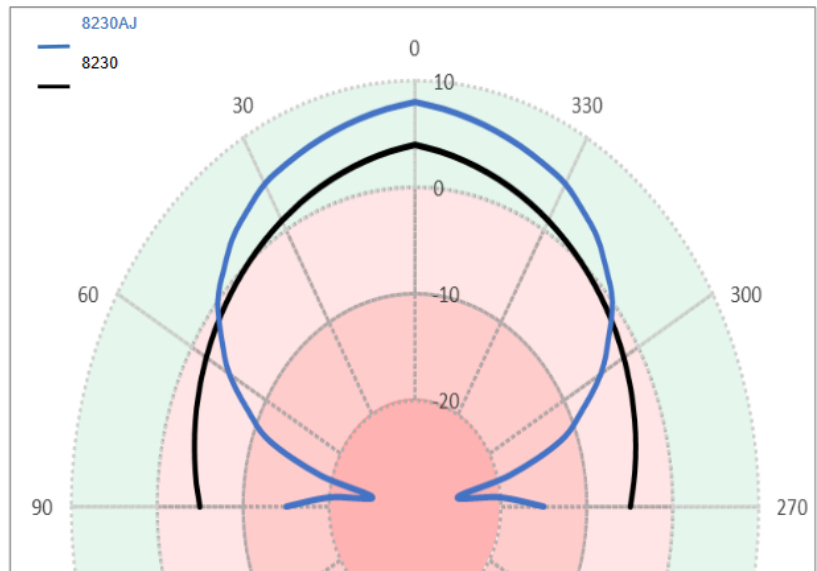


Horizon Blocking

Typical Antenna

Simple Horizon Blocking Antenna – 8230AJ

Radiation Pattern (RHCP)



- Standard 8230 antenna pattern is hemispherical – covers full sky [black line]
- 8230 AJ pattern has nulls near the horizon (less than 30° elevation) [blue line]
- Most interference comes from the ground (low elevation angles) and therefore is blocked.

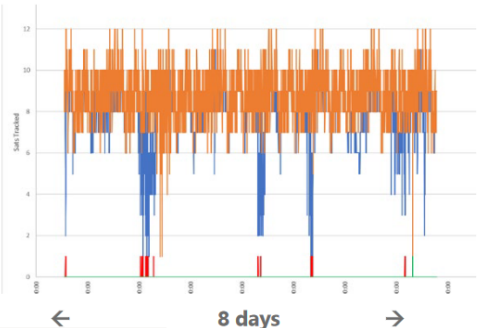
Resilient Timekeeping for Critical Infrastructure | 2020



EXAMPLE: SIMPLE AJ ANTENNA FIELD TEST FOR TIMING APP

- Two GNSS Time Servers with internal Rb Holdover oscillators: side by side, one with Standard the other with AJ Antenna
- Experiencing suspected “Privacy Jammer” interference – next to a trucking company
- AJ Antenna drastically reduced GNSS dropout (Holdover Events) over a one-week period

	Standard Antenna	AJ Conical Antenna
Holdover events	40	4
Total time in Holdover	1 hour 32 minutes	41 seconds
Longest holdover event	14 minutes 26 seconds	17 seconds
Average holdover event	2 minutes 18 seconds	10 seconds
Satellite alarms	31	2



Resilient Timekeeping for Critical Infrastructure | 2020 orolia

Released/made available: ~ 12 Jan 2018

Resistance with ohm meter is similar to 8230 approx 5.6 M ohms

Warranty: 1 year

Description: GPS/GNSS Anti Jam Outdoor Antenna supporting GPS L1, GLONASS L1, BeiDou B1, Galileo E1, and QZSS L1, with L-bracket for vent pipe/pole mounting via metal straps (included). Compatible with CA01-0N0N, CAL7XXX or CALP7XXX cables.

MFG/Part Numbers

- **MFG/MFG P/N:** Tallysman [33-3742AJ-14-01](#) (click for shortcut to datasheet in Arena)
- **Our P/N for just the Model 8230AJ antenna itself:** [E025R-0001-0013](#) (in Arena)
https://app.bom.com/items/detail-spec?item_id=1244560953&version_id=10929298648&orb_msg_single_search_p=1
- **Our P/N for the antenna kit,** (including: L bracket two hose clamps, two tie wraps): 1222-0004-0600

Certificate of Compliance (RoHS and Reach, IPC-A-610, FCC part 15)

- **Refer to CoC document :** [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8230AJ](#)

Declaration of Conformity/MIL-STD-810

- Refer to Tallysman Declaration doc: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8230AJ](#)

8230AJ Specs

The Model 8230AJ is an active GPS/GNSS antenna covering the following bands:

- GPS L1
- GLONASS L1
- Beidou B1
- Galileo E1
- QZSS L1

The active antenna circuitry provides 40dB of gain and requires 2.5 to 16 V_{DC} at 21 milliamps (provided by a Spectracom receiver over the antenna cable) to operate.

GPS Antenna Specifications

Electrical

Type: Active

Frequency: 1559 to 1606 MHz

Out-of-Band Rejection:

- < 1500 MHz: > 50 dB
- > 1650 MHz: > 50 dB

Gain: 40 dB from internal LNA

Antenna Pattern: 0 dB at zenith

15 dB or more rejection at < 30 degrees elevation

Connector: N type, female

Recommended Cable: Low Loss LMR-400 Equivalent

Maximum Cable Length: 125 meters (400 ft.) maximum with most Orolia equipment and LMR-400 equivalent cable;

250 meters (800 ft.) maximum with Inline Amplifier - Model 8227

Power: 2.5 to 16 Volts, 19 milliamps (typical), powered by receiver

Mechanical

Size: 100 mm dia. (3.9");

101.5 mm H (4") from base to top;

127.2 mm H (5") including "N" connector

Enclosure: Radome: High Temperature UV Resistant Polycarbonate;

Base: Zamak White Metal

Weight: 370g (13.1oz)

Compliance: IP67 and RoHS

Temperature Range: -40° to +85° C (-40° to +185° F)

Mounting: L-bracket (included) for vent pipe/pole mounting via hose clamps (included), PVC pipe sold separately

Warranty

1-Year Limited¹

¹The warranty period may be dependent on country.

8230AJ Environmental: IP67, REACH, and RoHS compliant

- For Reach report, refer to: <..\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8230\Reach Declaration>

Electrical:

Freq range: 1559 to 1606 MHz

LNA Gain: 40dB min.

Supply Current: 19 mA typ.

Supply Voltage: 2.5 to 16 VDC nominal (12VDC recommended max.)

Noise: 1 dB typ.

Axial Ratio at Zenith over full bandwidth: <2dB typ. ≤3dB max

Dimensions and drawings

- Refer to 8230 Install Guide (1222-5000-0050) in Arena (https://app.bom.com/items/detail-spec?item_id=1202835947&version_id=10221286288)

Maritime environment/shipborne use of the 8230AJ

Questions from John Fischer about 8230AJ/replies from Tom Richardson (Jan, 2019)

Q From John Fischer: We are looking into using this antenna aboard ships, so we asked our friends at Portsmouth to look at this suitability, and they can back with some issues. However, the 3 items below could be issues for any of our installations. I've included my question in Violet after each item.

A Email from Tom Richardson We may have some conflicting technical requirements between land installation and maritime installation.

What maritime technical standards were they referring to?
I haven't seen DC isolation as a requirement, but it is probably valid.
I would get Tallysman involved for a quote on re-design of the antenna to specific requirements.
I attach data sheets and cert for reference.

From: John Fischer <john.fischer@orolia.com>

Sent: Thursday, January 10, 2019 5:14 PM

To: Tom Richardson <tom.richardson@orolia.com>; Keith Wing <keith.wing@orolia.com>

Cc: David Sohn <david.sohn@orolia.com>; Lisa Perdue <lisa.perdue@orolia.com>

Subject: Potential issues with the 8230AJ antenna

- Base plate (and fixings) are electrically connected to the RF connector outer. 100% DC (power) isolation between the antenna metal parts ships metal structure is demanded by maritime technical standards. Failure mode grounding out of an active DC path by the fixing bracket even on the DC negative rail will typically cause the vessels grounding (earth) fault monitoring system to trip out.
Maybe we could mitigate the lack of DC isolation by adding a plastic tube sleeve into bracket fitting kit but that will need further investigation.

Is DC isolation ever a requirement for our installations? We have that requirement sometimes on our chassis products. I am not familiar with maritime requirements but the 8230AJ antenna is an active antenna that needs power from the receiver. The power in our product has chassis ground connected to DC supply negative. We would have to re-design for isolated power. Then isolate from ships chassis. I would also question the surge arrestor installation requirements.

- With soft alloy metal (Zamak) metal base plate in combination with the Stainless-steel ring fixing screws may not prove the best combination overtime in marine environment. The screws will erode into the metal alloy plate (resulting in white dust). That not to say its not well made, each of the screws has an isolation washer and is with silicone grease applied which is good and should slow the aging in an extreme marine environment.

I think this could be an issue. I know in the past, we would use marine qualified antennas even for our fixed site installations just because of the corrosion issues. Salt spray is an issue even on coastal installations. I'm surprised this one isn't all stainless. Does the standard Tallysman antenna have this problem too?

Standard 8230 antenna is the same material.

- I am not finding any proof of EU CE or FCC compliance labelling on the product or in the data sheet. It has an active amplifier component, minimum it needs is an EU complaint manufactures CE label (with declaration behind it) and probably an FCC statement.

They may be dealing with an Engineering prototype and not a production unit, but I will verify. But we do get CE Mark/FCC on all our products, including antennas, yes? Does our standard Tallysman antenna have CE Mark?

8230AJ has FCC and ICE certification but not CE emissions. The only CE part of the cert is for material, RoHS and REACH. I don't know what part of CE EMI it would comply with.

Model 8230 (Tallysman P/N TW3470/TW3472) (discontinued ???)

Antenna, GPS-GLONASS, 40dB, 3 Filter

Tallysman P/N 32-3472-01-01

In Arena: https://app.bom.com/supplier-items/detail-spec?item_id=1205134746

<http://www.tallysman.com/index.php/gnss/products/antennas-gpsglonass/tw3470-tw3472/>

****Model 8225 GPS antennas (prior to ~Dec 2013)**

Shortcut to manual (8225-5000-0050): <I:\New Released\Manuals\8225-xxxx-xxxx>

Note about the manual when the order ships: Since we started to send product manuals on CD, we still continue to send a paper copy manual with the antenna (the Model 8225 antenna manual is not on the manual CD)

Shortcut to our data sheet: [I:\Marketing\ Product Data Sheets \(archive\)](I:\Marketing\ Product Data Sheets (archive))

[I:\Marketing\ Product Data Sheets \(archive\)\GPS Antennas & Accessories](I:\Marketing\ Product Data Sheets (archive)\GPS Antennas & Accessories)

Shortcut to Model 8225 in Customer Service: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230_8225, 8225S, 8226, 8227 and grounding kit

Shortcut to Manufacturer's Data Sheets: <I:\Engineering\Engineering Shared\Spectracom parts\081030 - 8225 antenna>

Model 8225 Declaration of Conformity

- Refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Declaration of Conformity>

Note: The Declaration of Conformity for the Model 8225 antenna is included in the SecureSync's Declaration of Conformity Certificate.

Per Dave Sohn (15 Jun 15): it includes EN 60950-1:2006/A11:2009 for safety. We don't test to EN61000-6-1:2007 or EN 61000-6-3:2007, instead testing against EN 55022:2006/A1:2007 for Class A emissions, and EN55024:1998/A2:2003 for immunity.

Replaced by Model 8230 GNSS antenna = Model 8230 antennas started shipping 27 Sept 2013

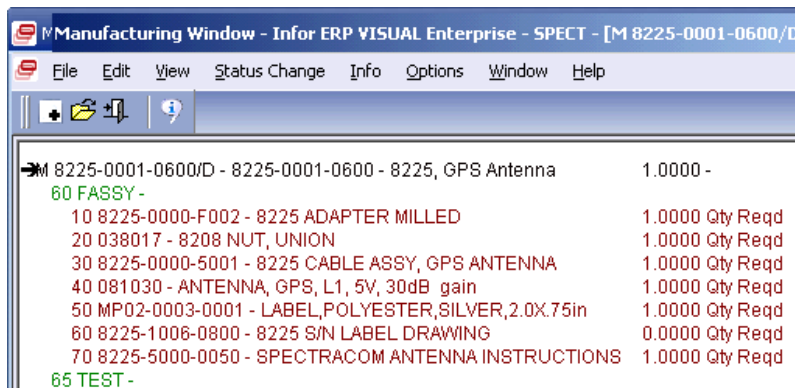
Current draw of Timing 1000 antenna (5vdc): 27ma

Minimum operating DC voltage for Timing 1000 antenna: 4.5vdc

Antenna impedance

With the red test probe on the center pin of the cable and the black test probe on the outer thread, the Model 8230 GNSS antenna impedance is about **5.6 Mohm**.

Model 8225 GPS antenna assembly



Manufacturing Window - Infor ERP VISUAL Enterprise - SPECT - [M 8225-0001-0600/D	
File Edit View Status Change Info Options Window Help	
8225-0001-0600/D - 8225-0001-0600 - 8225, GPS Antenna	1.0000 -
60 FASSY -	
10 8225-0000-F002 - 8225 ADAPTER MILLED	1.0000 Qty Reqd
20 038017 - 8208 NUT, UNION	1.0000 Qty Reqd
30 8225-0000-5001 - 8225 CABLE ASSY, GPS ANTENNA	1.0000 Qty Reqd
40 081030 - ANTENNA, GPS, L1, 5V, 30dB gain	1.0000 Qty Reqd
50 MP02-0003-0001 - LABEL,POLYESTER,SILVER,2.0X.75in	1.0000 Qty Reqd
60 8225-1006-0800 - 8225 S/N LABEL DRAWING	0.0000 Qty Reqd
70 8225-5000-0050 - SPECTRACOM ANTENNA INSTRUCTIONS	1.0000 Qty Reqd
65 TEST -	

Most recent antenna we were using for the Model 8225 antenna

Synergy Systems “Timing 1000 Rev B” GPS antenna (Extended temperature range antenna)



Timing1000 w/TNC connector

- **Link to Synergy website:** <http://www.synergy-gps.com>
- **Link to Synergy data sheet:** http://www.synergy-gps.com/images/stories/pdf/anttiming1000_tn892.pdf

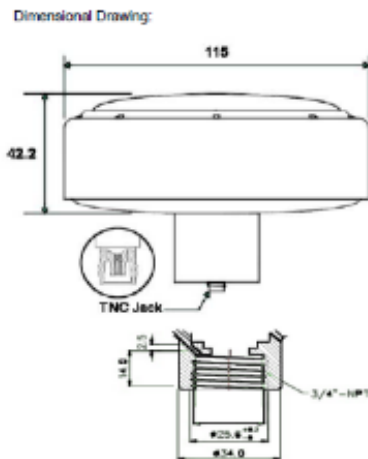
Our P/N: 081030 (in Arena at: https://app.bom.com/items/detail-sourcing?item_id=1202848106&version_id=10221273668)

Manufacturer's P/N: 10001044G Rev B

MTBF: Refer to: [MTBF/MTTR \(for all products\)](#)

CE Declaration of Conformity - EMI/EMC certificate for Model 8225. Refer to: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8225, 8225S, 8226, 8227 and grounding kit](#)

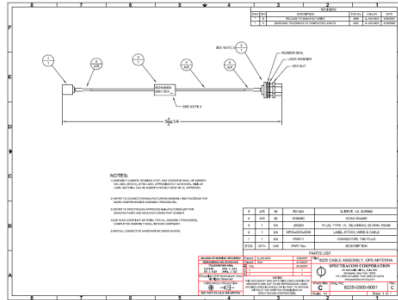
Antenna dimensions (as shown below): Refer to: http://www.synergy-gps.com/images/stories/pdf/anttiming1000_tn892.pdf



Cut-in date and S/Ns: Rev B of the Timing 1000s started shipping about 1/4/2011 with a cut-in S/N of 12950

Antenna Specs:

- **Connector:** TNC connector on the antenna itself (we shipped a P/N **8225-0000-5001** TNC to Type N adapter cable attached to the antenna)



- **GPS band:** L1 only (not L2 so it can't be used with SAASM receivers).
- **For SAASM receivers, refer to:** [Model 8225S](#)
- **IP rating:** [IP rating/Ingress rating \(for all products\)](#)
- **Antenna Gain:** 30dB typical
- **Antenna impedance:** ~62 ohms.
- **Antenna DC voltage range:** 4.5 to 5.5vdc
- **Extended temperature specs**

Email from Russ Cope on 1/4/2011 regarding the extended temp Model 8225 antennas:

The newer version Antenna has arrived today and we have begun making shipments to our customers.

The Label on the Antenna from the supplier contains "Rev B" so we will know that it is the new extended temperature version. Also, for reference the starting Spectracom S/N for this newer version of the 081030 is 12950.

The supplier (Synergy) starting S/N is 3007553.

(Email from Russ Cope on 1/4/2011)

The current Synergy Systems Timing 1000 Antenna Synergy P/N 10001044G (meaning the ones shipped prior to ~1/4/2011), is specification limited to a lower operational temperature of -30°C.

Synergy requested the antenna manufacturer redesign the relevant electronics in the Timing 1000 antenna to allow -40°C operation.

The antenna sample recently shipped to Spectracom incorporates this (-40°C) capability. All of the other specifications remain unchanged. (For specs on this antenna, except the lower temp range specified here, refer to Timing 1000 Rev A antennas below)

The extended range **(-40°C)** Timing 1000 antenna will replace the current **(-30°C)** antenna.

General Characteristics:

Parameter	Value
Operating Frequency:	1575.42 MHz, +/-1.023 MHz
Output Impedance:	50 Ohm
VSWR:	1.5:1 max
Polarization:	Right Hand Circular
Azimuth Coverage:	360°
Axial Ratio	3 dB max
Gain Characteristics of Antenna Element:	+5 dBi typically at zenith
Filtering:	30dB minimum @ Fo+/-50 MHz
LNA Gain:	30dB typical
Noise Figure:	2.0dB max
Power Requirements:	4.5-5.5 VDC
Power Consumption:	27mA@4.5V, 0.12W typ

Environmental Specifics

Parameter	
Operating Temperature Range:	
Storage Temperature Range:	-40° C to +90° C
Humidity:	95% noncondensing
Water Proof	Water proof (Test condition IP66)

Radiation / search pattern

Email from Tom Richardson: I don't have a radiation pattern.

Polarization: Right Hand Circular

Azimuth Coverage: 360°

Axial Ratio: 3 dB max

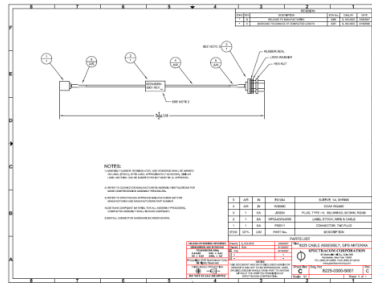
Earlier GPS antenna used as Model 8225 antennas

Specs on the Model 8225 (Synergy Systems Timing 1000 Rev A)

(Timing 1000, Rev A, which stopped shipping ~ 1/4/2011. For the newer extended temp range Timing 1000, refer to the Model 8225 Rev B antennas above).

- **Our P/N:** 081030 (same as it still)
- **Manufacturer's P/N:** 10001044G
- **Link to Synergy website:** <http://www.synergy-gps.com>
- **Link to Timing1000 GPS antenna data sheet:** <I:\Engineering\GPS Antennas> (AntTiming1000)
- **Antenna dimensions:** Refer to http://www.synergy-gps.com/images/stories/pdf/anttiming1000_tn892.pdf
- **Connector:** TNC connector on the antenna itself (we shipped a P/N **8225-0000-5001** TNC to Type N adapter cable attached to the antenna)





General Characteristics:

Parameter	Value
Operating Frequency:	1575.42 MHz, +/-1.023 MHz
Output Impedance:	50 Ohm
VSWR:	1.5:1 max
Polarization:	Right Hand Circular
Azimuth Coverage:	360°
Axial Ratio	3 dB max
Gain Characteristics of Antenna Element:	+5 dBi typically at zenith
Filtering:	30dB minimum @ Fo+/-50 MHz
LNA Gain:	30dB typical
Noise Figure:	2.0dB max
Power Requirements:	4.5-5.5 VDC
Power Consumption:	27mA@4.5V, 0.12W typ

Environmental Specifications:

Parameter	Value
Operating Temperature Range:	-30° C to +85° C
Storage Temperature Range:	-40° C to +90° C
Humidity:	95% noncondensing
Water Proof	Water proof (Test condition IP66)

Specs on the Model 8225 (Synergy Systems SA-300) Antennas

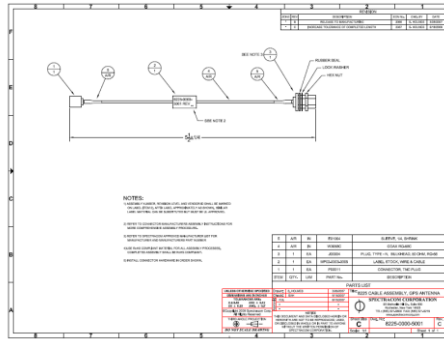
- Started shipping after May 2008
- **Cut-In Serial Number** above S/N 9800
- Impedance: 62 ohms

Antenna Element	
Polarization:	R.H.C.P. (Right Hand Circular Polarization)
Absolute Gain @ Zenith:	+5 dBi typically
Azimuth Coverage:	360°
Gain @ 10° Elevation:	-1 dBi typically
Azimuth Coverage:	360°
Axial Ratio:	3 dB max.
Output VSWR:	1.5:1 max.
Amplifier Element	
General:	L1 frequency, 1575.42 MHz +/-1.023 MHz
LNA Gain:	30 dB typically
Bandwidth:	2 MHz min.
Noise Figure:	2.0 max.
Out-of-Band Attenuation:	30 dB min. @ Fo +/- 50MHz
Current Consumption:	27mA +/- 3mA
Overall Performance	
Center Frequency:	1575.42 MHz
Gain:	27 dB typ.
Noise Figure:	2.0 max.
Axial Ratio:	3dB max.
VSWR:	2.0 max.
Output Impedance:	50 Ω
Electrical Characteristics	

Electrical Characteristics	
Supply Voltage:	4.5-5.5V DC
Power Consumption:	27mA @ 4.5 volts, 0.12 watts typ. < 0.2 watts max.
Environmental Characteristics	
Operating Temperature:	-30° to +85° C
Storage Temperature:	-40° to +90° C
Operating Humidity:	95% RH, non-condensing
Waterproof:	100% waterproof at the rating of IP66

Specs on the earlier Model 8225A (“CCAB32AST01”) antennas

- Stopped shipping around May 2008
- Serial Numbers below 9800
- **Impedance:** 177 ohms
- **Connector:** TNC connector on the antenna itself (we shipped a P/N **8225-0000-5001** TNC to Type N adapter cable attached to the antenna)



****Model 8225S (GPS L1/L2 antenna for SAASM GPS receivers)**

- Link to our datasheet: (8225S) [I:\Marketing\ Product Data Sheets \(archive\)\GPS Antennas & Accessories](I:\Marketing\ Product Data Sheets (archive)\GPS Antennas & Accessories)
- Link to 8225S manual (1184-5000-0050) in Arena: https://app.bom.com/items/detail-spec?item_id=1202833258&version_id=10212776438&orb_msg_single_search_p=1
- Link to Antennas in Engineering drive (AntCom): <I:\Engineering\GPS Antennas>
- Our P/N for just the Model 8225S antenna by itself: E025-0005-0001
- Our P/N for the entire antenna mast assembly: 1184-0001-0600 (in Arena): https://app.bom.com/items/detail-spec?item_id=1202842013&version_id=10221282808
- Process detail (1184-0001-0600-PD) in Arena: https://app.bom.com/items/detail-spec?item_id=1202833257&version_id=10221289258

8225S MTBF/Quality reports/Test Reports

- Refer to E025-0005-0001 -> Files (in Arena): https://app.bom.com/items/detail-attach?item_id=1202842901&version_id=10221253538

MTBF (in Arena): https://app.bom.com/files/detail-summary?file_master_id=1235357857&file_id=1747140640

Manufacturer: AntCom Corp

- Link to MFG website (Click “GPS L1/L2 Antenna Catalog” to download info) <http://www.antcom.com/products/gps-gns-sbas-crpa.php>
- MFGs P/N for the Model 8225S antenna: 53G1215A-XN-1 (not RoHS compliant)

RoHS compliancy for 8225S L1/L2 antennas

- 1st gen 8225S is not RoHS compliant.
- 2nd gen 8225S (~Aug 2019) is RoHS compliant
- Refer to ECO-2250 and ECO-2211

ECO-2250

ECO-2211 (August 2019) releases RoHS compliant 8225S (Antcom P/N 53G1215A-XN-1-RoHS). This ECO releases the antenna to production. Another subsequent ECO will cut-over the antenna to this RoHS antenna.

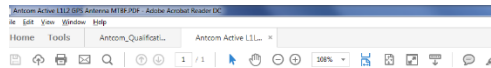
Summary

- **Original 8225S (AntCom P/N 53G1215A-XN)** is NOT RoHS compliant
- **Next Gen 8225S (AntCom P/N 53G1215A-XN-1-RoHS)** is RoHS compliant

Contact info for Antcom

tech@antcom.com

Email from Paul Myers (17 Jun 16): “I used tech@antcom.com and received a response from a Mr. Ken Lee regarding the antenna pattern I sent you.”



Antcom's Active L1/L2 GPS Antenna,				
MTBF CALCULATION PER MIL-HDBK-217F PARTS COUNT RELIABILITY PREDICTION METHOD				
ITEM	QUANTITY	FAILURE RATE PER 10 ⁶ HOURS	QUALITY FACTOR	TOTAL FAILURE RATE PER 10 ⁶ HOURS
CAPACITOR, CERAMIC	38	0.0030	3	0.4104
CAPACITOR, TANTALUM	2	0.0018	3	0.0108
CONNECTOR	4	0.0024	2	0.0432
PLT	4	0.014	8	0.448
IC, REGULATOR	1	0.0005	8	0.005
INDUCTOR	8	0.0017	4	0.0498
RESISTOR, WW POWER	6	0.014	3	0.252
SOLDERED CONNECTIONS	136	0.00007	1	0.00952
factor		1.29072		1.5
		1.93608	TOTAL	1.93608
				0.818507582
			MTBF (HOURS)	61600
			MTBF (YEARS)	89

Manufacturing Window - Infor VISUAL - SPECT - [M 1184-0001-0600/C]	
File Edit View Status Change Info Options Window Help	
1184-0001-0600/C - 1184-0001-0600 - 8225S GPS Antenna, L1-L2 1.0000 -	
10 BDASSY [SM]	
10 0300-1000-0014 - LABEL, SN TAG, Board	0.0000 Qty Reqd
20 1165-1000-0709 - Mast, Antenna	1.0000 Qty Reqd
30 1184-0001-0600-PD - 8225S GPS Antenna, L1-L2, Process De	0.0000 Qty Reqd
40 1184-5000-0050 - MANUAL, 8225S	1.0000 Qty Reqd
50 E025-0005-0001 - ANTENNA, GPS, L1-L2	1.0000 Qty Reqd
60 MP00002 - CABLE TIE, 8in, RoHS compliant	2.0000 Qty Reqd
70 MP02-0003-0001 - LABEL, POLYESTER, SILVER, 2.0X.75in	1.0000 Qty Reqd
80 MP08452 - HOSE CLAMP, 2in to 6in	2.0000 Qty Reqd

https://www.navtechgps.com/antcom_active_l1l2_gps_antenna_3_5/

From: <http://www.antcom.com/index.html>



Active L1/L2 GPS Antenna, 5" ground-plane, 3.5" circular, 33 dB, N-type connector, white

Part Number: 53G1215A-XN-1

Input Voltage: 2.5 to 24 V

Power Handling: 1 Watt

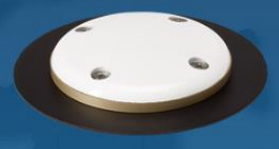
LNA Gain: 33 dB

LNA Options: passive, 20 dB, 33 dB, or 40 dB active

Connector(s): N-type

Alternate Connectors: MCX, MMCX, N, N-B, SMA, TNC, TNC-B, or cable

Color: white



Specs

- **Receives:** L1 (1575.42 MHz) and L2 (1227.60 MHz) GPS bands
- **Antenna Gain:** L1 gain is **33dB** L2 gain is **35dB**
- **DC Operating voltage range:** **2.5 – 24VDC**
- **Antenna Power draw** is **50 mA**
- **Noise Figure** of 8225S antenna, **3dB**

Cable loss allowed by the Model 1204-1A GB Gram SAASM receiver (Model MPE-S)

Per Paul Myers "23 Jun 16) Dennis H at Rockwell said from the Antenna to MPE-S they desired no more than an 8 dB loss.

Dept of Defense Form DD-1494 (DD1494 for SAASM)

- Refer to: "[I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8225S\DD-1494 Form](#)"

Email from Dave L to Morgan Randolph This must be an extended version of the DD-1494.

There is a section Receiver Equipment Characteristics form on page 3 dealing with the receiver and Antenna Equipment Characteristics on page 4 form for the 8225S antenna . That is what the customer was asking about.

Can we provide this information to them?

Reply from Morgan Randolph to Dave L (12 May 2020) Hey Dave, this should be what you need:

<https://www.oralia.com/documents/8225s-datasheet>

Hiro says we do not need a DD-1494 for the VersaSync because it is not transmitting.

Hi Morgan,

The Versasync does not emit any RF so a DD-1494 is not required. It's only required if you have an emitter (transmitter). (See the section labeled " APPLICATION PURPOSE" in the instructions page.)

-Hiro

Mil-STD design specs

- The antenna is designed to DO-160 and MIL-STD requirements
- **DO-160** discusses factors such as: Salt spray, Temperature and Altitude, Sand and Dust, Fluid susceptibility, Vibration, Icing, Humidity, and Waterproofness

Email from Antcom (25 Jan 2018) The antenna is designed to DO-160 and MIL-STD requirements. We have tested similar built products with DO-160 and MIL-STD requirements. Attached are some of the test reports.

Questions from Salesforce case 123365 (answers in yellow highlight are from Antcom, 25 Jan 18):

Some of my questions quickly summarized:

- 5) Is the electrical connection water proof? **Yes, see attached DO-160 report**
- 6) Where has the vendor fielded these antennas in the past? **Unknown, give Spectracom data on shipments, probably world wide.**
- 7) Request from vendor the vibration test reports. (claim's >30G's how?) **see DO-160 report**
- 8) Any EMI info? EMI testing required? **Yes, See EMI test report**
- 9) Has the GPS has been tested to operate in icing conditions? **Yes, see attached DO-160 report**
- 10) What does impact resistant mean? Can it take on Hail that is 3.5" in diameter? **Unknown**
- 11) Can the vendor provide Transmit Losses? To calculate signal levels through snow/ice loads. **Unknown**
- 12) Radome Hydrophobic? Icephobic? **Unknown**
- 13) Will the radome operate in motion? In wind. How much relative motion can there be to maintain a connection? **Unknown**

- 14) Is the GPS antenna really hermetically sealed? (It has screws through the radome.) **Yes**
- 15) What is the cable materials?
- 16) Is the polyurethane material a polyether urethane or some other type? We are investigating the quantity of future fungus growth.

CE/ ESD protection

- Refer to page 4 (test summary) of the 8225S CE test report : <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8225S\CE test report>



Test Report No. 774-5818B-1-1-NE

TEST SUMMARY

This test record demonstrates conformance of the Antcom Corp. L-Band/GPS Receiving only Antenna to the standards listed below.

Region	Specification	Title/Intent	Conforms Yes/No/NA	Comments
European Union (EU)	EN 55024 :98 (CISPR 24)	ITE Immunity		As per the following normative references (indicated by bullets):
	EN 300 386 v1.3.3 :2005-04	EMC Requirements for Telecommunications Network Equipment		
	• EN 61000-4-2	Electrostatic Discharge (ESD)	Yes	
	• EN 61000-4-3	Radiated RF Immunity	Yes	

Mechanical drawing/Dimensions for the antenna head

- Refer to “Model 8225S mech drawing” file in: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8225S>

(from http://www.antcom.com/documents/catalogs/Page/53G1215A-XT-X_L1L2GPSAntennas.pdf)



Parts included with 8225S antenna

8225S antenna assembly (1184-0001-0600) https://app.bom.com/items/detail-bom?item_id=1202842013&version_id=10299428918 includes the following items:



- **8225S antenna** (P/N E025-0005-0001)
- **Mast Assembly** (P/N 1165-1000-0709) https://app.bom.com/items/detail-spec?item_id=1202833257&version_id=10298096768
- **User manual** (P/N 1184-5000-0050)
- **(2) cable ties** (our P/N MP0002, 8in, RoHS compliant, weather resistant)
- **(2) hose clamps** (our P/N MP0842)
 - 2 inch to 6 inch, McMaster-Carr P/N 5322K22 (<https://www.mcmaster.com/#catalog/123/303/=162gggr>)

Quick-Release Clamps for Firm Hose and Tube
Clamps have a slotted hex-head screw that flips up to release the band for quick opening.
Clamps are for firm plastic and rubber hose and tube. Do not exceed the maximum torque or clamps may be damaged.
Zinc-plated steel offers fair corrosion resistance.
201 and 410 stainless steel have good corrosion resistance.
Note: When choosing a clamp, measure the outside diameter of your hose or tube with the fitting installed.
For technical drawings and 3-D models, visit our parts number.

Clamp ID Range		Band	Size	Temp	Max Torque	Drive Style	Hex Size	Reusable	Pkg	Pkg
inch	mm	Temp	Size	Temp	in.-lb.					
201 Stainless Steel with Zinc-Plated Steel Screws										
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K14	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K15	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K16	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K17	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K18	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K19	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K20	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K21	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K22	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K23	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K24	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K25	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K26	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K27	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K28	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K29	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K30	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K31	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K32	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K33	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K34	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K35	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K36	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K37	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K38	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K39	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K40	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K41	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K42	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K43	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K44	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K45	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K46	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K47	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K48	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K49	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K50	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K51	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K52	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K53	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K54	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K55	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K56	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K57	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K58	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K59	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K60	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K61	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K62	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K63	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K64	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K65	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K66	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K67	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K68	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K69	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K70	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K71	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K72	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K73	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K74	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K75	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K76	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K77	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K78	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K79	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K80	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K81	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K82	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K83	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K84	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K85	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K86	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K87	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K88	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K89	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K90	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K91	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K92	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K93	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K94	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K95	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K96	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K97	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K98	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K99	50	51
1/2" to 1 1/2"	12.7 to 38.1	-40° to 275°	35	Slotted External Hex	5/16"	Yes	10	5322K100	50	51

- **Our P/N for just the Model 8225S antenna by itself:** E025-0005-0001
- **Our P/N for the entire antenna mast assembly:** 1184-0001-0600 (in Arena): https://app.bom.com/items/detail-spec?item_id=1202842013&version_id=10221282808
- **Process detail (1184-0001-0600-PD) in Arena:** [https://app.bom.com/items/detail-spec?](https://app.bom.com/items/detail-spec?item_id=1202833257&version_id=10221289258)

Additional Accessories

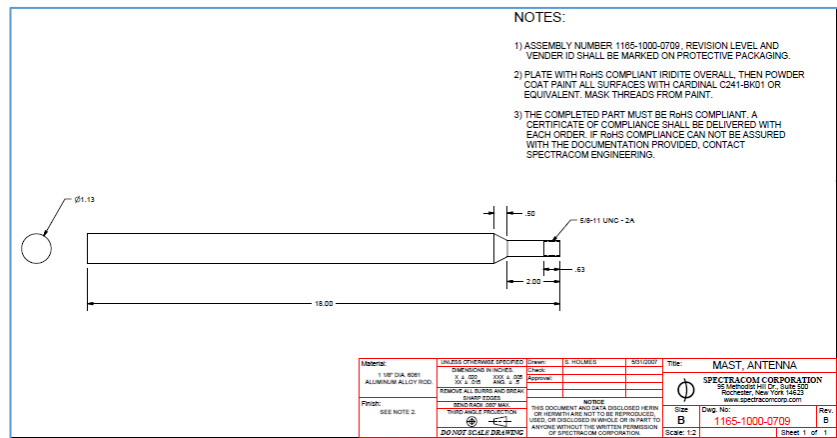
2. GPS Antenna Splitter - Model 8224
3. Antenna Surge Suppressor - Model 8226
4. Surge Protector Grounding Kit - Part Number 8226-0002-0600
5. Inline Preamplifier - Model 8227
6. Low Loss Antenna Cable - Model CAL7xxx
7. Indoor Plenum-rated Antenna Cable, CMP equivalent - Model CALP7xxx

Metal Mast assembly for 8225S antenna

- Our P/N: 1165-1000-0709

Metal (Not PVC)

Refer to (In Arena) https://app.bom.com/items/detail-sourcing?item_id=1202841049&version_id=10221253548&orb_msg_single_search_p=1&redirect_segno=6153405263



****Model ANT35 (ANT-35) GPS antenna (Discontinued)**



Note: The ANT-35 antenna has been replaced by the Model 8230 antenna. So, it's no longer available for purchase.

- **Link to our datasheet (35dB Epsilon-GPS):** [I:\Marketing\ Product Data Sheets \(archive\)\GPS Antennas & Accessories](#)
- **Link to our website:** <https://amxprd0610.outlook.com/owa/redir.aspx?C=TmaKPzNo70icEMkQXUdrFFX16-oFEdAl3hyCuKDG413Vd7LW3MHhXzkzp7djAsZD1EblA4gaZWk.&URL=http%3a%2f%2fwww.spectracomcorp.com%2fProductsServices%2fTimingSynchronization%2fGPSAntennasAccessories%2fEpsilonGPSAntenna%2ftabid%2f882%2fDefault.aspx>

Comparison of a Model ANT-35 to antenna Models 8230 or 8225

- Refer to “8230Comparison.pdf” [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8230\antenna comparisons](#)
- **Note:** this document is also on our website: <https://spectracom.com/documents/8230-gps-gnss-outdoor-antenna-datasheet>

September 30, 2013

Outdoor GPS Antenna Update - Model 8230 GPS/GNSS Antenna Replacement for 8225S and ANT-35

Introduction




Many Spectracom products have embedded GPS receivers. Typically used for time and frequency applications, these products are synchronized by processing the precise timing information contained in GPS signals. A typical installation uses an outdoor antenna installation to collect and transmit the RF of the collected signals to the embedded receiver. As a solutions provider, Spectracom offers GPS antennas and accessories from 3rd parties. Several factors have resulted in a change to some of the GPS antennas provided by Spectracom. This document will provide more information about the change.

What is the change?

On October 1, we are discontinuing the GPS antennas models 8225S and ANT-35 in favor for the model 8230 antenna.



Why the change?

A new antenna offers a variety of improvements. In addition to GPS L1, its frequency range covers GLONASS L1 signals as well. This feature allows us to integrate GPS+GLONASS receivers into our products without the need for specialized antennas to take advantage of the diversity of signals now available from global navigation satellite systems. We have already introduced the GLONASS + GPS option in SecureSync[®], and other products are on the way. The 8230 antenna has several other improvements: smaller/lighter, more gain and better filtering as shown in the chart below.

Model	8230	8225	ANT-35
Physical			
Frequency	1574-1606 MHz	1575.42 +/- 15 MHz	1575.42 +/- 1.023 MHz
Gain	40 dB	30 dB	35 dB typ
Out of band rejection	<1550 MHz: >50 dB >1640 MHz: >70 dB	Not specified	+/- 50 MHz: 60 dB typ
Op Temp	40 to 85 C	-30 to 85 C	-40 to 85 C
Size	66.5 mm dia x 47.5 mm h	89 mm dia x 70mm h	90 mm dia x 98.4 mm h
Weight	140 g	191 g	285 g typ
Mounting	Through hole clamped to included L-bracket compatible with post mount and ANT-KT mount	Threaded rod with flange mounted to included post	M4 screws, compatible with ANT-KT mount

Is the 8230 a drop in replacement for 8225 and ANT-35?

Yes, it has a female Type N connector to attach to an existing antenna cable, it uses the same power as supplied by the receiver, and will mount to a post or the ANT-KT with the included retaining nut and/or post mount L-bracket. What's more, every other GPS antenna accessory in our solutions set is compatible and continues to be available.



8230 mounted to a post via its included L-bracket *8230 mounted to a post via the ANT-KT*

Do I need a GLONASS or GNSS receiver to use the 8230?

No, the antenna works just fine with a receiver that is only capable of processing GPS L1 signals.

Will I be able to receive GLONASS signals if I use the 8230?

No, the antenna is capable of receiving the RF signals from GLONASS but it is the receiver that is embedded in the product that does the work. It is the combination of a GLONASS capable receiver and antenna that allows GLONASS signals to be used for synchronization.

What about SAASM?

The 8230 is not compatible with SAASM (encrypted GPS signals). We continue to supply the 8225S for SAASM products.

What about Galileo, Beidou and other GNSS signals?

The 8230 should work with any signal in 1574-1606 MHz range. However it is the receiver that is the critical component, not the antenna. Our roadmap includes adding more capability to our systems as other GNSS signals come online and receivers prove beneficial (cost comparable) and reliable. In the meantime, contact us if you have a specific need for synchronization to specific signals other than GPS or GLONASS L1.

An Oracle Group Business

Note from Tom Richardson (regarding Robert Houts from Harris): Customer has to realize that the GPS signal is a very low level signal, -130 dBm, and can be swamped by a large signal no matter what the filtering. No transmission is perfect, all have skirts, yada yada...

(235846): ANT-35 antenna mounting (Optional Model ANT-KT “Post Mount Kit”)



- **Spectracom P/N:** 235846
- **Optional ANT-35 mounting bracket datasheet:** [I:\Marketing\ Product Data Sheets \(archive\)\GPS Antennas & Accessories](I:\Marketing\ Product Data Sheets (archive)\GPS Antennas & Accessories)
- **In I drive:** <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\ANT-KT rugged post-mount>
- **In Arena at:**
 - https://app.bom.com/items/detail-references?item_id=1250397648&version_id=11047442308
 - https://app.bom.com/items/detail-spec?item_id=1202847124&version_id=10212764838

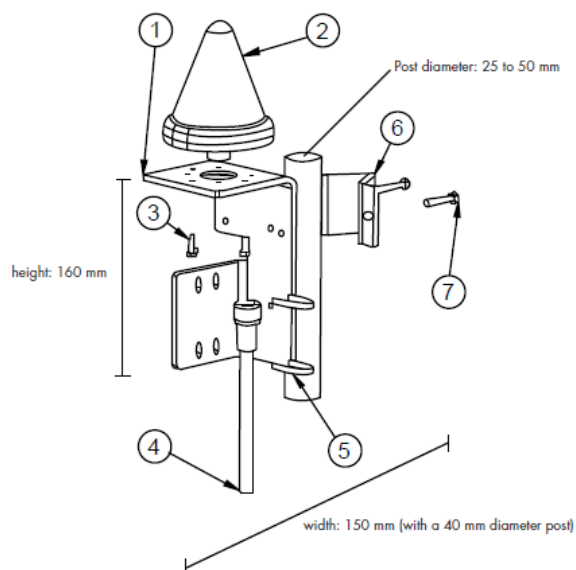
GPS Antenna Rugged Post Mount Kit

Model ANT-KT

The post mounting kit, sold separately from the antenna, allows you to mount a model 8230 or ANT-35 GPS antenna onto a vertical or horizontal post.

The steps needed to assemble the kit are as follows:

1. Clamp the GPS antenna (2) on the post bracket (1) with a retaining nut, or attach the GPS antenna (2) to the post bracket (1) with the four screws (3) depending on the type of antenna.
2. Insert the cable socket (4) into the antenna socket.
3. Insert the plastic cable tie (5).
4. If desired, use the supplied electrical tape to wrap the antenna cable connection to reduce exposure to moisture.
5. Rotate the post clamp (6) to obtain vertical and horizontal mounting.
6. Attach the post bracket (1) to the post with the post clamp (6), use the two screws (7), nuts and lock washers.



1. Post bracket
2. GPS antenna (ANT-35 model shown)
3. Screws (if necessary)
4. GPS cable
5. Plastic cable tie
6. Post clamp
7. Screws & washers

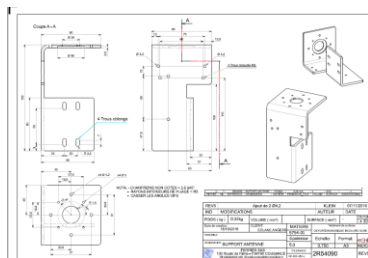


(Refer to above illustration) The optional Model ANT-KT post mounting kit allows you to mount the Epsilon GPS Antenna onto a vertical or horizontal pole. Kit includes:

1. Post bracket
2. GPS antenna (purchased separately)
3. Screws
4. GPS cable (purchased separately)
5. Plastic cable tie
6. Post clamp
7. Screws & washers

Mechanical drawing of the ANT-KT (in French)

- Refer to PDF (2R54090..) in: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\ANT-KT rugged post-mount>



BOM for ANT-KT (in Arena) https://app.bom.com/items/detail-references?item_id=1250397648&version_id=11047442308

Note: “Audros” is a PLM system (not the manufacturer of the parts)

Item Names below are translated from French

ANT-KT

Unreleased

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

Screws for the ANT-KT kit

ANT-35 Antenna packages for Epsilon Clocks

A) EC-PK1:

- GPS Antenna Pack for EBO3, EC1S, EC2S, EC3S
- Package includes (1) ANT35 antenna and mounting, (1) "through plate" lightning suppressor, and two cables.
- Refer to Salesforce for details:
https://na8.salesforce.com/_ui/search/ui/UnifiedSearchResults?searchType=2&sen=01t&sen=a0F&sen=a0E&sen=005&sen=006&sen=00Q&sen=501&sen=001&sen=00T&sen=003&sen=810&sen=00U&sen=500&sen=02i&sen=00O&sen=a04&sen=ka&sen=00a&sen=550&sen=0F9&str=EC-PK2+#!/fen=01t&initialViewMode=detail&str=EC-PK2

B) EC-PK2

- GPS Antenna Package for EC22S
- Package includes (2) ANT35 antennas and mounting, (2) "through plate" lightning suppressors, and two cables.
- Refer to Salesforce for details:
https://na8.salesforce.com/_ui/search/ui/UnifiedSearchResults?searchType=2&sen=01t&sen=a0F&sen=a0E&sen=005&sen=006&sen=00Q&sen=501&sen=001&sen=00T&sen=003&sen=810&sen=00U&sen=500&sen=02i&sen=00O&sen=a04&sen=ka&sen=00a&sen=550&sen=0F9&str=EC-PK2+#!/fen=01t&initialViewMode=detail&str=EC-PK2

Model 235884 LP-TP lightning suppressor for Epsilon Clocks (EC20S, EC22S, etc)



Shipped out of Spectracom France for their orders

Spectracom P/N: 235884

- In Salesforce: <https://na28.salesforce.com/01t80000001XZJz?srPos=0&srKp=01t>
- In Arena: https://app.bom.com/items/detail-bom?item_id=1202847125&version_id=10212764848&orb_msg_single_search_p=1
- Refer to on our website: <http://www.spectracomcorp.com/ProductsServices/TimingSynchronization/GPSAntennasAccessories/LPTPGP SLightningProtection/tabid/1184/Default.aspx>
- Type N connectors

Indoor GPS antennas

Skylight antenna (1213-0000-0600)

- Refer to Skylight info in the SecureSync Custassist doc: <..\SecureSync CustAssist.pdf>

Warranty period: Per Dave Sohn, one year warranty

Model 8228 window-mount antenna (8228-0002-0600)



- **GPS only antenna** (not Glonass, Galileo, etc capable)
- **Link to our website datasheet:** https://www.rolia.com/sites/default/files/document-files/8228_gps-indoor-window-mount-antenna.pdf
- **Link to MFG data sheet in Eng ("Motorola hawkactive"):** <I:\Engineerihawkng\LIBRARY\Parts>

- **Our P/N for just the antenna head:** E025-0001-0002 (in Arena) https://app.bom.com/items/detail-spec?item_id=1202842890&version_id=10221318308
- (Per ECO-1312) Alternate Model antennas for the 8228, due to discontinuance (in Arena): https://app.bom.com/items/detail-spec?item_id=1202842890&version_id=10298206588&
- **Link to 8228 manual (8228-0002-0600** in Arena at) https://app.bom.com/items/detail-spec?item_id=1202840940&version_id=10267450198&orb_msg_single_search_p=1&redirect_seqno=7139887998
- **Motorola P/N:** GCNLP271CA
- **World Products P/N:** WPANTG10D2299926
- **Our P/N 8228-0002-0600** (in Arena): https://app.bom.com/items/detail-spec?item_id=1202840940&version_id=10290389928

#	Item Number	Item Name	Category
1	8184-1000-0723 rev 2	8184 BRACKET, MOUNTING	Fabricated Metal
2	8228-0002-0600-PD rev 1	Process Detail, 8228 GPS Indoor Window Mount Antenna	Process Detail
3	8228-1006-0801 rev 1	Label, GPS Indoor Window Mount Antenna Kit	Label
4	CA01-0NSA-2050 rev 5	COAX CABLE Assy, N Male, SMA Female, 50FT	Cable Assembly
5	E025-0001-0002 rev 2	ANTENNA,GPS,WINDOW MOUNT	Antenna / Ferrite Core / Insulator
6	MAN8228 rev 6	8228 Installation Instructions	Manual
7	MP00110 rev 2	TAPE, DOUBLE COATED ACRYLIC FOAM, VHB	Miscellaneous Mechanical

Motorola antenna specs

General Characteristics	Antenna Description	<ul style="list-style-type: none"> • Low profile active microstrip patch antenna • Molded plastic radome • Electrically shielded LNA PWB assembly
	Operating Frequency	• L1 (1575.42 MHz, +/- 1.023 MHz)
Performance Characteristics	Input Impedance	• 50 Ohm
	VSWR	• 1.5 (typical) @ 1575.42 MHz
	Bandwidth	• 45 MHz @ 3 dB points (typical)
	Polarization	• Right hand circular
	Azimuth Coverage	• 360 degrees
	Elevation Coverage	• 0 degrees to 90 degrees
	Gain Characteristics of Antenna Element	<ul style="list-style-type: none"> • +2 dBic minimum at zenith (typical) • -10 dBic minimum at 0 degrees elevation (typical)
	Filtering	<ul style="list-style-type: none"> • -25 dB @ 1670 MHz (typical) • -25 dB @ 1480 MHz (typical)
	LNA Gain	• 24 dB (typical, including 6 dB cable loss)
	Noise Figure	• 1.8 dB (typical)
	Burnout Protection	• Protected from damage by RF signals, when the power received by the antenna is no greater than +17 dBm absolute maximum
	Dynamics	<ul style="list-style-type: none"> • Vibration: 7.7G per Military Standard 810E Method 514.4 • Shock: 100G (18 ms sawtooth) Military Standard 810E Method 516.4
Electrical Characteristics	Power Requirements	• 5 ± 0.5 Vdc 50 mV p-p ripple (maximum)
Physical Characteristics	Power Consumption	• 20 mA @ 5 Vdc (typical)
	Dimensions	<ul style="list-style-type: none"> • 49.6 L x 43.0 W x 18.0 H mm • 33.3 L x 29.8 W x 8.8 H mm (Substrate w/shield)
	Weight	• < 40 grams (housed assembly, less cable)
	Cable Connector	<ul style="list-style-type: none"> • 90 degree OSX/MCX (subminiature push on) • BNC • Call for other connector types (SMB, GT5...)
Environmental Characteristics	Antenna to Receiver Interconnection	<ul style="list-style-type: none"> • Single RG-174U type coaxial cable 6 meters (20 ft.) long (10 dB maximum loss at 1575.42 Mhz) • Single RG-174U type coaxial cable 203 mm (8 in.) long
	Operating Temperature	• -40°C to +100°C
	Storage Temperature	• -40°C to +100°C
	Humidity	• 95% noncondensing +30°C to +60°C
Miscellaneous	UV Radiation	• 1200 hrs. @ +63°C w/rain @ 12 min./hr.
	Salt Spray Test	• Spray 5% NaCl solvent at +35°C for 320 hrs.
	Optional Features	<ul style="list-style-type: none"> • Mounting options: <ul style="list-style-type: none"> - Magnetic mount - Direct mount • Substrate: patch antenna and shielded LNA on PWB with 6 meters of RG-316U type coaxial cable with 90 degree OSX/MCX connector

Antenna gain: 24dB

Window-mount bracket for 8228

- Our P/N 8184-1000-0723
- **Foam adhesive tape used on mounting bracket:** Our P/N is MP00110. Visual says it's a "DOUBLE COATED ACRYLIC FOAM, VHB"

Model 8228 antenna cabling

1) Cable attached to the antenna

- **Cable length:** 117 inches (just under 10ft)
- Terminated with SMA connector



2) 50 ft antenna cable (included with 8228 antenna)

- Coax Cable is LMR-195 (50 foot)
- Extension LMR195 cable is P/N CA10xxx.
 - Current 50ft cable shipping w/8228 has **Type N termination** on one end and **SMA connector** on the other



-
-
- Older SMA to SMA adapter (for use with older 8184/8189) is our P/N: **A000-001-0000?? (8228-0001-5000)** **Note (17 Aug 15 KW)** I don't believe this cable is still available.

Link to old PD for the 8228-0001-5000 (50 ft, SMA to SMA cable) <I:\Engineering\Archive\Released\091000 - 8228\Manufacturing\091000 - 8228 - Process Details\Cables\Current Release\8228-0001-5000.doc>

Q can someone confirm that the 8228 has an SMA on the end of the cable and that we just provide an "SMA to N" adapter with the antenna? This customer wants an SMA connector.

A Email from Keith (17 Aug 2015) The Model 8228 indoor GPS antenna (not Glonass capable) itself has a short length of coax (attached which is terminated with an SMA connector. The antenna is supplied with a 50 foot length of coax with an SMA connector on one end (to attach to the antenna) and a Type N connector at the other end (to attach to a Spectracom receiver, such as SecureSync).

Attached for your reference is a copy of the Model 8228 install manual.

P/N ACC325: Available SMA to Type N adapter

- Note the 50ft LMR-195 cable which ships with the Model 8228 is terminated on one end with an SMA connector to attach directly to the Model 8228. There is no longer a need to supply an SMA to N pigtail cable or adapter to attach the cable to the antenna.

Our P/N: ACC325

- (in Arena: https://app.bom.com/items/detail-spec?item_id=1202834983&version_id=10221283248&orb_msg_single_search_p=1&redirect_seqno=8404869091)



Email from Tony DiFlorio to a customer (18 Aug 15) I just confirmed that the connector on the receiver cable end is only available with an “N” connector. We no longer offer this antenna with SMA on the receiver cable end.

However, we do offer an SMA Male to N Male adapter # ACC325. Price: \$120 each. See below: Will this work for you?

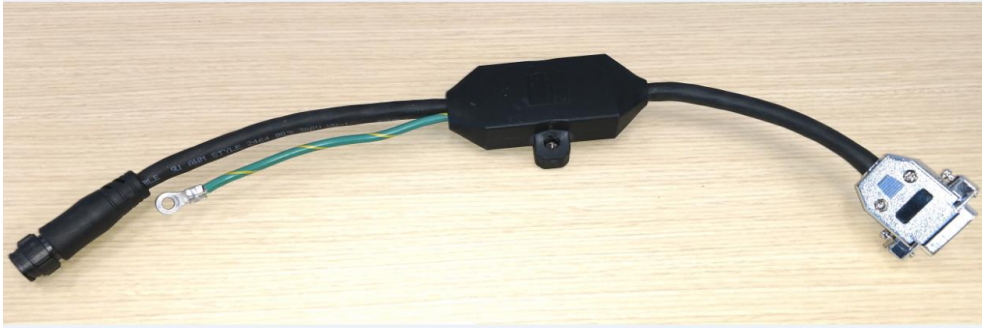
****Trimble Acutime GPS/GNSS Antennas (2000, Gold, GG and 360)**

1024 GPS week rollover (such as in the year 2019) for TSAT boards (Acutime antennas)

- Refer to: [GPS 1024 Week roll-over issue due to number of bits in the message \(GPS Epoch every 20 years\)](#)

Lightning Suppressor for Acutime antenna

Email from Tim T (Jan 2019) – approved by Dave S to send to customer. (Not in our catalog).



We already have something for the Acutime antennas. It is from a company called zap-tech.

<http://www.zap-tech.com/#pg-home-3>

The model number you would order is #40-422-001. (See attached data sheet and picture)

Timothy Tetreault

Model 1169 Fiber isolators/converters (for Invensys/Schneider electric) installed between Acutime Antenna and TSAT/TSyncE timing boards

- refer to (in this document): [Model 1169 GPS Fiber Optic Isolator \(TX and RX\) for GPS:](#)

Summary of the four different models of Trimble Acutime antennas that have been, or are still available from Trimble

- Listed below, most recent to earliest variant

1. **Trimble Acutime 360 Multi-GNSS Smart antenna** (GPS, GLONASS, Beidou, Galileo-ready) (refer to “A” further below)



Purpose: Replaces Trimble **Acutime-GG** antennas as a GNSS (multi-constellation) antenna

Part Numbers associated with Acutime 360

- Trimble P/N for Acutime 360 (raw antenna): 106406-00
 - In Arena: https://app.bom.com/supplier-items/detail-spec?item_id=1256243949&orb_msg_single_search_p=1
 - Our P/Ns for Acutime 360 antenna
1. **E025R-0004-0004** (*raw antenna, not yet reprogrammed, as we receive it from Trimble*): Acutime 360 antenna programmed by Trimble to output **Trimble TSIP** data
 - In Arena at: https://app.bom.com/items/detail-spec?item_id=1255453404&version_id=11133848698&orb_msg_single_search_p=1
 - in Salesforce at:
 2. **E025R-9000-0001**: Acutime 360 antenna reprogrammed at our factory to output **NMEA** data
 - In Arena at: https://app.bom.com/items/detail-spec?item_id=1255453450&version_id=11165392838

Process Detail for Acutime 360

- Link to Process Detail (E025R-9000-0001-PD) in Arena https://app.bom.com/items/detail-spec?item_id=1266844640&version_id=11338812588&
- In Salesforce at: (Apparently not yet in Salesforce, as of at least 9 July 2019)

Specs from Acutime 360 datasheet

ACUTIME™ 360 MULTI-GNSS SMART ANTENNA

GENERAL SPECIFICATIONS

Receiving Signal.....GPS, GLONASS, Galileo¹, Beidou
Positioning System.....SPS, Timing
1 PPS Timing Accuracy.....15 ns (1 sigma)
Update Rate.....1 Hz
Typical Min Acq Sensitivity.....-148dBm cold start
Typical Min Tracking Sensitivity.....-160dBm
Time to First Fix².....<46s (50%), <50s (90%) cold start
Typical Time to Re-acquisition.....<2s (90%)
Accuracy Horizontal Position.....<6m (50%), <9m (90%)
Accuracy Vertical Position.....<11m (50%), <18m (90%)

¹ Hardware ready: a firmware update is required to enable the Galileo constellation.
² The performance criteria and times given for TTFF & reacquisition are with GPS satellites in the constellation set.

INTERFACE CHARACTERISTICS

Serial Port.....2 serial port
Protocols.....TSIP, NMEA 0183
All ports support baud rates 4.8-115.2kbps; 8 data bits; E, O or no parity.

ELECTRICAL CHARACTERISTICS

Power.....+5VDC¹ to +36VDC, reverse polarity protection
Power Consumption.....<1.0Watt
¹ Reduced cable length @+5VDC to +12VDC

ENVIRONMENTAL SPECIFICATIONS

Operating Temperature.....-40°C to +85°C
Operating Humidity.....5%-95% RH non-condensing (+60°C)
Storage Temperature.....-55°C to +105°C
Ingress Protection.....IP67
EMC.....CE, FCC Class B

PHYSICAL CHARACTERISTICS

Dimensions.....95mm x 72.5mm
(3.74" D x 2.85" H)
Weight.....5.4oz (154grams)
Connector.....12-pin round, waterproof
Mounting.....1"-14 straight thread or 3/4" pipe thread

Mechanical Drawing

Visit www.trimble.com/timing for part numbers and information about where to buy.

Parts of the product are patent protected.
Trimble has relied on representations made by its suppliers in certifying this product as RoHS-II compliant.
Specifications subject to change without notice.
Trimble Navigation Limited is not responsible for the operation or failure of operation of GPS satellites or the availability of GPS satellite signal.

Associated ECOs (Engineering changes) for the Acutime 360 antenna

A) ECO-FAI-001886: FPGA issue for TSYNC-PCIE Cards (ECO effective 5 Dec 2018)

Link to ECO: https://app.bom.com/changes/detail-summary?change_id=2395198855&orb_msg_single_search_p=1

This ECO releases new software/FPGA for the TSync-PCIE that will fix the following issues relating to the Acutime 360 antenna:

- 1) An issue in interfacing to the new Acutime 360 when configured in TSIP.
- 2) An issue interfacing to any Acutime antenna when configured in NMEA mode.

B) ECO-FAI-002072: Release new Trimble Acutime 360 NMEA Programming (ECO effective 14 June 2019)

Link to ECO : https://app.bom.com/changes/detail-summary?change_id=2396525519&orb_msg_single_search_p=1

Link to Process Detail (E025R-9000-0001-PD) in Arena https://app.bom.com/items/detail-spec?item_id=1266844640&version_id=11338812588&

This ECO will release new process details for programming the new Trimble Acutime 360 antenna.

- 1) It releases new configuration file use to setup the Acutime 360.
- 2) It releases new software from Trimble to program the Acutime 360.
- 3) It updates the BOM for the programmed antenna, P/N: **E025R-9000-0001**

360s very soon.

Support for Acutime 360 antenna:

- Support to use Acutime 360 antenna was added in TSynC firmware update version 3.4.9 (~7 Dec 2018)
- Refer to **ECO-FAI-1886** in Arena: https://app.bom.com/changes/detail-summary?change_id=2395198855&orb_msg_single_search_p=1
Refer also to: [..\PSB, PSP software updates\TSYNC boards\TSync firmware updates \(PCIe, cPCI, PCI104\)\TSync-PCIe\TSync-PCIe firmware updates](..\PSB, PSP software updates\TSYNC boards\TSync firmware updates (PCIe, cPCI, PCI104)\TSync-PCIe\TSync-PCIe firmware updates)

Associated antenna mast: ??

P/N: 1159-0000-0700 (in Arena) https://app.bom.com/items/detail-spec?item_id=1202841005&version_id=10221291538&orb_msg_single_search_p=1&redirect_seqno=6678014486

Communication protocols (TSIP/NMEA-0813) / programming the Acutime 360 antenna

TSIP output data versus NMEA output data

A) TSIP data (default mode from Trimble)

TSIP: The Trimble Standard Interface Protocol (TSIP) consists of command packets and report packets

Acutime 360 GNSS Antennas (pre-configured at Trimble factory to output TSIP- not NMEA)

- Refer also to: <..\CustomerServiceAssistance.pdf>
- Our P/N **E025R-9000-0001** (in Arena at) https://app.bom.com/items/detail-spec?item_id=1255453450&version_id=11133851398&orb_msg_single_search_p=1
- being released with just the Acutime 360 on it. Final BOM will have PD and software to program for NMEA output. This will be added prior to customer shipment.

A) NMEA data (needed for compatibility with TSAT timing boards)

- **We reprogram the Acutime 360 antennas here for TSAT=PCI-33U/66U, TSAT-PCI-U, TSAT- PC104** (we switch the Acutime 360 antenna from using TSIP protocol to instead use **NMEA** protocol, which is the protocol the legacy TSAT boards use.
- **Trimble's Acutime 360 Data sheet:** <http://trl.trimble.com/docushare/dsweb/Get/Document-807197/>
- Acutime 360 User Guide: (??)

Note: as of at least 8 August 2018, we have not yet shipped any Acutime 360 antennas. but as the Acutime=GG antennas are now discontinued; we intend on transitioning to the

B) GG TSIP protocol output (Trimble format)

- Factory default/standard protocol setting for the Acutime-GG antenna is "**TSIP**" protocol
- **TSync boards** are configured in their EEPROM to use **TSIP** protocol to communicate with its external receiver

So we can send the Acutime-GG antennas out “unprogrammed”, when it’s being used with TSyncE boards

C) NMEA protocol (NMEA 0183) output

- All “Legacy” TSAT timing boards communicate with their external receiver using **NMEA** protocol (not TSIP protocol)
- So, we reprogram the Acutime-360 antennas here at the factory for **NMEA-0813** when they are being used with TSAT boards.

E025R-9000-0001: Acutime 360 GNSS Antennas (we reconfigure antenna to output “NMEA”, for companies such as Invensys/Schneider Electric)

- Refer also to [..\TimingBoardCustAssist.pdf](#)
- Our P/N **E025R-9000-0001** (in Arena at) https://app.bom.com/items/detail-spec?item_id=1255453450&version_id=11133851398&orb_msg_single_search_p=1
 - being released with just the Acutime 360 on it. Final BOM will have PD and software to program for NMEA output. This will be added prior to customer shipment.
 -
- Compatible with specialized TSync boards (**1191-9000-0600**) having an EPROM configured for NMEA protocol input (instead of the normal factory default TSIP protocol)

Summary of the Acutime-360 replacing the earlier Acutime-GG Smart antennas:

- The Acutime-360 antenna uses a different Model receiver (Res-SMT-GG) which can track GPS and Glonass satellites
- The Acutime-360 antenna has better sensitivity than the earlier Acutime Gold, to be able to track weaker signals?

Support to be able to use Acutime 360 antenna with TSyncE boards.

- Support to use Acutime 360 antenna with TSyncE boards was added in TSync firmware update version 3.4.9 (~7 Dec 2018)
 - Refer to **ECO-FAI-1886** (in Arena): https://app.bom.com/changes/detail-summary?change_id=2395198855&orb_msg_single_search_p=1
 - Refer also for TSync-PCIe firmware update info: [..\PSB, PSP software updates\TSYNC boards\TSync firmware updates \(PCIe, cPCI, PCI104\)\TSync-PCIe\TSync-PCIe firmware updates](#)

- Refer to Salesforce Case 197109

Email Keith sent to Apps (17 June 2019) For case 197109, I see Nidal has an existing TSync-PCIe customer inquiring about compatibility with the Trimble Acutime 360 antennas. The customer is inquiring on the status of this case, so I am trying to assist him with this case.

My understanding is that IF the following conditions are true:

- 1) a TSync board was previously being used with a Trimble Acutime antenna (requiring the TSync board to be configured as a TSyncE, external GNSS receiver)
- 2) and the firmware in the existing TSync board is updated at the factory, or in the field, to version 3.4.9
- 3) and the Acutime is programmed at the factory for NMEA output (instead of TSIP)- our internal P/N: E025R-9000-0001

The Acutime 360 antenna is now compatible with the TSync board. Can you confirm?

2. Trimble Acutime GG Smart Antenna (GPS / GLONASS / QZSS)

(More recent TSAT series GNSS antenna)



- **Trimble P/Ns:**

- **92626-05** for the newer **Multi GNSS** (GPS/Glonass/QZSS) version of this antenna
- **92626-00** (earlier **GPS-only** receiver) (now discontinued from Trimble- replaced by Acutime 360)

from <http://www.dpie.com/gps/timing/trimble-acutime-gg-smart-antenna>

92626-00 12-channel, RS-422 Acutime GG **GPS only** RS-422 smart antenna

92626-05 12-channel, RS-422 Acutime GG **Multi GNSS** RS-422 smart antenna

- **Our P/N for the raw, unprogrammed multi-GNSS antenna** (as we receive it from the supplier):

- **For Trimble 92626-00 (GPS-only):** **E025R-0004-0003** (in Arena at: https://app.bom.com/items/detail-spec?item_id=1202842906&version_id=10221223478)

Note (1 Aug 18): not confirmed, but it appears our P/N is the same for both the GPS-only and for the multi-GNSS antenna.

- **Our programmed P/Ns** (for TSAT boards)

For TSAT-PC104 and TSAT-PCI-U series: 1186-0000-5000

Note: As of at least 8 Nov 2018, we are still shipping Acutime GG antennas. Per Dave Sohn, Engineering has some “software” requirements for the newer Acutime 360 antennas, before we can cut-over to the 360s.

- **We program the antenna here for TSAT-PCI-U, TSAT- PC104** (we switch the Acutime-GG antenna from using TSIP protocol to instead use **NMEA** protocol, which is the protocol the legacy TSAT boards use.

➤ Acutime Data sheet:

➤ **Acutime GG User Guide:** (http://trl.trimble.com/docushare/dsweb/Get/Document-621953/Trimble_AcutimeGG_UG_1H.pdf)

Specs / Information for the Acutime GG Smart antenna

Acutime GG Smart Antenna




Highlights

- Multi-GNSS (GPS, GLONASS, QZSS)
- Improved Sensitivity
- Assisted GPS (A-GPS)
- Reduced TTFF (Time-To-First-Fix)
- Timing pulse synchronized to within 15nanoseconds (one sigma) of GNSS/UTC
- Weatherproof and corrosion resistant housing

Product Information

 [Data Sheet](#)

 [Where to Buy?](#)

 Timing@trimble

Timing

Solutions

- [Base Station Timing](#)
- [Manufacturing Test](#)
- [Frequency Reference](#)
- [Calibration Laboratories](#)
- [Traceability](#)
- [GPS Time Reference](#)
- [Custom Timing Solutions](#)

Acutime GG, Multi-GNSS Smart Antenna

The Trimble® Acutime™ GG Multi-GNSS (GPS, GLONASS, QZSS) smart antenna is the latest generation Acutime product of integrated GNSS technology in a rugged and weatherproof self-contained unit. The Acutime GG is an integrated pipe thread-mounted multi-GNSS receiver, antenna and power supply solution in a single environmentally sealed easy to install enclosure.

The Acutime GG multi-constellation smart antenna design continues Trimble's line of GPS smart antennas, which have been in production since 1991.

This antenna is the perfect solution for precise timing and network synchronization needs, including broadband wireless applications. It provides an extremely cost-effective and independent (within the firewall) timing source for any application, such as fault detection systems and synchronization of wireless networks.

Key Features & Benefits

Parts & Accessories

Support

Key Features:

- Multi-GNSS (GPS, GLONASS, QZSS)
- Improved Sensitivity
- Assisted GPS (A-GPS)
- Reduced TTFF (Time-To-First-Fix)
- Timing pulse synchronized to within 15nanoseconds (one sigma) of GNSS/UTC
- Weatherproof and corrosion resistant housing

Max cable length

- From the Trimble Acutime-GG user manual “For custom-length cables of up to 550 m (**1800 feet**), contact Trimble”

Pin-out info

Serial port interfaces

The pin-out descriptions and color codes for the standard un-terminated cables and DB-25 interface cable are as follows:

Acutime GG Connector	Wire Color	Function	DB-25 Interface	Protocol
Pin 1	Red	DC Power	Pin 1	+5 VDC to +36 VDC
Pin 2	Violet	Port B: Receive -	Pin 25	TSIP RS-422
Pin 3	Orange	Port B: Receive +	Pin 13	TSIP RS-422
Pin 4	Brown	Port B: Transmit -	Pin 11	TSIP RS-422
Pin 5	Yellow	Port B: Transmit +	Pin 23	TSIP RS-422
Pin 6	White	Port A: Receive -	Pin 24	Not Used
Pin 7	Gray	Port A: Receive +	Pin 12	Not Used
Pin 8	Green	Port A: Transmit -	Pin 10	NMEA / TSIP RS-422
Pin 9	Black	DC Ground	Pin 7	Ground
Pin 10	Blue	Port A: Transmit +	Pin 22	NMEA / TSIP RS-422
Pin 11	Orange w/ white stripe	1 PPS Transmit +	Pin 21	RS-422
Pin 12	Black w/ white stripe	1PPS Transmit -	Pin 9	RS-422

Communication protocols (TSIP/NEMA-0813) / programming the Acutime-GG antenna

- **TSIP:** The **Trimble Standard Interface Protocol (TSIP)** consists of command packets and report packets,

C) GG TSIP protocol

- Factory default/standard protocol setting for the Acutime-GG antenna is “**TSIP**” protocol
- TSync boards are configured in their EEPROM to use **TSIP** protocol to communicate with its external receiver. So we can send the Acutime-GG antennas out “unprogrammed”, when it’s being used with TsyncE boards

D) NMEA protocol

- All “Legacy” **TSAT** timing boards communicate with their external receiver using **NMEA** protocol (not TSIP protocol)
- So we reprogram the Acutime-GG antennas here at the factory for **NMEA-0813** when they are being used with TSAT boards.

Summary of the Acutime-GG replacing the earlier Acutime Gold Smart antennas:

- The Acutime-GG antenna uses a different Model receiver (Res-SMT-GG) which can track GPS and Glonass satellites
- The Acutime-GG antenna has better sensitivity than the earlier Acutime Gold, to be able to track weaker signals.

Compatibility of the Acutime-GG antenna with Spectracom Timing boards

1. To use the Acutime-GG GNSS antenna with the TSAT series timing board, a firmware upgrade of the TSAT board may be required (at least firmware version 2.11)

Note: A TSAT board firmware upgrade to version 2.11 is required for earlier version TSAT boards for it to be compatible with this newer GNSS (GPS and Glonass capable) antenna. This newer Acutime-GG antenna is compatible with:

- **TPRO/TSAT-PCI-U-2 and TPRO/TSAT-PCI-66U** boards with firmware version 2.11 or higher installed (Refer to ECN 3257, July 2013)
- **TPRO/TSAT-PC104** boards with firmware version 2.11 or higher installed (Refer to ECN 3283, Aug 2013)

2. Desire to use the newer Acutime-GG antenna with a TsyncE-PCIe board (external receiver)

- Refer to knowledge base article excerpted further below and in Salesforce at:

There have been two variants of the **Acutime-GG Smart** antennas:

- The **first** edition was a **GPS-Only** antenna (Trimble P/N 92626-00 and Spectracom P/N **E025R-0004-0003**)
- The **second/current** edition is a **Multi-GNSS** (GPS/Glonass/QZSS) antenna (Trimble P/N: 92626-05).

Note: The predecessor to the Acutime-GG antennas was the **Acutime Gold Smart** antennas (Trimble P/N: 55238-00, Spectracom P/N **E025R-0004-0002**)

As also discussed below (as an FAQ), older TSyncE-PCle boards needed a firmware update to at least **firmware version 2.2.1 (verified with the LS_GetVersion 0 call)** to be compatible with the Acutime-GG Antennas. TSync firmware versions prior to version 2.2.1 are only compatible with the earlier Acutime Gold Smart antennas (not compatible with the Acutime-GG antennas)

TSync firmware version 2.2.1 was released on 18 March 2013. The TSync Serial Number cut-in for TSync boards shipping from the factory with version 2.2.1 (or a newer version) installed were **Serial Numbers 2247, 2251 and higher.**

edited Knowledge Base Article

Q. Do I need a timing board firmware update when replacing a smart antenna for my TSAT or TSync?

Note: This article applies to bus-level timing boards that utilize an external GPS/GNSS antenna-receiver combination.

A Spectracom bus-level timing boards can be synchronized via global navigation satellite signals. In 2014, a design update included a new antenna-receiver, Trimble's Acutime GG, which replaced the end of life Acutime Gold. When replacing an antenna-receiver for a Spectracom timing board manufactured prior to 2014 with the current Acutime GG, use these guidelines as the antenna-receiver may require an update to the board's firmware. Contact the factory to determine if a board manufactured in 2014 requires the update. Any board manufactured in 2015 or later will be compatible.

In all cases, the Acutime GG is programmed specifically for the Spectracom model it is intended for, so the model must be known when placing an order for a replacement antenna.

TSyncE-PCle or TSync-PCle-0Y2 (any model that ends in '2'): requires an update to at least **version 2.2** firmware. This update can be applied in the field via the Spectracom driver.

TSAT-PCI-U-2, TSAT-PCI-66U, or TSAT-PC104: requires an EPROM update for any unit manufactured before 2014 - return to the factory or consider replacing the board with a newer one. May require an update if manufactured in 2014 (contact factory). You can determine if an update required by checking the firmware version via the driver. Any version before 2.11 (July 30, 2014) requires an update.

TSAT-cPCI or TSAT-PMC: no action required - the new antenna-receiver is compatible with the hardware design of any fielded unit.

Important Note (original written 29 Jan 2014 KW and modified on 1 Aug 2018) TSync firmware **update version 2.20** has been released for TSync-PCle boards, This Acutime-GG antenna will not work properly with the TSync timing boards, if an earlier firmware version is still installed in the TSync board.

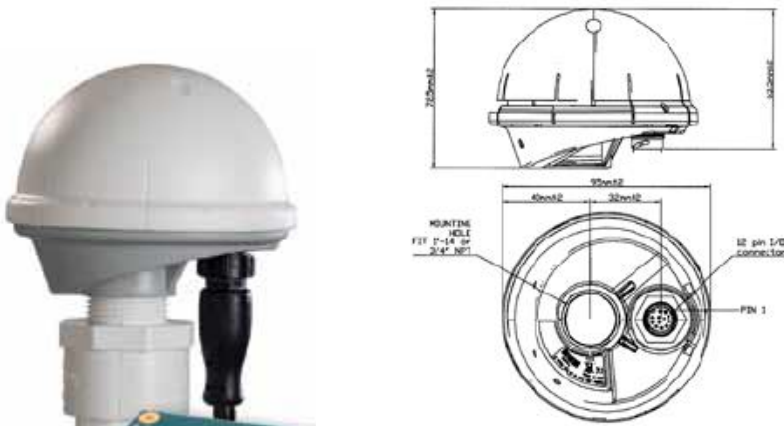
The Trimble P/N for the earlier style antenna (**Acutime Gold Smart**) which is compatible with earlier TSync firmware is 55238-00 (refer to "B" below)

Associated antenna mast:

P/N: 1159-0000-0700 (in Arena) https://app.bom.com/items/detail-spec?item_id=1202841005&version_id=10221291538&orb_msg_single_search_p=1&redirect_seqno=6678014486

3. **Acutime Gold Smart GPS Antenna (discontinued)**

- **Trimble P/N:** 55238-00 (in Arena at: https://app.bom.com/supplier-items/detail-spec?item_id=1203069067&orb_msg_single_search_p=1)
- **Our Raw P/N:** **E025R-0004-0002**
- **Our programmed P/Ns:**
For TSAT-PCI-U, TSAT-PC104, TSAT-PC: 1159-0000-5000
For TSAT-VME: 1156-0000-5000



- Was replaced by the newer Acutime-GG (GPS and Glonass) antenna
- GPS-only antenna for TSAT-PCI-U boards (does not support other constellations, sync)

Programmed for TSAT-PCI-U, TSAT-PC-104 and TSAT-PC

Trimble P/N: 55238-00

- Our raw P/N for the raw antenna: E025-0004-0002
- Our programmed P/N for PCI-U, PC104, PC: 1159-0000-5000

Links/shortcuts

- **Link to Trimble website:** <http://www.trimble.com/timing/acutime-gold-gps-antenna.aspx?dtID=features>
- **Link to Trimble data sheet:** http://trl.trimble.com/docushare/dsweb/Get/Document-366428/022542-002_Acutime_DS_0207_lr.pdf
- **Link to Acutime User Guide:** <http://www.trimble.com/timing/acutime-gold-gps-antenna.aspx?dtID=features>

Important Note (22 Sept 2014) This Model is no longer available from Spectracom! Refer to **ECO-000026** (in Arena) for more info.

Based on Purchase history, these antennas appear to have started shipping around **Oct/Nov 2007**

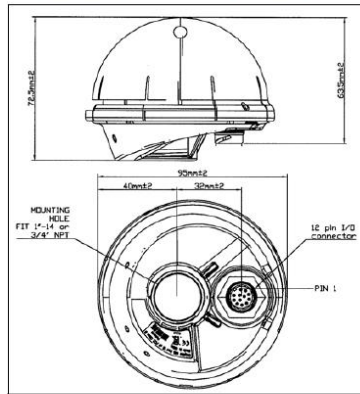
Specs: Operating temp -40C to +85C

Mobile mode operation: We do not program these antennas to support mobile applications. It should only be used in stationary applications only.

Dimension drawing

- From the Acutime User Guide: <http://www.trimble.com/timing/acutime-gold-gps-antenna.aspx?dtID=features>

The following diagram shows the module dimensions of the Acutime Gold:



PHYSICAL CHARACTERISTICS

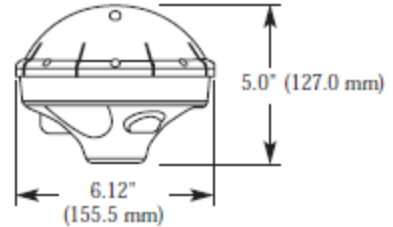
Dimensions: 6.12" D, 5.0" H (155.5mm x 127.0mm)

Weight: 12.8 oz (363 g)

Connector: 12-pin round, waterproof

Mounting: 1"-14 straight thread

Mechanical Drawing:



Serial port interfaces

The pin-out descriptions and color codes for the standard unterminated cables and DB-25 interface cable are as follows:

Acutime Gold connector	Wire color	Function	DB-25 interface	Protocol
Pin 1	Red	DC Power	Pin 1	+5 to +36 VDC
Pin 2	Violet	Port B: Receive -	Pin 25	TSIP RS-422
Pin 3	Orange	Port B: Receive +	Pin 13	TSIP RS-422
Pin 4	Brown	Port B: Transmit -	Pin 11	TSIP RS-422
Pin 5	Yellow	Port B: Transmit +	Pin 23	TSIP RS-422
Pin 6	White	Port A: Receive -	Pin 24	Event Input
Pin 7	Gray	Port A: Receive +	Pin 12	Event Input
Pin 8	Green	Port A: Transmit -	Pin 10	NMEA / TSIP RS-422
Pin 9	Black	DC Ground	Pin 7	Ground
Pin 10	Blue	Port A: Transmit +	Pin 22	NMEA / TSIP RS-422
Pin 11	Orange w/ white stripe	1 PPS Transmit +	Pin 21	RS-422
Pin 12	Black w/ white stripe	1PPS Transmit -	Pin 9	RS-422

4. Trimble Acutime 2000 Smart Antenna (the original KSI TSAT-PCI 5V antenna) (discontinued)

- Trimble P/N: 39091-00
- Our Raw P/N: E025R-0004-0001
- Our programmed P/Ns:

For cPCI and PMC: 1141-0000-5000



- The Acutime 2000 Smart antennas were the first Acutime antennas, for the original KSI TSAT-PCI 5V boards
- Link to datasheet: https://www.artisan-g.com/TestMeasurement/79079-1/Trimble_ACUTIME_2000_GPS_Smart_Antenna
- Based on Purchase history, these antennas appear to have shipped from January, 2006 until around October/ November 2007.
 - **Trimble P/N:** 39091-00
 - **Programmed for** TSAT-PCI
 - **Our Raw P/N:** E025-0004-0001
 - **Our programmed P/N:** 1141-0000-5000

Mobile mode operation: We do not program these antennas to support mobile applications. It should only be used in stationary applications only.

Used with Legacy TSAT Timing boards and TSyncE-PCIe timing boards (with external GPS receiver). Note this antenna is not used with TSyncI-PCIe boards (which have the GPS receiver attached to the TSync board).

Email sent to Jim Russell at Goodrich on 9/1/10 The GPS antenna specifications for the Spectracom TSAT-PCI-66U bus-level timing boards, the GPS antenna specifications are contained in Table 2.10, page 2-3 of the TSAT-PCI-66U user manual (attached, in case you don't already have a copy of this document). For your convenience, I have pasted this table below:

Table 2.10—GPS Receiver/Antenna Specifications	
Number of Satellites	6
Acquisition Time (cold start)	1 minutes typical
Re-acquisition Time	<1 minute
Frequency	L1 frequency, C/A code (SPS), continuous tracking receiver, static overdetermined clock mode (default)
Sync to UTC	Within 15 nanoseconds (static)
Accuracy Horizontal Position	<8 meters (50%) <9 meters (90%)
Accuracy Altitude Position	<11 meters (50%) <18 meters (90%)
Altitude	0 m to +18,000 m (0 to +59,055 feet)
Size	3.74" D, 2.85" H (95mm x 72.5mm)
Weight	5.4 oz (154 g)
Pole Mount	1"-14 straight thread or 3/4" pipe thread
Operating Temp	-40° to +65° C (-40 to +185 °F)
Storage Temp	-55° to +105° C (-67 to +221 °F)
Operating Humidity	95% RH, non-condensing @ 60 °F

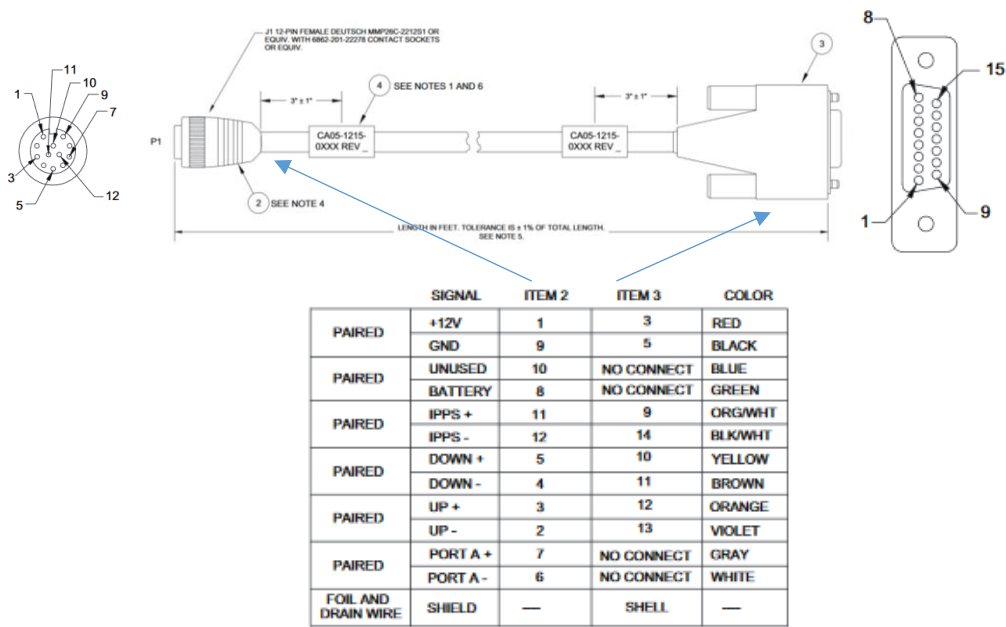
Note that this GPS antenna is a receive-only antenna. EMI interference is limited to the active components inside of the antenna (minimal EMI interference). Multiple GPS antennas can be installed near each other with minimal separation required.

Known issues with Acutime 2000 antennas

A) “1997” year issue now occurring with Acutime 2000 antenna’s

- (Oct, 2016) Invensys/Schneider Electric reported TSAT boards with an Acutime 2000 antenna are now being set to a year of “1997”.
- Solution is to replace the Acutime 2000 antennas with Acutime GG antennas. This requires any TSAT board having firmware version prior to 2.11 be returned to the factory for firmware update. Versions prior to v2.11 are not compatible with Acutime GG antennas.
- Refer to “TSAT Firmware update needed when using a newer Acutime GG” in the Timing board assist doc for more details on this antenna swap-out.

Antenna cable (CA05-1512-0100 and CA05-1512-0200) pin-out:



Link to our datasheet: We don't currently have one, as far as I am aware:

Acutime 100 foot extension cable

- Our P/N:CA05-1515-0100
- For more info on this 100 ft extension cable, refer to “CA05-1515-0100” in the Timing board assistance doc:

TSAT-Dome antenna (Acutime antenna) mounting:

The TSAT dome antenna is attached to a Schedule 40 PVC mast with a 1 5/16 inch outside diameter. The top of the mast assembly has a 1 inch threaded mating connector which screws into the bottom of the antenna. The mast assembly has a groove in it, so the antenna cable can be threaded up the inside of the mast assembly to the top of this connector. The mast is approximately 20 inches long.

The mast assembly includes two metal hose clamps (approximately 18 inches long) that can be wrapped around the mast assembly to attach it to a stantion on the roof (such as a metal railing, vent duct, etc) for vertical mounting of the mast assembly. Spectracom also offers the Model 8213 flat-roof mount which is a weighted-base/stand (like the umbrella stands used with for tables) that the mast assembly can slide into to keep it standing straight-up. The Figure below shows the Model 8213 at the bottom of the mast assembly (this picture shows the Model 8225 GPS antenna attached to the top of the mast, instead of the TSAT dome antenna, but the TSAT dome antenna is mounted in the same fashion).



Acutime Antenna programming

- Acutime antennas for TSAT boards are programmed using TeraTerm and an RS-485 to RS-232 converter (programming needs to be verified or performed at the factory).

The Acutime antenna that is used with the TSAT bus-level timing boards are pre-programmed at the factory to inter-operate with a specific Model of TSAT Timing board. For example, they can be pre-programmed to work with a PCI-U board, or they will be programmed differently to operate with a cPCI board, instead (The programming of the antenna changes the baud rate at which the GPS receivers communicate with the timing boards). The programming for use with the cPCI boards is not the same as the programming for the PCI boards, so the GPS antennas are not cross-compatible with other types of boards of which the antenna was not pre-programmed for at the factory.

They will need to purchase additional antennas that are pre-programmed to operate with either PCI boards or with cPCI boards, as specified in the order. Just changing the pin-out of the connector will allow it the antenna to be able to operate with either board type.

The only exception to the need to have the antennas pre-programmed is with the TSync-PCIe boards. The boards themselves program the GPS antennas when they are first connected, so the antennas do not have to be pre-programmed for this board. The "caution" is if a customer happens to have a mix of TSAT and TSync-PCIe boards, if they move a GPS antenna from a TSAT board to a TSync board, the antenna will be re-programmed for TSync-PCIe operation and will not operate again with a TSAT board unless it's returned to us for reprogramming.

The "more recent" Acutime antennas will have a Part Number label applied to the antenna to indicate what type of timing board it has been pre-programmed to operate with. The following are the Part Number for the pre-programmed GPS antennas:

- **1159-0000-5000:** Programmed for TSAT PCI-U, TSAT-U-2, TSAT-66U, TSAT-PC104 and TSAT-PC
- **1156-0000-5000:** Programmed for TSAT-VME timing boards
- **1152-0000-5000:** Programmed for TSAT-cPCI and TSAT-PMC timing boards

Feb 29th rollover issue with GPS antenna (Acutime 2000).

Sigrid, (March 2008).

Between 2000 and 2005 you purchased 367 ea. of the 39091-00 Acutime 2000.

Acutime 2000, build date of 2000 started with version 2.02 up until July 2005 with a firmware release of 3.06 but NO PART NUMBER CHANGE.

There is a firmware issue with the original version 2.02 of Acutime 2000 that will indicate the leap day, Feb 29, to be reported as March 1.

That is, in protocol msg (Remove TSIP, NMEA) that use the Day/Month/Year format, for leap years, both Feb 29 and March 1 are reported as March 1 (Month 3, Day 1).

This problem only affects the reported date and does not affect Acutime timing outputs.

The problem is present in all FW versions that support the original Acutime 2000 HW with old flash part.

The problem is not present in the latest FW version - v3.06 - for Acutime 2000 with updated flash.

However, v3.06 is not backward flash compatible with the flash part on the original Acutime 2000 version 2.02 due to a component change. Simply stating, the version 3.06 ROM file cannot be uploaded to the older version 2.02 units.

The fix is to have the customer purchase a new antenna.

Acutime vs. Older GPS antennas

KSI had two types of antennas for the TSAT boards. The older antennas were Trimble part number 34104-62. These were replaced by the Acutime 2000 antennas. The two antennas are different. Changes had to be made to the TSAT boards to use the new Acutime antennas. Therefore, the new antennas are not compatible with the old antennas.

****Non-Spectracom ANTI-JAM GPS Antennas**

******Novatel Model GAJT antenna**

- **Refer to:** <http://www.novatel.com/products/gnss-antennas/gajt/>
- Pronounced “gadget”)
- These antennas are NOT available from Spectracom
- Good for localized GPS jamming
- Very expensive antenna

Email from Lisa Perdue (1 Dec 14)

The GAJT is about 25k-27kUSD if I am remembering correctly.

Keith is right in that if the jamming is right on top of the antenna will not be able to block it, but normally the jammers are not that close and the antenna will work. It would probably work well for the type of jamming we suspect is happening at the Harris site.

Because of that jamming situation and the potential for others, Spectracom has been working on a lower cost solution for our customers. We are working with a partner company to develop an antenna using a similar approach to the GAJT antenna, at less than half of the cost of the GAJT and that would be directly compatible with our NetClock and SecureSync products (no additional integration work by the customer is needed).

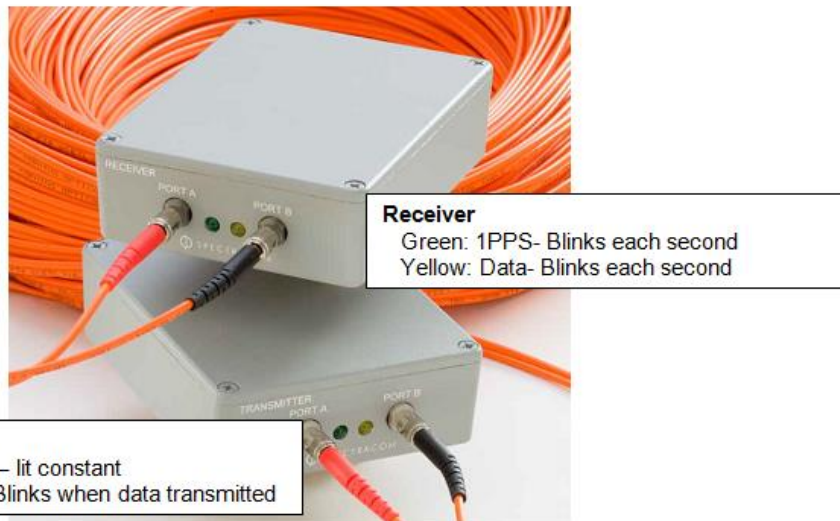
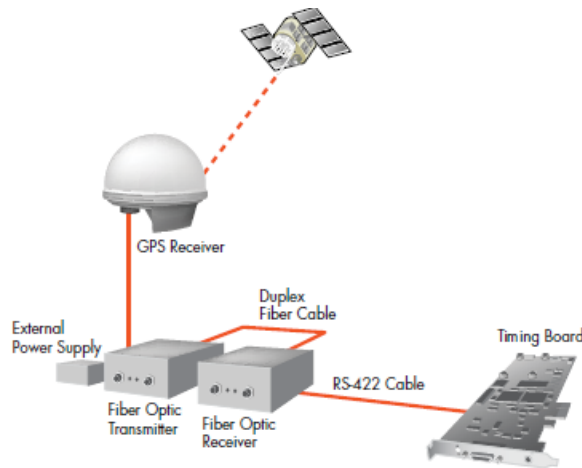
If you would like to discuss this project further, I am copying our CTO, John Fischer, on this email. He would be the point of contact for discussion on our new product.

Model 1169 GPS Fiber Optic Isolator (TX and RX) for GPS:

- Fiber Optic isolators (for Invensys/Schneider electric) to run the Acutime GPS antenna long distances from a TSAT timing board

1. **Refer to datasheet:** [I:\Marketing\ Product Data Sheets \(archive\)\Bus-Level Timing Boards](I:\Marketing\ Product Data Sheets (archive)\Bus-Level Timing Boards)
2. **Refer to manual (1169-5100-0050) in Arena:** https://app.bom.com/items/detail-spec?item_id=1203165689&version_id=10221246188
3. **Link to other information:** <I:\Engineering\Archive\Released\1169 - GPS Optic Isolator>

Note: These devices are Spectracom-produced parts (non-serialized)



Function:

The fiber optic technology that is used in the GPS Optic Isolator units eliminates the risk of equipment damage due to lightning or other high voltage interferences. Frequently, telecom applications require this type of solution, which eliminates the need for costly lightning arrestors.

Part Numbers

Ordering Information

GPS Optic Isolator Kit: Model P0972VZ



Spectracom P/N	Description
1169-TXFO-0600	GPS Optic Isolator TX (Transmitter)
1169-RXFO-0600	GPS Optic Isolator RX (Receiver)

Input power

Optic Transmitter (P/N 1169-TXFO-0600)

1. Uses External Power Supply
2. **Input:** 90 V to 264 V AC, 50 Hz to 60 Hz
3. **Output:** 12 V DC 600 mA or better

Optic Receiver (1169-RXFO-0600)

1. Powered by 15 pin connector on TSAT timing board, via supplied cable

Ports (on both the Optic TX and Optic RX)

A (Green): For 1PPS data from Acutime antenna

B (Yellow): For RS-485/RS-422 Data from Acutime antenna

Fiber cable used between TX and RX:

2. Uses Duplex with ST connectors
3. Max fiber cable distances: Fiber cable can be up to 500 meters (1640 ft) long (between Optic Transmitter and Optic Receiver)
4. (2) 100 meter (653 ft) fiber cables supplied (One for 1PPS and one for RS-485)

LEDs:

A) OPTIC TRANSMITTER (P/N 1169-TXFO-0600)

The **green** LED indicates power. It should illuminate continuously. If the green LED does not illuminate green, check the power supply.

The **yellow** LED will blink when data is transmitted on Port B.

OPTIC RECEIVER (P/N 1169-RXFO-0600)

The **green** LED will blink every second.

The **yellow** LED should blink in synchronization with the yellow LED (Port B) of the Transmitter unit.

Symmetricom/Microsemi GPS/GNSS antennas (for use with SecureSyncs/NetClocks)

A) Symmetricom/Microsemi Model 142-614-50 / AT575-142 antennas



Symmetricom SyncServer GPS
Antenna 5V-12V 142-614-50



Symmetricom AeroAntenna GPS
12dB 5V MCX Antenna

- This is a “12vdc” (L1 band only) antenna from AeroAntenna
 - Apparently, it will accept 5 to 18 VDC power- per <http://80.243.176.74/new-symmetricom-142-614-50-at575-12v-i509936/> “This antenna will also work equally well with receivers supplying 5V”
 - **Power:** “25 mA @ 5V-12V (supplied by card)”.
- It apparently has a BNC Connector, while we use a type N connector. So, an adapter will be needed.
- It reportedly has **41dB gain** (per <http://www.prostudioconnection.com/Symmetricom-SyncServer-GPS-Antenna-5V-12V-142-614-p/232517452228.htm> “Gain 41dB”)

Specs

L1 GPS Antenna AT575-142

Technical drawing of the L1 GPS Antenna AT575-142. It shows a side view and a top view. Dimensions include a 3.00 inch diameter for the antenna head, a 1.25 inch height, and a 1.30 inch width. It also shows a 0.5 inch diameter for the mounting hole and a 0.5 inch diameter for the antenna head. A note indicates that all measures are in inches and 1 inch equals 2.54 cm.

The GPS antenna AT575-142 from AeroAntenna Technology, Inc. is a high-quality low cost single frequency GPS antenna with integrated ground plane, ideal for pole mounting.

Options:

- amplification (gain) ± 2 dB: 00 (passive), 12 dB (20 mA), 26 dB (35 mA), 40 dB (50 mA), other on request
- input voltage: 5 - 18 VDC
- HF connector: TNC male, BNC male, other on request
- 3/4" NPT internal thread for mounting

Applications:

- Marine and land navigation
- Hydrographic surveys
- Survey
- Machinery control
- GPS deformation monitoring
- GPS Timing Receiver

Specification

Frequency	1575 \pm 10 MHz	Amplifier		Finish	weatherable Polymer
Polarization	right hand circular	Noise figure	max. 2,5 dB	Dimensions	\varnothing 76,1 mm x 80,5 mm
Axial Ratio	max. 1,5 dB	Impedance	50 Ω	Weight	max. 227 g
Radiation Coverage	4,0 dBic 0° = 0° - 3,0 dBic 0° < θ < 75° - 7,5 dBic 75° \leq θ < 80° - 8,0 dBic 80° \leq θ < 85° - 9,0 dBic 85° \leq θ = 90°	VSWR	< 2.0 : 1	Operating Temperature	- 55°C to + 85°C
		Band rejection	30 dB @ 1535 MHz, 60 dB @ 1615 MHz	Designed to	DO-160C
		Power handling	1 Watt		

Q We are spooling up to replace eighteen ancient MicroSemi (Symmetricom) S200s & S350s with good, ecologically responsible Spectracom NetClock 9400s with organically sourced free-range Rubidium from right here in the good ol' USA.

Are the GPS antennas (antennae ?) from the MicroSemi appliances compatible with the Spectracom units. We have already purchased the Spectracom antenna install kits, but in the interest of the end-of-year "Git 'er Done" imitative from upper management, can we limp by with the existing GPS antenna hardware?

Boiling water with Uranium was my Navy specialty, so I am not up on satellite antenna specifications. Since they are the same source for the same signal I'd like to think they are interchangeable, but then VHS vs. Beta-Max...

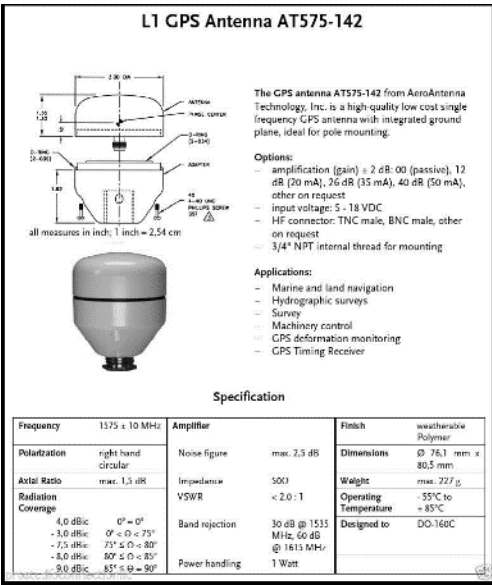
A **From Dave Lorah (14 Nov 17)** I am glad you are pursuing the humane action of installing new SecureSync Appliances in your systems.

The Symmetricom antennas are 12VDC powered. I believe their model number is 142-614-50 or AT575-142. If that is true it will accept 5 to 18 VDC power and (maybe) should work on our SecureSync 5VDC systems. I believe it will but to my knowledge it has never been tried.

They use a BNC Connector and we use a type N connector, so an adapter will be needed. There is the question of cable loss and if there is enough gain in those antennas to overcome long cable lengths. I think if the cables are under 100 feet it should work. Again, the only way to know is to try one and see.

But no harm will be done to the SecureSync (9400) if you connect these antennas.

Here is a data sheet I found on EBAY.



GPS/GNSS COMBINERS / SPLITTERS / SURGE SUPPRESSORS / PREAMPS / FILTERS

GPS/GNSS Combiners

Note: (per Keith, as of at least Nov, 2017) I don't believe we currently offer any GPS/GNSS Combiners. The Info below, for a combiner from GPS Source, was for a project Lisa Perdue was building and not for us to offer for resale.

- **Refer to** (in Arena): https://app.bom.com/items/detail-spec?item_id=1227762132&version_id=10643947668&
- Our P/N for the raw combiner: E025-0003-0026
- **Mfg and P/N:** GPS Source C21A-SF-S

Description: 1-2GHz combiner for GNSS signals, DC Blocked on output port.

Model 235896: 2/4/8 way GPS power splitter for Epsilon Clocks



- 2/4/8-way GPS splitter shipped out of Spectracom France for Epsilon Clock products (such as EC20S, EC22S, etc)
 - 2-way splitter -reference : SP1-T2
 - 4-way splitter : reference : SP1-T4
 - 8-way splitter : reference : SP1-T8
- Spectracom P/N: 235896
- **In Arena:** app.bom.com/items/detail-whereused?item_id=1227131403&version_id=10632170538
- **In Salesforce:** not in Salesforce
- **Shortcut to datasheet** (in Arena): https://app.bom.com/items/detail-spec?item_id=1227131403&version_id=10632170538

Specs

IP rating: IP50

Gain

Gain in the GPS band The gain is negative since the product is passif:

- 2-way = - 3,5 dB,
- 4-way = - 7,5 dB,
- 8-way = - 10.5 dB

**Model 8224 GPS Splitters

- **Shortcut to Model 8224 Data Sheet:** (on our website or in Sharepoint)
- **Shortcut to Manufacturer's Data Sheets (GPS networking ALDCB, L1 LDCB, etc) :**
<I:\Engineering\Engineering Shared\Spectracom parts\E025-xxxx-xxxx>

International shipping Regulations (HTS code, EAR and ECCN Number)

- Refer to (in this document): [Export control \(HTS and ECCN numbers\) for all products](#)

For all Model 8224s

Regulation: EAR

ECCN: 7A994

US/Europe HTS code: 8517.62.0050

Variants of the Model 8224 GPS splitters (Configurations/Part numbering scheme)

- **Shortcut to list of all Model 8224 variants in Salesforce:**
<https://na28.salesforce.com/ui/search/ui/UnifiedSearchResults?searchType=2&sen=00a&sen=0F9&sen=a04&sen=02i&sen=ka&sen=00O&sen=00Q&sen=001&sen=003&sen=a0A&sen=01t&sen=005&sen=500&sen=006&sen=810&str=8224#/fen=01t&initialViewMode=detail&str=8224>

Inputs:Outputs	1:2	1:2	1:4	1:4	1:8	1:8
Typ Insertion Loss/Gain ¹	-5.5 dB	22 dB	-8.5 dB	18 dB	-10.5 dB	4.5 dB
Max Footprint (not including connectors) ²						
Length	3.25" / 82.5 mm		3.94" / 100 mm		7.09" / 180 mm	
Width	2.5" / 63 mm				3.35" / 85 mm	
Height	1.3" / 32 mm					
Max Weight	10 oz / 286 g		11.8 oz / 340 g		16.2 oz / 459 g	

¹ Gain via internal amplifier requires power source.

² Contact factory if dimensions are critical to your installation.

Ordering Information

Model

8224-ABCDE

A	B	C	D	E
Number of Outputs	DC-blocked Outputs	Amplifier	5VDC on Input	External Power
2 4 8	1-DC-pass one output 0-DC-block all	1-Yes 0-No	5-Yes 0-No	0-None 1-9-32VDC customer supplied 2-110 VAC with USA plug 3-220 VAC with EU plug 4-240 VAC with UK plug

*As our source of supply may change, these specifications are considered typical and subject to change without notice. If you have a specific requirement, contact us so we can be sure to supply you a splitter with the exact specifications needed for your application.

November 20, 2014 - 8224(H)

Specifications subject to change or improvement without notice.

- Power connectors for external input power splitters (“110”, “220”, “240” or “DC”)

Network Power Supply		
Source Voltage Options	VOLTAGE INPUT	STYLE
	110VAC	Transformer (Wall Mount)
	220 VAC	Transformer (Wall Mount)
	240 VAC (United Kingdom)	Transformer (Wall Mount)
	Customer Supplied DC 9-32 VDC	Military Style Connector

Note: DC connectors are MIL-STD-704 or MIL-STD 1275B compliant

Screenshot below is from: <https://www.gpsnetworking.com/faqs/poweroptions>

Power Options

All of the products offered by GPS Networking can be configured to support common power source specifications. Currently, we offer the following power source options for our powered products.

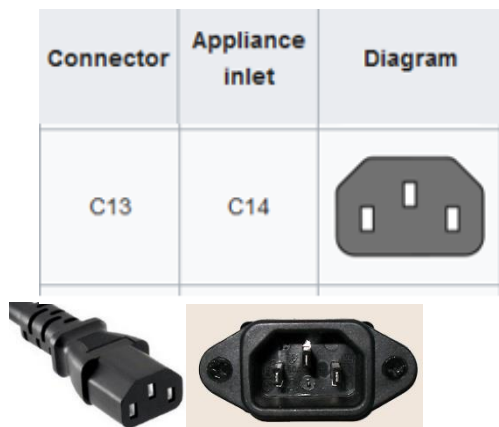


STANDARD MILITARY DC CONNECTOR (MC OPTION)



Input voltage range: 9 – 32 VDC

Desire to use C13/C14 power connectors for Model 8224 splitter



**(Model 8224 shown with two prong 110VAC
US/North America power connector)**

Q In the DC they're only going to have PDU's that support C13/C14 output connectors. Can you confirm if your adapter supports a power lead that can interface with that? If not, can you supply a US power lead and do you do a US power connector to an IEC320 C13/C14 PDU output as an adapter?

Note: Splitters listed in the table further below in red text provide amplification (signal gain for a “built-in” 8227)

Note: if the “GPS splitter description” field is highlighted in yellow, it’s not a DC-pass-through splitter (it has external input power)

Note: The chart below (from the 8224 datasheet) indicates the breakdown for each of the five numbers after “8224” (such as 8224-21050):

Ordering Information

Model

8224-ABCDE

A	B	C	D	E
Number of Outputs	DC-blocked Outputs	Amplifier	5VDC on Input	External Power
2 4 8	1–DC-pass one output 0–DC-block all	1–Yes 0–No	5–Yes 0–No	0–None 1–9-32VDC customer supplied 2–110 VAC with USA plug 3–220 VAC with EU plug 4–240 VAC with UK plug

Is there 5vdc present from the GPS/GNSS receiver to the splitter?

Our Model Number	Our Part Number	GPS splitter Description (green is external input power)	Gain (dB)	Simulates antenna connected	GPS Networking P/N (unless otherwise noted)	Link to datasheet
8224-20000	E025-0003-0030	Passive GPS Splitter, 1:2, DC-block all ports (No Power supplied to the RF input)	N/A	yes	LDCBS1X2-N-all ports blocked for DC	https://app.bom.com/items/detail-spec?item_id=1233695065&version_id=10754894208
8224-21050	E025-0003-0001	1:2,no amp	N/A	yes	LDCBS1X2-N	https://app.bom.com/supplier-items/detail-spec?item_id=1203306198
8224-80152	E025-0003-0002	1:8,amp,iso,110V transformer (US)	45dB	yes	NHI-ALDCBS1x8-N/5/110	https://app.bom.com/supplier-items/detail-spec?item_id=1203306199
8224-41050	E025-0003-0003	1:4,no amp	N/A	yes	LDCBS1X4-N	https://app.bom.com/bom-auth/detail-download/4ZoWxo/1747089176/LDCBS1X4.pdf
8224-20151	E025-0003-0004	1:2,amp,DC	20dB	yes	NALDCBS1X2-N/5/MC	https://app.bom.com/supplier-items/detail-spec?item_id=1203306201
8224-20052	E025-0003-0005	1:2,no amp,110V	N/A	yes	NLDCBS1X2-N/5/110	https://app.bom.com/bom-auth/detail-download/4sWKIL/1747089497/LDCBS1X2.pdf
8224-40052	E025-0003-0006	1:4,no amp,110V	N/A	yes	NLDCBS1X4-N/5/110	https://app.bom.com/bom-auth/detail-download/sTsUTn/1747089176/LDCBS1X4.pdf
8224-20152	E025-0003-0007	1:2,amp,110VAC	20dB	yes	NALDCBS1X2-N/5/110	https://app.bom.com/bom-auth/detail-download/D9S0h6/1747089313/ALDCBS1X2.pdf
8224-40152	E025-0003-0011	1:4, 110VAC	16dB	yes	GPS Source P/N: S14-A16-P110/5-NF	https://app.bom.com/bom-auth/detail-download/pbDpA6/1747089246/1559-TS-GPS-1X4-Splitter-04.pdf
8224-40152	E025-0003-0012	1:4,110VAC	21dB	yes	GPS Source P/N: S14-A-P110/5- NF	https://app.bom.com/supplier-items/detail-spec?item_id=1203069063
8224-40153	E025-0003-0037	1:4, with amp, 220 VAC with EU plug		?	NALDCBS1X4-N/5.0/220	https://app.bom.com/supplier-items/detail-sourced?item_id=1271744567&version_id=
8224-20051	E025-0003-0017	1:2,no amp, DC	N/A	yes	NLDCBS1X2-N/5/MC	https://app.bom.com/bom-auth/detail-download/mU4BCa/1747087101/GPS%20Networking%20LDCBS1X2%20Rev%20A%207-11-07.pdf
8224-40151	E025-0003-0018	1:4,DC	N/A	yes	NALDCBS1X4-N/5/MC	http://www.navtechgps.com/gps_networking_ldcbs1x4_passive_antenna_splitter_1x4/
8224-81150	E025-0003-0019	1:8, amp, DC-pass (no external input power)	13dB		ALDCBS1X8-N	http://www.navtechgps.com/gps_networking_aldcbs1x8_active_antenna_splitter_1x8/
8224-80151	E025-0003-0020	1:8,amp,DC	14dB	yes	NALDCBS1X8-N/5/MC	https://app.bom.com/bom-auth/detail-download/MjzTF6/1752139089/ALDCBS1X8%20ProdSpec2015.pdf
8224-40053	E025-0003-0021	1:4,no amp,220V	N/A	yes	NLDCBS1X4-N/5/220	https://app.bom.com/bom-auth/detail-download/7zaqBT/1747089176/LDCBS1X4.pdf
8224-20054	E025-0003-0022	1:2,no amp,240 VAC with UK plug	N/A	yes	NLDCBS1X2-N/5/240	https://app.bom.com/items/detail-spec?item_id=1221547550&version_id=10533047968
8224-21150	E025-0003-0023	1:2, with amp, DC-pass (no external input power)	22dB	yes	ALDCBS1X2-N	https://app.bom.com/items/detail-spec?item_id=1221579726&version_id=10533641818&
8224-20153	E025-0003-0024	1:2, with amp,220 VAC with EU plug	22dB	yes	NALDCBS1X2-N/5/220	https://app.bom.com/items/detail-spec?item_id=1221579829&version_id=10533643468
8224-40000	E025-0003-0025	1:4, no amp	N/A	yes	LDCBS1X4-N	https://app.bom.com/items/detail-spec?item_id=1227707648&version_id=10642751258&
8224-20053	E025-0003-0027	1:2, no amp, 220 VAC power, 5V on input	N/A	?	NLDCBS1X2-N/5/220	https://app.bom.com/supplier-items/detail-attach?item_id=1229923435&version_id

						=
8224-20154	E025-0003-0028	1:2, with amp, 240 VAC with UK plug	22dB	yes	NALDCBS1X2-N/5/240	https://app.bom.com/items/detail-spec?item_id=1230554562&version_id=10696303518&
8224-40154	E025-0003-0029	1:4, with amp, 240 VAC with UK plug	17dB	yes	NALDCBS1X4-N/5/240	https://app.bom.com/items/detail-spec?item_id=1232815434&version_id=10735350198&
8224-20000	E025-0003-0030	1:2, DC-block all ports	N/A	?	LDCBS1X2-N-All Ports Blocked For DC	https://app.bom.com/items/detail-spec?item_id=1233695065&version_id=10754894208&
8224-41150	E025-0003-0031	1:4, w/amp	17dB	?	ALDCBS1X4	https://app.bom.com/changes/detail-summary?change_id=2388340868&
8224-80153	E025-0003-0034	1:8, with amp	13dB	yes	NALDCBS1x8	https://app.bom.com/items/detail-sourcing?item_id=1240388121&version_id=10863547528
8224-80154	E025-0003-0035	1:8, with amp; 240 VAC with UK plug	14dB	yes	NALDCBS1X8-N/5.0/2400	https://files.bom.com/download/cc38D6e50FcULIZ3W3J5cwOhmEs1yFbG/igsdcqhozlmnfvnqbgdnoinstntbcsxye/ALDCBS1X8ProdSpec2018.pdf

DC input from power supply to the GPS splitter

A) MC (Military style connector) input range for power supply is 9-32 vdc

Note: Power source is supplied by the customer (not supplied by Spectracom).

Network Power Supply		
Source Voltage Options	VOLTAGE INPUT	STYLE
	110VAC	Transformer (Wall Mount)
	220 VAC	Transformer (Wall Mount)
	240 VAC (United Kingdom)	Transformer (Wall Mount)
	Customer Supplied DC 9-32 VDC	Military Style Connector

I was able to locate the specs on the Military Style DC power connector for the 8224 external DC powered splitter:

Amphenol part numbers:

- **MS3102E-10SL-4P** = Mil DC connector
- **MS3106A-10SL-4S** = Mil DC mating connector
- **MS3057-4A** = Strain Relief

Pin-out of the external input power connector (splitter can accept 9-32vdc to output 5vdc to the antenna).

Positive

Return

5vdc provided to the Antenna

- (Active splitter Models only)
- Active splitters power the GPS antenna with 5vdc
- GPS networking splitters:

Output Voltage Options ⁽¹⁾	DC VOLTAGE OUT	MAX CURRENT OUT FOR CORRESPONDING Vout ⁽²⁾
	5 V	120mA
	7.5V	140mA
	9V	150mA
	12V	180mA
	15V	220mA
	Custom	TDB
Pass/Block DC Options		
Pass DC ⁽¹⁾	All Ports Pass DC	
DC Blocked ⁽¹⁾	J2 is DC blocked, Pass DC from J1 to ANT.	
RF Connector Options		

(Passive splitter Models only)

- Passive splitters just pass the 5vdc voltage from the receiver to the GPS antenna.

8224 Warranty period (all Model variants): 1 year from date of purchase

Model 8224 Declaration of Conformity

- Refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Declaration of Conformity>

Note: The Declaration of Conformity for the Model 8230 antenna is included in the SecureSync's Declaration of Conformity Certificate.

Per Dave Sohn (15 Jun 15): it includes EN 60950-1:2006/A11:2009 for safety. We don't test to EN61000-6-1:2007 or EN 61000-6-3:2007, instead testing against EN 55022:2006/A1:2007 for Class A emissions, and EN55024:1998/A2:2003 for immunity.

Q. Just wondering if I could put a splitter in for another project that needs a GPS feed. Is that something that isn't advised? If it is something that can be wired in, does it have to go into a certain spot in the circuit?

A. Reply from Dave Lorah You can certainly use a GPS Splitter to share a GPS signal but some precautions need to be taken to avoid attenuating the GPS signal too much. The splitter should be placed on the output side of the F.O. Receiver. A two-way splitter will have two outputs. One is a DC pass-through which will supply DC power to the F.O. Receiver and the other is DC blocked. So, care must be taken not to disconnect the DC pass-through side or power to the F.O. receiver will be interrupted, causing loss of GPS Signal to the second device.

The GPS Splitter has an insertion loss of about 6 dB so it will attenuate the signal a bit, reducing the maximum cable length allowable between the F.O. receiver and the SecureSyncs.

The length of cable from the splitter to the second device will further attenuate the signal. If the second device can be located a short distance to the SecureSync it would be ideal.

Spectracom does offer a splitter with a built-in amplifier if signal attenuation is a problem. This model does not use the GPS receiver power from the SecureSync antenna output but requires an external power supply of 5V.

I should also mention influence from the second device could affect the SecureSync GPS Signal. There would be a possibility of GPS Signal loss to the SecureSync if there was a malfunction on the second device.

I have attached a data sheet describing our GPS Antenna Splitters. Please let me know if you have any questions.

Some of the various Models of GPS splitters we offer

Model 8224-2 (Two-Way GPS splitter)

Spectracom P/N: E025-0003-0001

(GPS networking P/N: LDCBS1X2-N)

<http://gpsnetworking.com/datasheet%20replacements/LDCBS1X2.pdf>

Note: The GPS receiver connected to port J1 powers the antenna. The other GPS receiver port is DC blocked.

Recommendation to use a DC or AC input splitter instead.

Email Keith sent to a customer (5 Aug 31) Thanks for sending the picture of the current GPS splitter. As I expected to see, this particular two-way GPS splitter uses the GPS receiver (NetClock) connected to port J1 to power the GPS antenna. The NetClock connected to port J2 does not power the antenna. As long as a NetClock is connected to J1 and powered-up, the antenna is able to be powered and able to send the GPS signal to both NetClocks. But if the NetClock that is normally connected to J1 is disconnected from the splitter or is powered-down for any reason, the antenna will no longer be powered and will stop supplying the GPS signal to both NetClocks. Once the NetClock is reconnected to J1 or powered-up again, both NetClocks can then track GPS satellites again (as you were observing).

For complete redundancy of the two NetClocks, it's best for each NetClock to have its own GPS antenna. However, running two antenna cables to the roof in order to use two separate antennas can be difficult (to nearly impossible)! The Model **8224-2-DC (DC input supplied by the customer)** or the Model **8224-8-110 (110VAC input supplied by the customer)** are the recommended replacements for this splitter, to prevent the condition you were observing from occurring again. These two splitters don't use either Ports J1 or J2 to power the antenna. Instead, these two splitters use customer-supplied DC (8224-2-DC) or 110VAC (8224-8-110) power to power to the antenna. As long as there is a bench power supply or other DC power source available at the site, the 8224-2-DC is the recommended replacement. Otherwise, the 8224-8-110 uses 110VAC power. Since this site is in Japan, if they don't have 110VAC power available, they will want to use the 8224-2-DC splitter.

Model 8224-4 (Four Way GPS splitter)



Spectracom P/N: E025-0003-0003

(GPS networking P/N: LDCBS1X4-N)

<http://gpsnetworking.com/datasheet%20replacements/LDCBS1X4.pdf>

Note: The GPS receiver connected to port "J1" powers the antenna. The other GPS receiver ports are DC blocked.

Model 8224-8 (Eight-Way GPS splitter)

Spectracom P/N: E025-0003-0002

(GPS networking P/N: NHI-ALDCBS1X8-N/5/110)

<http://gpsnetworking.com/datasheet%20replacements/ALDCBS1X8.pdf>

Input power: 110VAC input from a wall wart. See note below.



Note (21 Oct 2013): The Model 8224-8 we offer uses 110VAC input from a wall mount power transformer. GPS Networking also offers this GPS splitter with 220VAC input, but we don't currently offer it in this configuration. If a customer needs 220VAC input, refer them to GPS Networking to purchase it directly from them.

Model 8224-2-DC (Two Way GPS splitter with external DC input)

Spectracom P/N: E025-0003-0004

(GPS networking P/N NALDCBS1X2-N/5/MC)

<http://gpsnetworking.com/datasheet%20replacements/ALDCBS1X2.pdf>

- Has built-in amp for 20 db gain
- Customer needs to provide their own 5vdc power supply (such as a benchtop power supply or wall adapter).
- Apparently, the DC connector//strain relief is supplied with the splitter when we receive it from our vendor.

Military style DC power connector

I was able to locate the specs on the Military Style DC power connector for the 8224 external DC powered splitter:

Amphenol part numbers:

- **MS3102E-10SL-4P** = Mil DC connector
- **MS3106A-10SL-4S** = Mil DC mating connector
- **MS3057-4A** = Strain Relief

Pin-out of the external input power connector (it can accept 9-32vdc in order to output 5vdc to the antenna).

Note: Power source is supplied by the customer (not supplied by Spectracom).

Positive

Return

Model 8224-20051 ()

Spectracom P/N: E025-0003-0017

GPS networking P/N NLDCBS1X2-N/5/MC <https://app.bom.com/bom-auth/detail-download/mU4BCa/1747087101/GPS%20Networking%20LDCBS1X2%20Rev%20A%207-11-07.pdf>

- Customer needs to provide their own 9-32 vdc power supply (such as a benchtop power supply or wall adapter).
- Apparently, the DC connector//strain relief is supplied with the splitter when we receive it from our vendor.

Military style DC power connector

I was able to locate the specs on the Military Style DC power connector for the 8224 external DC powered splitter:

Amphenol part numbers:

- **MS3102E-10SL-4P** = Mil DC connector
- **MS3106A-10SL-4S** = Mil DC mating connector
- **MS3057-4A** = Strain Reli

RoHS compliancy for the Model 8224

here.

<https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/products/SecureSync/default.aspx>

Per Tom Richardson (1 Apr 15 KW) It is included in the SecureSync RoHS Cert located

Specs for the Model 8224 splitters

- Refer to: <I:\Engineering\Engineering Shared\Spectracom parts\E025-xxxx-xxxx>

Per Model 8224 mfg data sheet ("GPS Networking ALDCBS1X2"):

Dimensions: Height: 1.3" Length (not including connectors)

Body: 2.5" Base Plate: 3.25" Width (not including connectors): 2.5" Weight: 10 oz. (286 grams)

Operating Temp. Range: -40° to + 75°C

Military Specs for the 8224s from GPS Networking

Q. (2/22/12 KW) From Jeremy Thomas (Spectracom UK)

I believe these are likely to be suitable for aircraft use as are ruggedized and of industrial design, however am checking if there is any actual certification.

Reply from Mark.Kreckeler@selexgalileo.com

I have been looking into your GPS splitter for Aircraft question some more and engineering have come back with the following; 'These splitters have not been mil tested but are designed and built to mil spec 810. We know that both of these splitters as well as those others that we offer have been used by the US military in air craft as well as in militaries and NASA.'

I hope this is satisfactory but welcome any questions. Please advise how you wish to proceed.

Mil Qualifying Standards for the standard Model 8224 (8224-2):

Mil Qualifying Standards for the standard Model 8224 (8224-2):

ENVIRONMENTAL	REQUIREMENT	PART SPECS (LDCBS1X2-N)
Indoor Humidity - Operational	20% to 60%	100%
Humidity - Non-Operational Storage & Transportation, In a Packaged Configuration	0% to 100%	100%
Atmospheric Pressure – Operational	1084mb to 700mb (sea level to 9842 feet)	Far Exceeds (Mil Std 810F)
Atmospheric Pressure - Non-Operational & Transportation	1084mb to 572 mb (sea level to 15,000 feet)	Far Exceeds (Mil Std 810F)
Metal Whiskers	Any pure tin (100% Sn) internally or externally?	NO
Qualification Method:	Qualification / reliability data for this or similar part? Please provide report	MTTF >150,000 hours No report available for LDCBS1X2
Please PROVIDE MATERIAL INFORMATION	connectors' material and finish	Nickel Plated Aluminum
Please PROVIDE MATERIAL INFORMATION	case material and finish	Nickel Plated Aluminum
Please PROVIDE MATERIAL INFORMATION	lid material and finish	Nickel Plated Aluminum

EMI:

MIL-STD: 461/462
(EMI)

CE01, CE04, CS01, CS02, CS06, RE02, RS02,
RS03 @ 200 Volts/Meter from 14Khz to 40Ghz

ENVIRONMENTAL:

MIL-STD 810D
(Environmental)

Vibration (514.3, Proc. 1)
Category 6 (helicopters)
Rain(506.2 Proc. 1)
Humidity(507.2, Proc 2, cycle 4)
Fungus(508.3, Proc. 1)
Salt/Fog(509.2)
Explosive Atmosphere(511.2, Proc 1)
Bench Handling Shock(516.3 Proc 6)
Temp/Altitude(520.0 Proc 3)
Acceleration(513.3, level = 6G's)
Gunfire Vibration(519.3)

Bands: Supports both L1 and L2 bands

Desire to use one antenna on more than one clock (internal GPS splitters that we use on the racks)

- Requires the use of special GPS splitters
- +5vdc out from clock has to be isolated.
- Contact WR inc at 1-800-463-3063
- Mini-circuits zfbt-4r2g-ft to power antenna/preamp
- Mini-circuits zapd-2-n Four-way splitter
- Mini-circuits zb8pd-2-n Eight-way splitter
- Need to remove tops on 8 way splitters and cut traces at each output and add 0.1 uFd caps across cuts.

****Troubleshooting Model 8224

A) Troubleshooting 8224s that use one dedicated GPS receiver to power the GPS antenna (Models 8224-2 and 8224-4)

- Disconnect the cable connected to the “Antenna” port. With a GPS receiver connected to J1, verify ~4.9vdc is present on the “Antenna” port (allowing the splitter to power the antenna). If not, verify there is ~4.9vdc on the end of the cable that attaches to J1 (the port used to drive the antenna).
- Try swapping the cables attached to ports J1 and J2
- Temporarily bypass the GPS splitter and then verify if the GPS receiver starts tracking satellites.

Email from Keith (22 Apr 2013) In case you weren't already aware, one of the two GPS receiver ports is dedicated to powering the GPS antenna (J1) while the other one blocks the DC power from the GPS receiver that is used to power the antenna (J2).

In order for the GPS antenna to remain powered-up at all times, a GPS receiver (such as a Spectracom NetClock or SecureSync) must always be powered-up and connected to port J1 on the splitter (the DC pass-through port). If a GPS receiver is only connected to port J2, the antenna will not be powered and the GPS receiver connected to this port will therefore not be able to track any satellites.

In order to better assist you, I have some questions for you:

- 1) Are you using Spectracom GPS receivers (such as SecureSync or NetClock)? If so, what Models are they?
- 2) Is there currently a GPS receiver powered-up and connected to both ports J1 and J2 (with the GPS antenna connected to the “Antenna” port)?
- 3) If there is, is only one of the two GPS receivers tracking satellites? Or is neither receiver tracking satellites?
- 4) Have you tried swapping the cables connected to ports J1 and J2 and after a few minutes verified if either receiver is tracking satellites?
- 5) If neither GPS receiver is tracking satellites, is the GPS antenna installed outdoors with a good, clear view of the sky (preferably 360 degrees)?
- 6) Have you tried bypassing the GPS splitter to verify the GPS receiver is able to track at least one satellite without it being inline?
- 7) Does “Antenna Sense” report “OK”? Or does it instead indicate either “UC” or “OC” (in SecureSync and Models 94839489, this is reported in the Status -> Inputs -> GPS page of the browser. In the NetClock 9200/9300 series, it's reported in the Status and Logs -> GPS Signal Status page of the browser)?

As long as a GPS receiver is connected to at least J1 and with the antenna connected to the splitter, try bypassing the GPS splitter with a type N barrel to verify that GPS receiver can track at least one satellite (the Spectracom receivers need to track at least four satellites for initial sync to occur). Or, temporarily relocate the receiver and connect it directly to the cable that attaches to the GPS antenna. Verify it can track at least four satellites. If it continues to track 0 satellites, this means the issue is not with the GPS splitter. Let us know the Model of the GPS receiver and we will send you additional information to troubleshoot this condition.

B) Troubleshooting 8224s that use externally provided DC voltage to power the GPS antenna (Models 8224-8-110 and 8224-2-DC)

- 1. Disconnect the cable connected to the “Antenna” port. Verify ~4.9vdc is present on the “Antenna” port (allowing the splitter to power the antenna). If not, verify external input power is being applied to the splitter.**
- 2. Temporarily bypass the GPS splitter and then verify if the GPS receiver starts tracking satellites.**

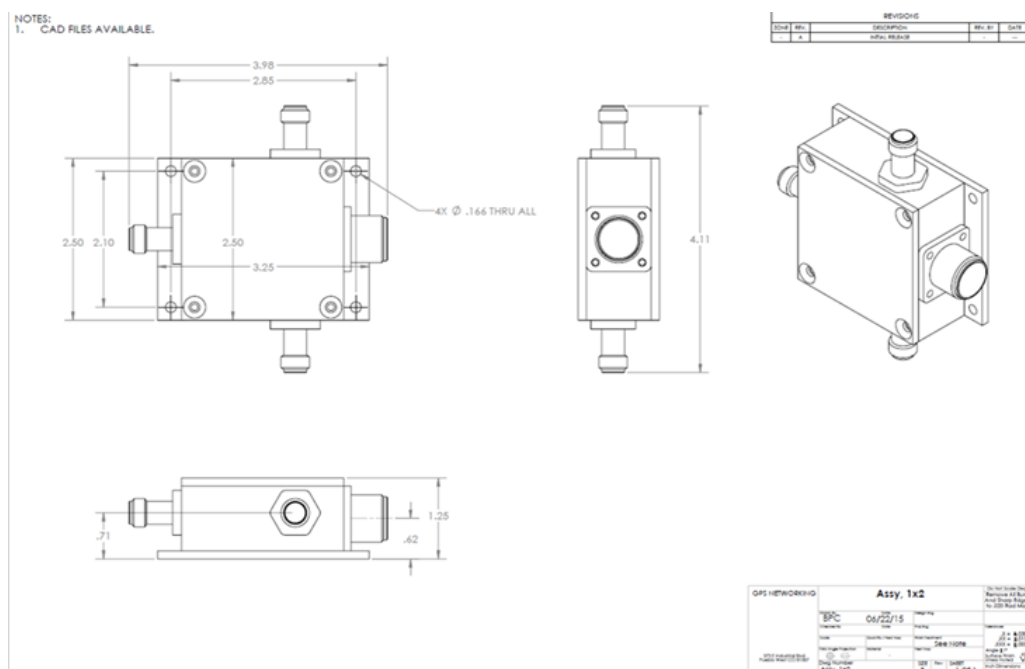
To better assist you, I have some questions for you:

- A) Are you using Spectracom GPS receivers (such as SecureSyncs or NetClocks)? If so, what Models are they?
- B) Is only one of the two GPS receivers tracking satellites? Or is neither receiver tracking satellites?
- C) Have you tried swapping the cables connected to ports J1 and J2 and after a few minutes verified if either receiver is tracking satellites?
- D) If neither GPS receiver is tracking satellites, is the GPS antenna installed outdoors with a good, clear view of the sky (preferably 360 degrees)?
- E) Have you tried bypassing the GPS splitter to verify the GPS receiver is able to track at least one satellite without it being inline?
- F) Does “Antenna Sense” report “OK”? Or does it instead indicate either “UC” or “OC” (in SecureSync and Models 94839489, this is reported in the Status -> Inputs -> GPS page of the browser. In the NetClock 9200/9300 series, it's reported in the Status and Logs -> GPS Signal Status page of the browser)?

Try bypassing the GPS splitter with a type N barrel to verify that GPS receiver can track at least one satellite (the Spectracom receivers need to track at least four satellites for initial sync to occur). Or, temporarily relocate the receiver and connect it directly to the cable that attaches to the GPS antenna. Verify it can track at least four satellites. If it continues to track 0 satellites, this means the issue is not with the GPS splitter. Let us know the Model of the GPS receiver and we will send you additional information to troubleshoot this condition.

Email from Pierre (7 Sept 17) I already made a research on Internet and I found the following details:

Reply from Dave Lorah: That same drawing is all I can find also. This is part of the GPS Networking data sheet



****Model 8226 GPS Surge Suppressor**



Links/shortcuts

- **Shortcut to Model 8226 Data Sheet (on our website):** <https://www.rolia.com/documents/8226-datasheet>
- **Shortcut to Model 8226 in Customer Service:** <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8226 and grounding kit>
- **Shortcut to MFG Data sheets:** <I:\Engineering\Engineering Shared\Spectracom parts\067012 – 8226>
- **Shortcut to 8226 manual (8226-0002-0050) in Arena:** https://app.bom.com/items/detail-spec?item_id=1202835968&version_id=10221286488&orb_msg_single_search_p=1&redirect_seqno=8541583122

Spectracom P/N's:

(Note: we don't sell/offer just the 8226 by itself. Have to purchase 8226-0001-0600 for 8226 and L bracket)

- **E025-0007-0001:** Just the surge protector itself
- **8226-0001-0600:** Surge suppressor, connectors, L bracket (customers have to purchase this kit to get an 8226)
- **8226-0002-0600:** Surge suppressor grounding kit
- **P051-0001-0100:** Field installable type N connectors
- **MP10-0000-0100:** L mounting Bracket

General information on surge protectors

- **Additional Nextec grounding recommendations:**
<http://www.nexteklightning.com/pdf/datasheets/FPLNFNFBxxx.pdf>

Note about the manual when the order ships: Since we send product manuals on CD, we still continue to send a paper copy manual with the antenna (the Model 8226 antenna manual is not on the manual CD)

MFG: NexTec, Inc. Westford, MA (978) 486-0582

Model: SurgeGuard

MFG. Data sheet: <http://www.nexteklightning.com/pdf/datasheets/FPLNFNFBxxx.pdf>

General questions (replies in red are from Tom Richardson, 29 Jan 17)

Q What is the recovery time of GPS Surge arrestor if ever the vicinity was strike by lightning? Almost instantaneous but depending on the amount of energy that was coupled into the surge arrestor it might have become damaged.

A Reply from Keith (29 Jan 17) Per the Surge Suppressor data sheet

(<http://nextek.com/products/product/fplnfnp05/>) the suppressor has a 10ns response time. But the data sheet doesn't indicate recovery time. I assume it's less than one second once the voltage is no longer exceeded

Q The antenna was mounted on metal pole. Does this make the antenna more likely to be struck by lightning? There are taller metal structures around the vicinity. **The cable itself is metal. Any object mounted in the air is subject to lightning strikes.**

Note: for both questions above from the same dealer, Tom said to refer to the two links below:

Info from Tom Richardson (29 Jan 16)

- Nextek has an education center and I would direct any questions to them as they are the “experts”.
<http://nextek.com/education-center/>
- Polyphaser is also a good source of information about lightning protection.
<http://www.polyphaser.com/services/media-library/lightning-facts>

MTBF for Model 8226

- Refer to (in this doc): [MTBF/MTTR \(for all products\)](#)

Model 8226 Declaration of Conformity

- Refer to: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Declaration of Conformity](#)

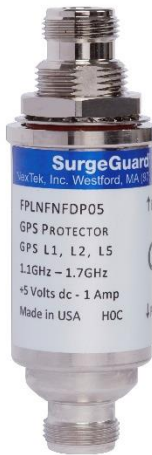
Note: The Declaration of Conformity for the Model 8226 surge suppressor is included in the SecureSync’s Declaration of Conformity Certificate.

Per Dave Sohn (15 Jun 15): it includes EN 60950-1:2006/A11:2009 for safety. We don’t test to EN61000-6-1:2007 or EN 61000-6-3:2007, instead testing against EN 55022:2006/A1:2007 for Class A emissions, and EN55024:1998/A2:2003 for immunity.

UL 1449 certification question

Email from Jodi to Marty with GMA (19 Nov 2018) I listened to your voicemail. I did a little research so I wanted to touch base before we leave for the evening. I do not see that the surge suppressor is UL 1449 certified. The documentation does not indicate this. I do see CE certification, but not UL.

Nextek FPLNFnFBP05: Most recent Model 8226 (Replacement to the Polyphaser Surge suppressors)



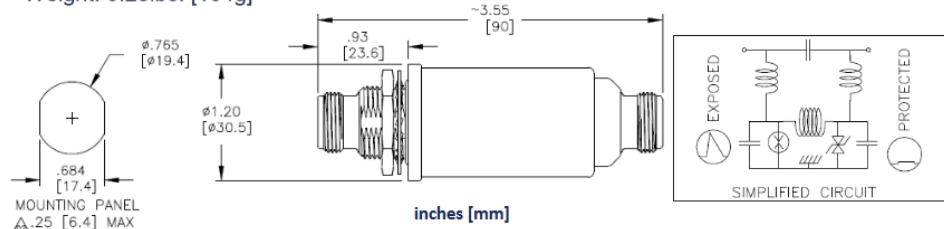
Below is from datasheet: <https://nextek.com/products/product/fplnfnfdp05/>



Product Specification FPLNFnFDxxx

Mechanical Specifications

Weight: 0.23lbs. [104g]



Optional - Mounting bracket order P/N 750-0632-00

Recommended Panel/Bulkhead Mounting Torque: 15ft-lbs (20.3Nm)

Links

- NexTek datasheet on Web: <https://nextek.com/products/product/fplnfnfdp05/>
- Link to datasheet (in Arena) https://app.bom.com/files/detail-summary?file_master_id=1234731052&file_id=1746169149
- Link to BOM (in Arena) https://app.bom.com/items/detail-bom-nested?item_id=1202840937&version_id=10212766028&nested_bom_p=1

3D CAD drawing of Nextek suppressor (from NexTek): [..\..\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8226 and grounding kit\NexTek 8226\3D CAD drawings](#)

Part Numbers

- Most recent MFG and Model Number: **Nextek FPLNFnFBP05**

- Our P/N for 8226 by itself: **E025-0007-0001**
- Our P/N for the Model 8226, L bracket, etc: **8226-0001-0600**

Ships with:

- L Bracket (**MP10-0000-0100**), two field-installable type N connectors (**P051-0001-0100**) and instruction sheet

Connectors: Labeled as “Exposed” and “Protected”



Waterproof: Case- Yes (per MFG data sheet) Connectors- No

Input Power: + 5Vdc, 1A

IP Rating: IP68 [IP rating/Ingress rating \(for all products\)](#)

IP68	Protected from total dust ingress.	Protected from long term immersion up to a specified pressure.
------	------------------------------------	--

Compatible with: GPS (L1, L2, L5), Galileo, EGNOS, WAAS and Glonass

Recommended gauge ground cable: Per Nextec- “Ground the protector within 3ft (1m) of entry into the protected area. Ground bond conductors should be less than 3ft (1m) feet long. Ground bond conductors should be 2X the area of the coaxial shield, or a minimum of 6 AWG (15mm²) for a 7-16 or **10 AWG (3.5 mm²) for an N protector.**”

Environmental Specifications

Temperature Range	-40°C to +90°C
Salt Fog	MIL-STD-202 Method 101D / Condition B (35°C/48 hrs)
Immersion	MIL-STD-202 Method 104A / Condition A (65°C to 25°C w/NaCl – 2 cycles)
Moisture Resistance	MIL-STD-202 Method 106E (65°C/98% RH condensing/240 hrs)
Temperature Shock	MIL-STD-202 Method 107D / Condition B-1 (25 cycles -65°C to +125°C)
Life (Elevated Temperature)	MIL-STD-202 Method 108A / Condition A (96 hours at 100°C)
Dust and Waterproof Rating	IEC529 IP68 (dust-tight and water proof 24 hrs / 1 m)
Vibration	MIL-STD-202 Method 204D / Condition D (10Hz-2kHz 0.06”DA/20g)
Mechanical Shock	MIL-STD-202 Method 213 / Condition A (50g/11ms ~24”)

Mounting and Grounding/Connector tightening

Minimum recommended distance between 8226 and protected equipment

- A) PolyPhaser recommends at least 7 feet of cable separation between the surge suppressor and the protected equipment.**

Email Keith sent to Sadie (13 May 2014) To answer this question, there is actually a minimum recommended distance (cable distance, not necessarily physical distance) between the 8226 and the SecureSync. It has to do with the amount of time that it takes for the 8226 to switch from "inline" over to ground. Theoretically, high voltage could go past the surge suppressor before the 8226 switches to ground. If the 8226 was connected directly to the SecureSync, that surge would go into the equipment. But by having at least a minimum length of cable after the 8226, the voltage will go backwards to the surge suppressor and out to ground, when the 8226 does actually switch. The voltage then doesn't have time to get to the equipment before its shunted to ground.

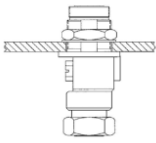
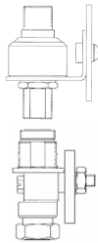
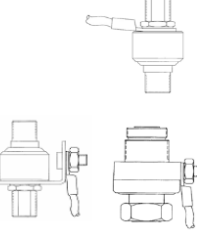
PolyPhaser recommends at least 7 feet of cable between the surge suppressor and the protected equipment, to prevent any high voltage getting into the receiver. The current Model we use is from NexTec. I don't have a recommendation from them, though it's likely to be similar.

There shouldn't be any physical limitation on how close the 8226 is to the SecureSync, as long as it's not touching the case. But NexTec recommends the 8226 be installed within 3 feet of the cable coming into the area of where the SecureSync is located.

Refer to: <http://www.nexteklightning.com/pdf/datasheets/FPLNFBxxx.pdf> for the info below

Mounting and Grounding

Ground the protector within 3ft (1m) of entry into the protected area. Ground bond conductors should be less than 3ft (1m) feet long. Ground bond conductors should be 2X the area of the coaxial shield, or a minimum of 6 AWG (15mm²) for a 7-16 or 10 AWG (3.5 mm²) for an N protector.

		
Through Panel / Bulkhead	To a ground bar or panel surface	Grounded by a wire jumper or strap
<ul style="list-style-type: none">+ Best grounding and shielding+ Strain relief loop needed for rigid cable+ Mounting hole size for each connector	<ul style="list-style-type: none">+ Better grounding+ Easily installed with simple holes+ Cable should include strain and drip loop	<ul style="list-style-type: none">+ Good ground with a short wire+ Accommodates cable movement+ Very easy installation

Tightening

Mount the protector and tighten the connector coupling nuts and mounting or grounding nuts to ensure long term reliable operation.

Component	N Mount Nut	N or TNC Coupling Nut	7-16 Mount Nut	7-16 Coupling Nut	M8 (Boss)	M5 (Bracket)
Inch-pounds	80	12	300	200	130	40
N-m	10	1.4	35	22	15	4.5

Other Application Tips

1. Select the protector based on the RF frequency, connector, RF power and dc capability.
2. Limit the unprotected coaxial lead-in into the protected zone to 3' (1m) to reduce high energy into the protected area. For severe exposure locations, use a bulkhead mount to eliminate this risk.
3. Make sure that the mounting surfaces are clean, dry and fully tightened.
4. If a protector is rigidly mounted, install a strain relief bend in large coaxial cables.
5. Allow for access to replaceable components, preferably with access ports oriented down.
6. Use weatherproof mating connectors. Field terminations may need moisture wrap.
7. Do not install during wet or rainy conditions. Do not use wet hands. Use a screwdriver to tighten the mounting nuts.

Operation of the Model 8226 / voltages

Email from Dave L (11 Dec 2020)

The Model 8226 Surge Suppressor is rated for the following voltages:

Nominal Voltage (Antenna supply voltage) = 5V

Maximum Voltage = 6.7 V

Let Through Voltage (Trip point) = 8V

Q Voltages exceeding the impulse suppressor trip point are shunted to the system ground.] What is the specific content of the impulse suppressor trip point? What is the specific voltage value?

A Reply from Danny Loke to a customer (11 Dec 2020) Please find OEM datasheet attached.

All the specs are inside.

Clamping voltage for our P05 variant is +8Vdc.

At normal operation, the arrestor is a straight-through connector (there is a metal conductor inside the arrestor).

What happens is when a lightning strike at or near the antenna, the whole area will be energised instantaneously ... so the transient current induced into the cable/antenna is very high instantaneously.

The special gas in the arrestor will instantly reacts to this sudden change in current and becomes conductive, thus shorting the metal bar to the chassis inside the arrestor.

Hence, all harmful current will be shorted to Earth Ground.

Troubleshooting the Model 8226

1) Passing the 5vdc to the GPS antenna

(KW 8 Nov 2012). Based on a test Tom Richardson and I performed, the 5vdc should still be passed to the GPS antenna, whether the surge suppressor is installed correctly or if it's installed backwards (it should track satellites in either orientation).

If the GPS receiver only tracks with it installed backwards, there is an issue with the preamp (refer to Salesforce 6603 for Ben Lamm). It will need to be returned to us for evaluation.

Email Sam Otto sent to Open Access after talking to the manufacturer (7 Mar 2013): You may measure as low as 50K with the positive meter test lead to either center pin, negative test lead to case. The negative meter test lead to either center pin, positive test lead to case should measure lower as long as it does not measure a direct short. These values will measure differently depending on the quality of the meter being used which is dependent on the voltage being provided through the Zeiner diode.

A more accurate test would be connecting a Meter with a Diode setting across the center pin and case.

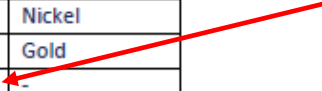
- Meter negative test lead to either center pin, positive test lead to case: ~ 0.4 volts
- Meter positive test lead to either center pin, negative test lead to case: Overload wont shunt

In addition, you may apply 5 VDC across either the input or protected side and measure 5 VDC on the other side. 5VDC to either center pin, common to the case.

3) Blue liquid inside the surge suppressor

Material and Finish

Component	Material ^{1,2}	Finish
Outer Parts	Aluminum	Nickel
Center Contact	BeCu	Gold
Insulator	PTFE	-
Gasket	EPDM or SIL	-



Email Keith sent to Sean Pedersen (23 Oct 2013) Regarding the mysterious “blue liquid” inside the lightning arrestor, I can say this is definitely the first time in almost 17 years I’ve heard of this!!! I’m not sure what it would be, but can say it’s not normal! Very strange indeed! My first thought was that it may have suffered a direct lightning strike, but then it’s strange that the GPS antenna still works (The antenna hasn’t ever been replaced at this site, has it)?

I just Googled the manufacturer’s data sheet for the surge suppressors and learned something new J ! They use a synthetic chemical called **Polytetrafluoroethylene (PTFE)** inside the suppressor for cooling (<http://en.wikipedia.org/wiki/Polytetrafluoroethylene>). Its Teflon (the same chemical used as non-stick coating on cookware and thread seal tape/thread dope). It must be the gasket/seal for this chemical is leaking. If the suppressor is less than 5 years old, we can assign an RMA Number for it to be returned to us for evaluation. In order to assign an RMA number, I just need to know the desired return ship to address and to whom it should be made attention to (if not yourself). I will respond with the RMA Number and the address to send it to.

Earlier Models of PolyPhaser surge suppressors (Not currently shipping)

- Spectracom P/N for the Model 8226 itself: E025-0007-0001
- More recent PolyPhaser Model: **DGXZ+06NFNF-A** (see “GX series surge suppressors” below)
- Even earlier PolyPhaser Model: IS-MR50LNZ+6 (see info further below)

Polyphaser GX series surge suppressors:

- Info below from: <http://www.transtector.com/SiteMedia/SiteResources/FamilyDataDocuments/1464-044.pdf?ext=.pdf>


Example of Naming Convention for GX Family**

D	GX	J	+	06	D	M	F	-	A
Frequency Band	Series	Type	Positivity	Voltage	Surge Side Connector Type	Surge Side Connector Gender	Protected Side Connector Gender		Lid Configuration

COAXIAL RF SURGE PROTECTION

GX Series

The GX Series of RF DC pass surge arrestors are engineered for RF coaxial applications where DC current is needed on the coaxial line. The GX Series can be used on GPS and other active antenna systems that operate in the range from DC to 2700 MHz.



FEATURES

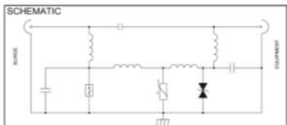
- Frequency ranges from DC to 2.7 GHz
- Patented hybrid surge protection
- Repeatable RF performance after surge
- Flexible bulkhead and bracket mounting options
- Weatherproof when installed
- 7/16" DIN, N-Type and TNC

STANDARDS

- Weatherproof: IEC 60529 IP 67
- Bellcore TA-NWT-000487
- Procedure 4.11, Wind Driven (120 MPH)
- CE and RoHS

PATENTED LIGHTNING ARRESTOR TECHNOLOGY

The GX product family is based on PolyPhaser's patented hybrid protection technology. This hybrid circuit integrates the quick response of a silicon avalanche suppression diode (SASD) with the surge handling capabilities of a MOV and gas tube. The GX technology has been field tested for more than a decade and has been used in critical RF networks world-wide.



GENERAL SPECIFICATIONS*

Insertion Loss	<0.1dB
VSWR	<1.1 or Better Over Frequency Range
Return Loss	>20dB
Max Operational Current	4A
Typical Surge Withstand	20KA/8/20µs Waveform
GXU Bias-T	SMA Connector as DC injector

1st Three Identifiers

Identifier	Frequency Range
ADX	DC to 50MHz
BGX	40MHz to 400MHz
CGX	400MHz to 1200MHz
DGX	800MHz to 2500MHz

Type

Type	Description
E	Extended Frequency
H	High Power
J	Bias-T w/ Injector Port
Z	DC Pass

Connector Types

Connector Types	Description
D	7/16" DIN
N	N-Type
T	TNC

Example of Naming Convention for GX Family**

D	GX	J	+	06	D	M	F	-	A
Frequency Band	Series	Type	Positivity	Voltage	Surge Side Connector Type	Surge Side Connector Gender	Protected Side Connector Gender		Lid Configuration

*Confirm with product specific datasheet for detailed specifications
**Not all combinations available

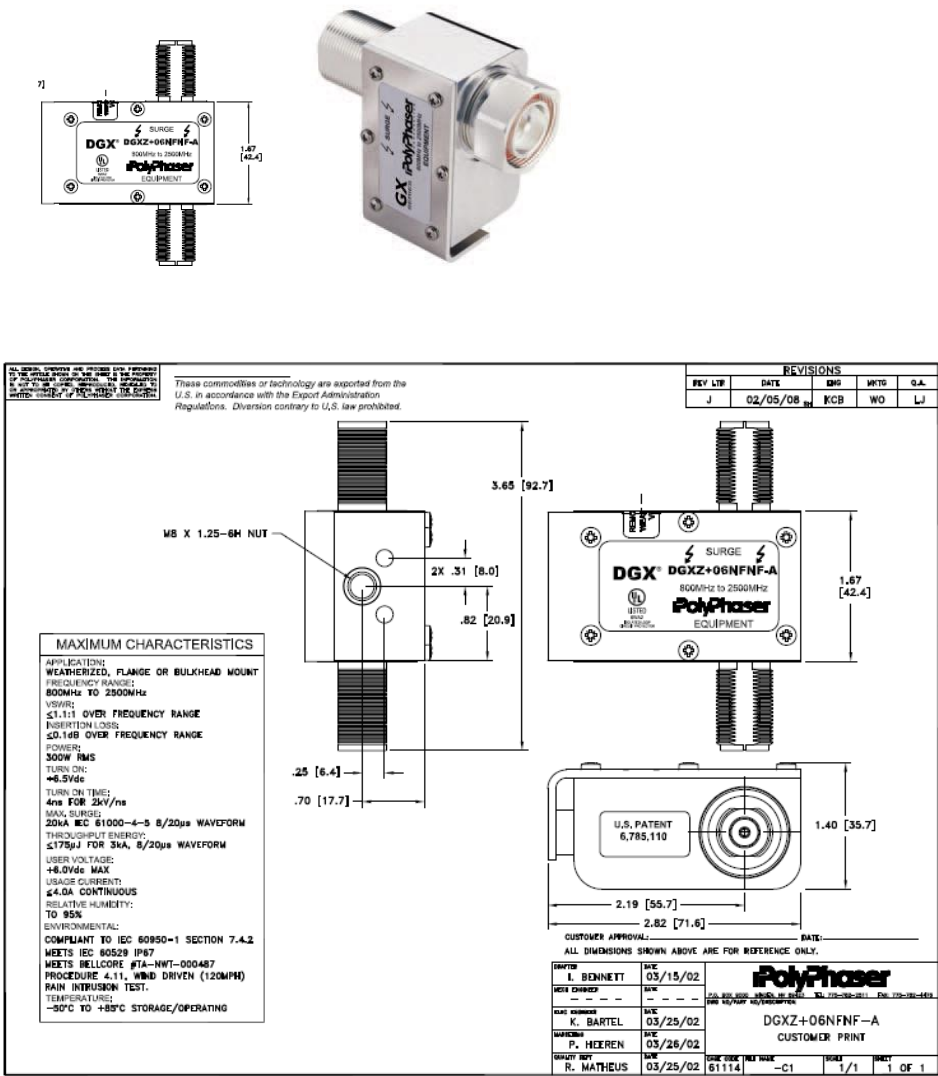
Polyphaser Model “DGXZ+06NFNF-A”

- link to PolyPhaser “GX” series surge suppressors: <http://www.transtector.com/SiteMedia/SiteResources/FamilyDataDocuments/1464-044.pdf?ext=.pdf>

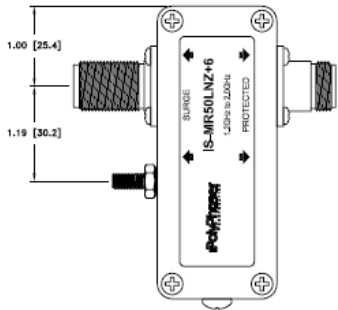
11/16/09 KW: The Model 8226 has a label on one side of it that shows the words “Surge” and “Equipment”. “Surge” should go towards the antenna and “Equipment” should go towards the Model 9389.

10/27/10 KW: The new PolyPhaser suppressor we are shipping (Model DGXZ +06NFNF-A) has a cutoff of both +6.5vdc

as well as -6.5vdc. The current 8226 data sheet only specifies the +6.5vdc cutout (not the -6.5vdc). New Model is labeled the same way-as described above.



B) Even earlier PolyPhaser Model: IS-MR50LNZ+6 (Not currently shipping)



Earlier PolyPhaser Surge Suppressor (IS-MR50LNZ+6)

**Field installable clamp connectors supplied with 8226

- **Spectracom P/N:** P051-0001-0100
- **Mfg:** Amphenol
- **Digikey P/N:** 82-202-1006 (<http://www.digikey.com/?curr=USD>)
- Two field-installable Type N connectors are provided with each Model 8226 (requires soldering but no crimpers)

Keywords:

☐ In stock
☐ Lead free
☐ RoHS Compliant

All prices are in US dollars.				
Digi-Key Part Number	ARF1020-ND	Price Break	Unit Price	Extended Price
Quantity Available	357	1	17.70000	17.70
Manufacturer	Amphenol-RF Division	10	12.01000	120.10
Manufacturer Part Number	82-202-1006	25	8.57000	214.25
Description	N COAX CON BELDEN 9913	100	7.86000	786.00
Lead Free Status / RoHS Status	Lead free / RoHS Compliant	500	6.22998	3,114.99
		1,000	5.92002	5,920.02

Quantity Item Number Customer Reference

Image shown is a representation only.
Exact specifications should be obtained from the product data sheet.

<http://media.digikey.com/photos/Amphenol Photos/82-202-1006.jpg>

Model 8226 RoHS compliancy

Q. (From Tony Diflorio) Do you guys know if the 8226 and the 8226-0002-0600 grounding kit are RoHS compliant?

A. (reply from Tom Richardson on 1/18/12): They are RoHS compliant.

Link to a customized RoHS compliancy certificate: [EQUIPMENT\SPECTRACOM EQUIPMENT\8225, 8225S, 8226, 8227 and grounding kit\8226 and grounding kit\RoHS compliancy](#)

Note: This RoHS certificate was created for and indicates Hughes. Need to edit this before forwarding it to anyone else.

L Mounting bracket for surge suppressors (Bulkhead to flange adapter)

Spectracom P/N: MP10-0000-0100

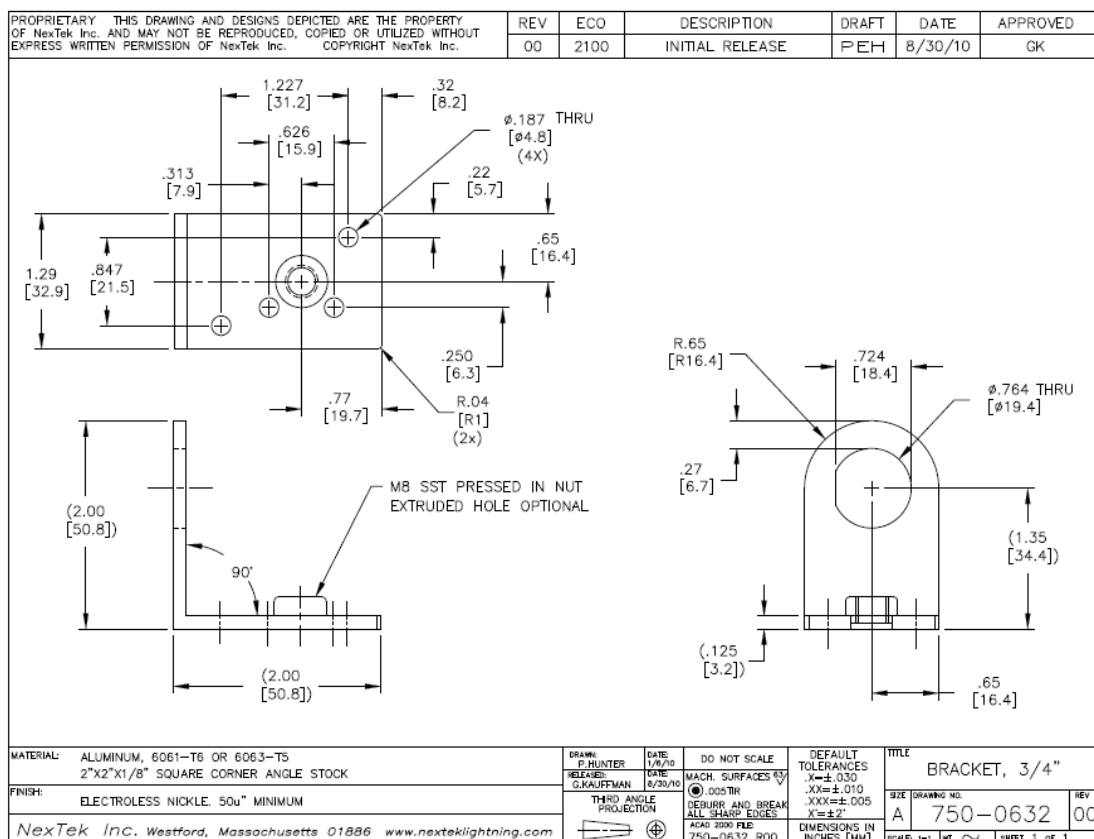
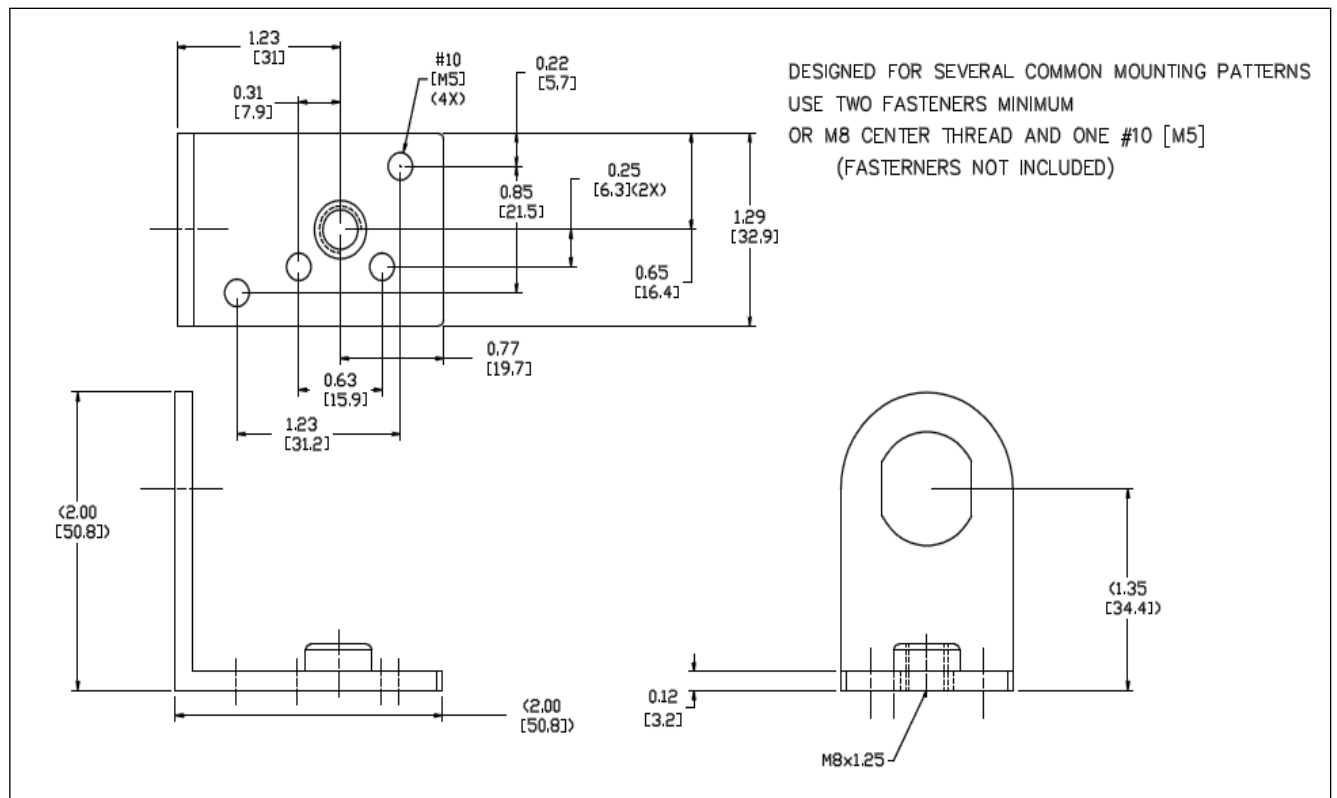
- Link to bracket in Arena: https://app.bom.com/items/detail-spec?item_id=1202834197&version_id=10212780588
- Nextek P/N: 750-0632-00
- 3D CAD drawing (from NexTek): [..\\EQUIPMENT\\SPECTRACOM EQUIPMENT\\8230, 8225, 8225S, 8226, 8227 and grounding kit\\8226 and grounding kit\\NexTek 8226\\3D CAD drawings](#)



Model 8226 mounting bracket (L bracket)

- Mounting bracket is included with all Model 8226s
- Link to manufacturers drawings and documents: [I:\\Engineering\\Engineering Shared\\Spectracom parts\\MP10-XXXX-XXXX](#)
- Current vendor and their P/N: Nextek 750-0632-00

The drawing of their L bracket is below, with all references to them removed (so as to help prevent customers from buying direct instead of from us. Before sending this drawing to a customer, first check the Part Spec record in the link directly above to ensure the “Nextek 750-0632-00” bracket is still the selected bracket for the Model 8226).



Q. What size bolt goes into the L-shaped bracket for the lightening protection device?

Note: I have found that a 8mm regular thread seems to be slightly loose; however a 5/16 regular thread will only screw in partway. I've been undecided if the 5/16 hits a locking part of the device or if it is the wrong screw.

A From Sam Otto (5 Sept 2013) I contacted our distributor for the L-shaped bracket after I could not find a diagram or any specifications for the bracket. They sent me a copy of the attached drawing.

The Hole is a M8 SST Pressed in Nut extruded Hole. The screw size is a M8x1.25.

****Ground cable for surge suppressors**

One example of a heavy duty grounding cable from Anixter
(Will Hickey believes we shipped this cable with PlantCML orders back in 2004)

<http://www.anixter.com/north-america/us/en/product-detail.6G-0401-04.html>

- Spectracom P/N W040-0004-0501
- Anixter P/N: 6G-0401-04

****Custom surge suppressors (not supplied by Spectracom)**

Raycap RF1-NFF-23 suppressors

Q. my local building engineer wants to use these Raycap RF1-NFF-23 type suppressors. It is a gas tube just like yours with a little higher insertion loss. Do you approve? Any concerns? They wanted to put yours and this device on both ends of the coax circuit but I told them they were crazy and could only use one. Naturally, they went with the VZW standard.

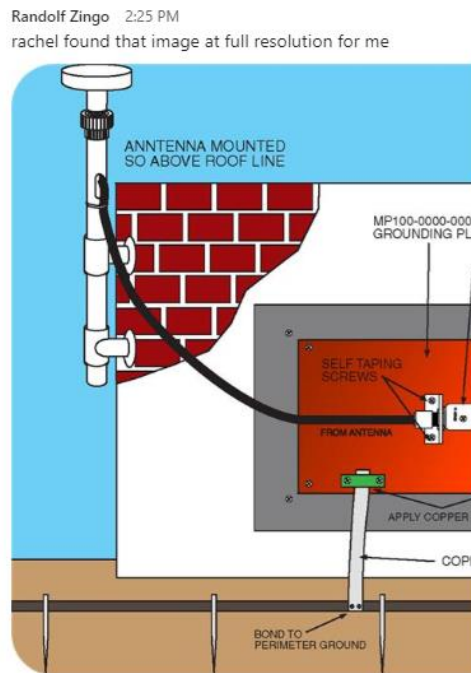
A. Reply from Dave Lorah (15 Oct 2013) I took another look at these specs and I do not see any harm in installing these surge suppressors in the system. These are gas discharge devices and will provide some added protection. These should not used as a substitute for the 8226 surge suppressors however. The RF1-NFF-23 will discharge at voltages over 230 Volts. The 8226 will discharge voltages above 6.7 Volts. Using the RF1 device alone will not provide enough protection for the low voltage receiver.

The RF1 device should be placed between the antenna and the 8226.

*Model 8226-0002-0600 (Surge Suppressor Grounding Kit)

General info about the Grounding kit.

(Picture below is available in the Model 8226 user manual. Note a similar picture is in the 8226 datasheet, but is in black/white)



- We don't purchase the kit in its entirety from one source.
- Instead, we purchase just the copper plate from one of a couple different companies (such as Polyhaser originally, or Harger)
- We then assemble the rest of the components into the box that the Ground plate arrives in.
- The box gets labeled with our P/N and the contents of the kit.

Associated Links

- 8226 datasheet on our website: <https://www.rolia.com/document/8226-datasheet/>
- Grounding kit info in custassistance folder: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8226 and grounding kit>

Associated Part Numbers

- Our P/N for the whole kit: 8226-0002-0600



- **8226 user manual (for both Surge suppressor and ground plate):** 8226-0002-0050
- **BOM (Items included):** 8226-0002-0600
- **Process Detail (assembly of the kit):** 8226-0002-0600-PD

BOM 8226-0002-0600 (Items included)

- **Refer to (in Arena)** https://app.bom.com/items/detail-spec?item_id=1202840938&version_id=10212766038&orb_msg_single_search_p=1&redirect_seqno=5749857021

Components included in the kit

Qty	Item Name	Our P/N	Manufacturer P/N
1	Standard 8226 manual	8226-0002-0050	N/A
1	Panel, Copper Ground	MP10-0000-0001	PolyPhaser CU-SPGP
1	Clamp, Ground Rod	MP26-0001-0001	ILSCO AGC-1
1	Connector, post	MP26-0002-0001	ILSCO CP-4
10 FT	Hookup, 4AWG, PVC, GRN, THNN, 600V	W040-0004-0501	6G-0401-04

Manufacturers/Suppliers of the copper ground panel:

- Polyphaser CU-SPGP (Copper Single Point Ground kit)
- Harger CUSPGPW <https://www.harger.com/product/single-point-ground-window> (in Arena) https://app.bom.com/supplier-items/detail-attach?item_id=1203069528
- Nextec ?

Installation/Documentation which ships with Grounding kit:

Kit ships with:

- Document from the specific supplier of the ground plate (Such as from Harger, for instance)
- 8226 install manual (which includes info on installing grounding kit)
 - **Manual P/N** 8226-0002-0050 (in Arena at: https://app.bom.com/items/detail-spec?item_id=1202835968&version_id=10421754778&orb_msg_single_search_p=1)

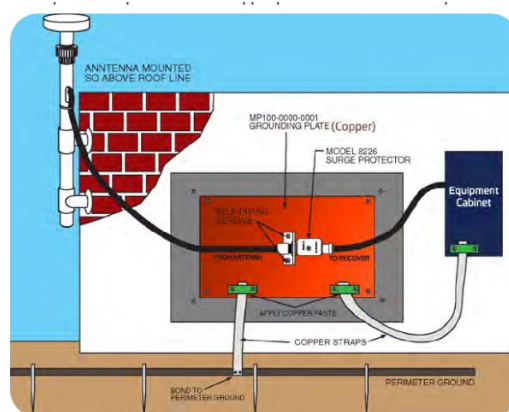


Figure 1-3: Grounding kit panel installation

- Refer to [EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8226 and grounding kit\Grounding kit](#)

Note: This document was obtained from “Engineering Specification” on the Polyphaser website:
<http://www.smithspower.com/brands/polyphaser/products/grounding-and-bonding/cu-spgp>

Grounding kit RoHS compliancy

Q. (From Tony Diflorio) Do you guys know if the 8226 and the 8226-0002-0600 grounding kit are RoHS compliant?

A. (reply from Tom Richardson on 1/18/12): They are RoHS compliant.

Link to a customized RoHS compliancy certificate: [EQUIPMENT\SPECTRACOM EQUIPMENT\8225, 8225S, 8226, 8227 and grounding kit\8226 and grounding kit\RoHS compliancy](#)

Note: This RoHS certificate was created for and indicates Hughes. Need to edit this before forwarding it to anyone else.

Individual components included in the kit:

Process Detail (8226-0002-0600-PD) for assembly of kit

- In Arena at: https://app.bom.com/items/detail-spec?item_id=1217052327&version_id=10443067548
- Refer to: [I:\New Released\Process Details\8226-xxxx-xxxx Process Details\8226-0002-0600](#)

(MP10-0000-0001) Copper ground panel:



- Refer to <http://www.smithspower.com/brands/polyphaser/products/grounding-and-bonding/cu-spgp>
- MFG: apparently purchased from Harger
- **Harger P/N CUSPGW** (in Arena at: https://app.bom.com/supplier-items/detail-sourced?item_id=1203069528)
- **PolyPhaser P/N CU-SPGP** (in Arena at: https://app.bom.com/supplier-items/detail-sourced?item_id=1203069529)

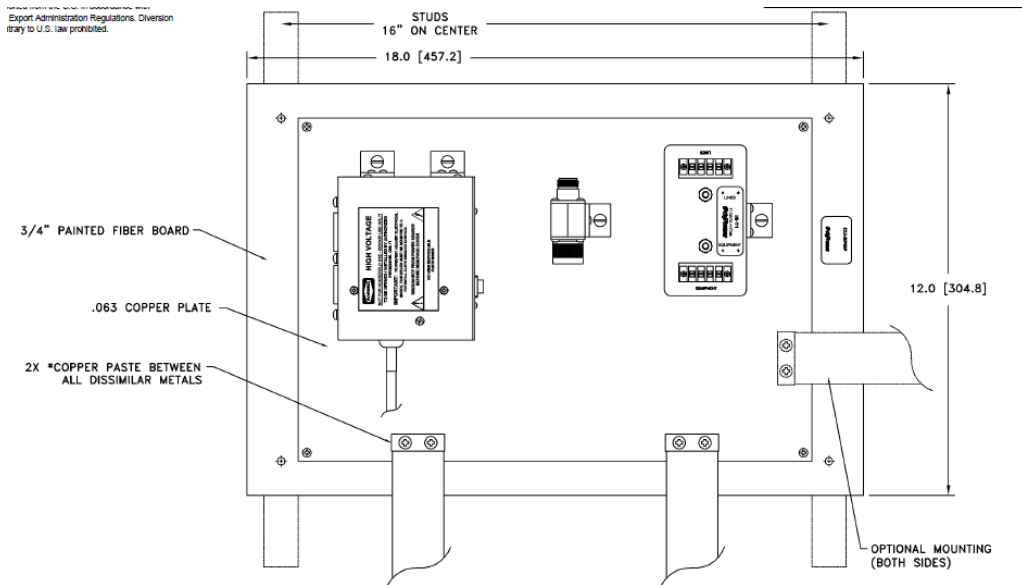
Corrosion/oxidation/minor scratches on the grounding plate when received

- Minor scratches on the surface of the plate will be inherently removed when the plate is installed. The surface needs to be scrubbed with an abrasive pad when it's installed. This will remove any scratches. See the note below
- The copper plate will inherently have oxidation. The surface needs to be scrubbed with an abrasive pad when it's installed. This will remove the oxidation. See the note below

Note: Per the instruction sheet shipped with the grounding kit “The copper surface should be cleaned with an abrasive pad, removing any oxidation or contaminants prior to mounting the protectors”.

Dimensions of the copper plate / Fiber backing board

- (12 x 18 inches, outside diameter of the Fiber board)
- Drawing below (*Polyphaser CU-SPGP*) is from the document referenced above

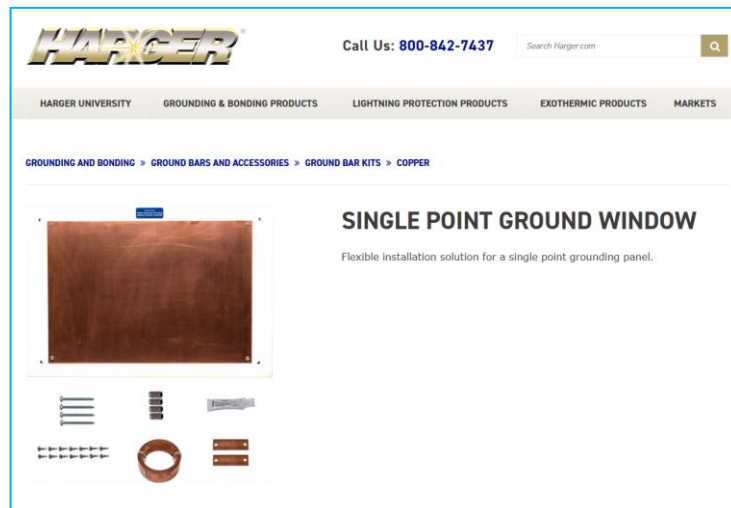


Various Suppliers we can/have purchased the copper plate from:

A) Harger Copper plate (CUSPGPW)

(in Arena) https://app.bom.com/supplier-items/detail-attach?item_id=1203069528

<https://www.harger.com/product/single-point-ground-window>

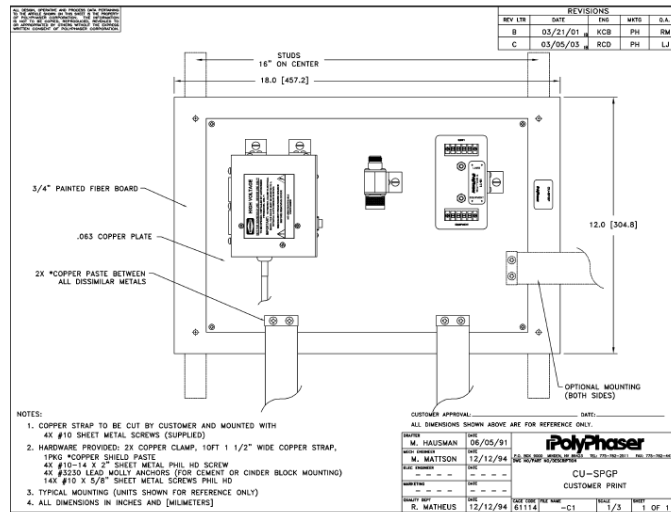


B) PolyPhaser Copper plate (CU-SPGP)

3D CAD Drawing for just the plate (.step file)

- Refer to link at bottom of: <https://www.polyphaser.com/supplemental-hardware-materials-low-inductance-grounding-cu-spgp>
- Also saved in I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8226 and grounding kit\Grounding kit

(Polyphaser CU-SPGP)



C) Nextec?

(MP26-0001-0001) 1/2" to 1" Water Pipe Ground Rod Clamp:

- Refer to: <https://www.platt.com/platt-electric-supply/Ground-Clamps-Dual-Rated/IlSCO/AGC-1/product.aspx?zpid=29106>



(MP26-0002-0001) Copper Post Connector (lug for the cable)

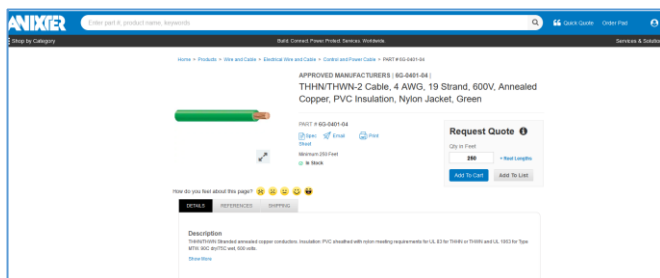
Refer to: <https://www.platt.com/platt-electric-supply/Mechanical-Lugs-Copper-1-Conductor/IlSCO/CP-4/product.aspx?zpid=29150>

- Can accept 14 to 4 AWG cable (4AWG cable supplied)



(W040-0004-0501) 10 Ft of 4 AWG Copper ground cable

- Refer to: https://www.anixter.com/en_us/product-detail.6G-0401-04.html



****Model 8227 GPS amplifier**

Links/shortcuts

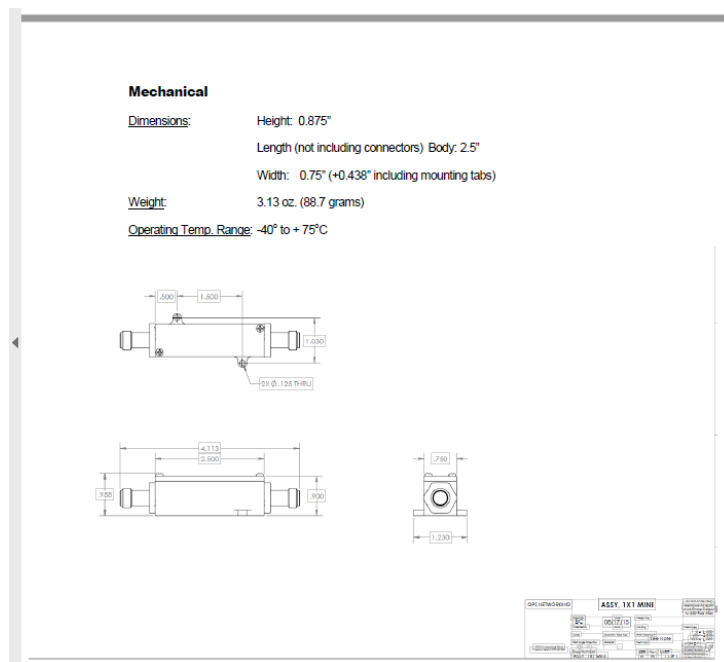
- Shortcut to **Model 8227 Data Sheet**: <I:\Marketing\Product Data Sheets\GPS Antennas & Accessories>
- Shortcut to **Model 8227 in Customer Service**: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8227>
- Shortcut to **MFG data sheet in Eng**: <I:\Engineering\Engineering Shared\Spectracom Parts\067011 - 8227>
- Link to **GPS Networking's datasheet** (their P/N is MLA20RPDC-N with the N indicating type N connectors)
<http://gpsnetworking.com/datasheet%20replacements/MLA20RPDC.pdf>

Part Numbers

#	Item Number ▲	Item Name
1	8227-0001-0600 rev 6	8227 INLINE AMPLIFIER
2	8227-0001-0600-PD rev 6	8227 Inline Amplifier PD
3	8227-1003-0800 rev 2	8227 Inline Amplifier Label
4	8227-1006-0800 rev 1	8227 S/N LABEL DRAWING
5	8227-5000-0050 rev E	8227 User Manual

Mounting/Diagrams/Mechanical drawings

- Refer to “**MLA10RPDC PropdSpec2015.pdf**”: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8227> (drawing excerpted below)



Model 8227 CE Declaration of Conformity

- Refer to : <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Declaration of Conformity>

Note: The Declaration of Conformity for the Model 8227 is included in the SecureSync's Declaration of Conformity Certificate.

Per Dave Sohn (15 Jun 15): it includes EN 60950-1:2006/A11:2009 for safety. We don't test to EN61000-6-1:2007 or EN 61000-6-3:2007, instead testing against EN 55022:2006/A1:2007 for Class A emissions, and EN55024:1998/A2:2003 for immunity.

Model 8227 Specifications

Connectors: Type N Female

Gain: 20 ± 3 dB

Noise figure of inline amplifier, 3.5 dB

VSWR: $\leq 1.5:1$

Power: 3 - 9 VDC, 7.5 ± 1 milliamps

Power draw is 15 mA

- Powered in-line from 5vdc provided by the GPS receiver (no external DC input power required).

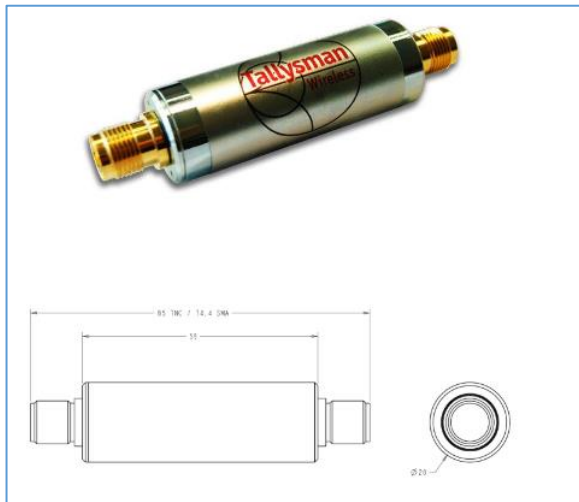
Newer style Rectangular 8227 (our P/N "AR02-1587-2002" from GPS Networking (their P/N MLA20RPDC-N) started shipping around Sept 2011= 9.3 kohms.



- This preamp has **20dB** gain
- Sometime before 12/7/11 (not sure exactly when), we started shipping this preamp from GPS Networking.
- The end that is labeled as ("Antenna DC Thru") goes towards the GPS antenna
- The end that is labeled as ("J1 DC Thru") goes towards the GPS receiver
- Pass-through voltage is about 4.8vdc- Tom Richardson is a little concerned that this voltage may be too low to allow two of these to be installed in-line for greater gain
- **Square 8227** (Shipped after around 5/1/08) = 91kohms on receiver end
- **Circular 8227** ("Starlink", I believe) = (Shipped before about 5/1/08) = 152 ohms on receiver end
- **Square 8227** (GPS networking P/N MLA 20RPDC-N) = ~7 Mohms on J1 (about 3 ohms from end to end)

Qualified alternate source for 8227s

Tallysman Model TW125B (P/N 32-0125B-14)



("ANT": arrow points toward the antenna)

- Refer to ECO 1327 (in Arena): https://app.bom.com/changes/detail-summary?change_id=2393885741&

Description of ECO: Approve Tallysman p/n 32-0125B-14 as alt source for Spectracom part # AR02-1587-2002

Manufacturer's information (Tallysman)

<http://www.tallysman.com/gnss-antennas.php>

MFG: Tallysman Wireless, inc
106 Schneider Road, Unit 3
Ottawa ON K2K 1Y2 Canada
Tel 613 591 3131
Fax 613 591 3121
sales@tallysman.com

Contact Tom Richardson sent to me:

Gyles Panther
gyles.panther@tallysman.com

- **Tallysman P/N 32-0125B-14 (TW125B)**
 - **DigiKey P/N 32-0125B-14-ND** <https://www.digikey.com/product-detail/en/tallysman-wireless-inc/32-0125B-14/32-0125B-14-ND/5808166>

Specs for Tallysman Model TW125B

- **27dB** nominal gain

Refer to datasheet:: <https://www.tallysman.com/product/tw125b-inline-rf-amplifier/>



TW125B Low Current / Low Voltage 1.1 to 1.7 GHz 27dB gain In-line Amplifier

Specifications

Vcc = 3.3V, over full bandwidth, T=25 °C

Electrical

• Nominal Gain	27 dB +/- 0.2 dB typ.
• Pass Band Ripple	+/- 0.5 dB
• Impedance	50 Ohms
• Noise Figure	2 dB typ.
• Bandwidth	1.1 to 1.7 GHz
• Input VSWR	1.3:1 typ.
• Output VSWR	1.3:1 typ.
• Reverse Isolation	>35 dB
• Output P1dB	+9dB min
• Group Delay (w/o cable)	<1ns
• Output IP3	+14dBm
• Supply Range voltage	3 to 16 VDC Nominal, 12 VDC recommended operating max
• Supply Current	11 mA typ.

Mechanicals & Environmental

Mechanical Size (body dimensions only)	2.32" L x 0.787" Dia. (59 mm L x 20 mm dia.)		
Connectors	SMA Jack, TNC Jack, or N-Type Jack		
Torque Limitations (in. lbs)	N-type 6.5 – 8	TNC 9 – 11	SMA 3.6 – 4.5
Operating Temp. Range	-40 to +85 °C		
Enclosure	Nickel-plated brass		
Environmental	RoHS, REACH, and IP67 compliant		
Warranty	One year – parts and labour		

Ordering Information

• TW125B - 27dB gain In-Line Amp with SMA female on both ends	32-0125B-00
• TW125B - 27dB gain In-Line Amp with TNC female on both ends	32-0125B-01
• TW125B - 27dB gain In-Line Amp with SMA female on antenna side and TNC on output side	32-0125B-02
• TW125B - 27dB gain In-Line Amp with TNC female on antenna side / SMA female on output side	32-0125B-03
• TW125B - 27dB gain In-Line Amp with N-Type female on both ends	32-0125B-14 (premium applies)



36 Steacie Drive, Ottawa ON K2K 2A9 Canada
Tel +1 613 591 3131 Fax 613 591 3121 sales@tallysman.com

Per Alan Craford with Tallysman support: the preamp should be installed as close to the base of the antenna as possible. 200ft from the antenna is way too far away.

5vdc output from the preamp (to power the antenna)

- **GPS Networking:** 5vdc pass-through from the GPS receiver (this amp **consumes max 15mA**)
- **Tallysman (TW125B)** 5vdc pass-through from the GPS receiver (this amp **accepts 3 to 16vdc, consumes max 11mA typical**)
- **Starlink:** 5vdc pass-through from the GPS receiver (this amp **consumes 8 mA at 3vdc**)
- **Raven:** 5vdc pass-through from the GPS receiver (this amp **consumes <10mA**)

Cable connections to the preamp

Cable connections to the Model 8227 (GPS networking P/N “AR02-1587-2002”) (markings on the preamp)

- “Antenna” = Install this side on the cable to the antenna
- “J1” = Install this side towards the GPS receiver.

A) Cable connections to the Model 8227 (Tallysman 32-0125B-14 (TW125B) (markings on the preamp)

“IMPORTANT: Amplifiers are directional and must be installed in the orientation indicated on the product label.

(Arrow points towards the antenna)”

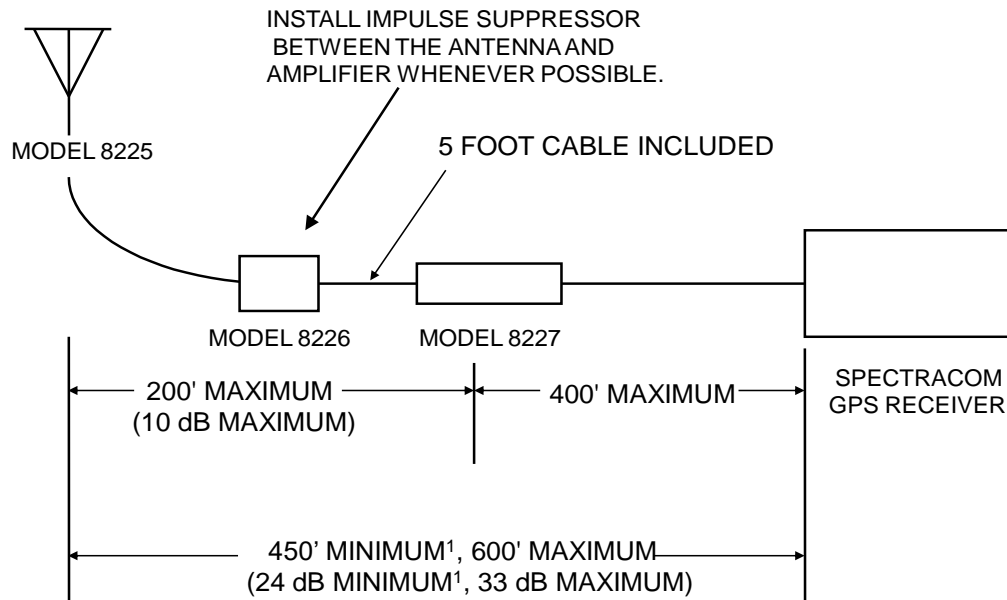
Cable connections to the Model 8227 (“MLA RPDC-N”) (markings on the preamp)

- “Antenna DC thru”: Install this side on the cable to the antenna
- “J1”: Install this side towards the GPS receiver.

IP rating: Refer to: [IP rating/Ingress rating \(for all products\)](#)

A) Single Model 8227 preamp installed

Note: below diagram should be updated to reflect 8230 antenna and longer cables)



1. Minimum cable required for Models 8183, 8183ES and 8189.

B) Dual Model 8227 preamps in-line between antenna and GPS receiver

4) RES-T/Res-SMT-GG/ublox (such as SecureSyncs)

There really are no “requirements” for using two inline GNSS amps, and there is nothing you need to do to the SecureSync or its antenna to support this. There is just one general recommendation on their placements inline, relative to the antenna for optimal operation.

The two Model 8227 preamps’ general recommended locations (relative to the cable distance from its Model 8230 GNSS antenna) are to help ensure each preamp gets a good amount of signal (not too much signal, but not too much noise, either).

For instance, it wouldn’t be very good to either:

- To put both preamps 5 ft apart from each other, with both located only 10 ft from the antenna (then 700 ft of cable to the receiver, for instance).
- Or to put both preamps within only 100 ft of the SecureSyncs, where they will be amplifying a lot of noise as the signal gets from the antenna through all the cabling to the amps).

The Model 8226 surge suppressor should be located on the antenna’s side of both Model 8227 preamps (**Model 8230 antenna** -> cable -> **Model 8226 surge suppressor** -> cable -> **1st 8227** -> cable -> **2nd 8227** -> cable -> **SecureSync**). This will allow the surge protector to help protect both Model 8227 preamps from surge damage, in addition to it also protecting the SecureSync,

The recommended approximate cable distances for optimal operation is to place the first Model 827 preamp approximately **100ft to 200ft** of cable away from the Model 8230 GNSS antenna, Then the second preamp should be approximately **300 ft of cable length from the first preamp**. Then cable the rest of the distance to the

SecureSync.

However, in the “real world” you may have to deal with conduit and access points in the conduit. Ideally if there is conduit involved, you would like the amplifiers located near access points in the conduit. the distances above are general recommendations and not “hard-set” to any specific value (if its easier to put the second preamp 350 feet from the first preamp, instead of 300 feet, not a problem at all!!

5) M12 receivers

M12 receivers have a typical current draw of about 15ma with a max of 80ma. The Model 8227 is about 7.5ma and the Model 8225 is about 27ma (~35ma combined)

A second preamp will add 7.5ma to the cable. Total with second preamp is 42ma (Within the 80ma maximum). However, due to amplifying noise, we don't recommend a third preamp be added to the line (However it might work- just hasn't ever tested it).

With two preamps, the first preamp should be about 10 dB loss from the antenna and the second preamp should be 10 dB loss from the first preamp. (**Note:** we have only tried the use of a second preamp here with a UT and VP- We Haven't tested for M12 use of two preamps).

6) Resolution-T GPS receivers

There is no specific rule for where to put the amplifiers, but the general rule is to install the amplifiers before the signal to noise ratio deteriorates due to the cable attenuation

It is generally best to install them closer to antenna then the NetClock

My personal recommendation you be first amplifier between 100 and 200 ft from antenna (you have successfully done 300 ft with the NTT installation) Second amplifier about 300 ft away from the first amplifier. Long cable from second amplifier to NetClock.

However, in the real world you have to deal with conduit and access points in the conduit. Ideally if there is conduit involved you would like the amplifiers located near access points in the conduit.

Email from Dave Lorah to Sylvain (We have in the past used two inline amplifiers to allow a 300 meter (1000 Ft) cable run. This does work. It is best to install the 8227's toward the front half of the cable length, one near the antenna and one halfway between the antenna and the receiver.

****GPS filters (Prevent signals from escaping through the GPS cable):**

- Refer to GPS Networking <http://gpsnetworking.com/GPS-filters.asp>
- As of at least Nov, 2017, Spectracom does not offer any GPS filters.

GPS OPTIC ISOLATORS/ CABLE/ MEDIA CONVERTERS (COAX AND FIBER)

****Model 1169 GPS Optic Isolator (TX and RX) for Invensys timing boards:**

- Refer to “1169” in the Timing board cust assist document: <I:\Customer Service\1- Cust Assist documents\TimingBoardCustAssist.pdf>

****1201-KIT-RF1-DUC (“StarLink”) Raven/Forsberg DUC**

- Down-Up coax cable converters for **GPS L1 band only** (Long distance coax cable runs)

Please note the 1201-KIT-RF1-DUC is **GPS L1 band only** (not compatible with SAASM or other constellations besides GPS)

NOTE: the DUC product line has been sold by Raven Industries to a company called Forsberg in the UK.
<http://www.forsbergservices.co.uk/>

Per Dave Sohn (18 oct 15) We are continuing to offer the DUC. We are just sourcing it from Forsberg now instead of Raven. So, customers can still purchase it from us directly.

Note: This kit uses coax cable. For fiber optic cabling instead, refer to: [Optical Zonu Fiber GPS converters](#)

Links/Shortcuts

- **Refer to** (Forsberg data sheet):
 - <http://www.forsbergservices.co.uk/index.php/products/gnss-gps-line-amplifiers/down-up-conveter/>
 - https://spectracom.com/sites/default/files/document-files/gps_antenna_rf_down-up_converter_kit_0.pdf
- **Bill of materials** (1201-0002-0600) in Arena: https://app.bom.com/items/detail-bom?item_id=1202845076&version_id=10404383268
- **Shortcut to the Spectracom Model 1201 datasheet (“GPS Antenna RF Down-Up”):**
<https://login.microsoftonline.com/>
- **Shortcut to Manufacturer’s datasheets:** [I:\Engineering\GPS Antennas](#) (look for “Raven”) Note this is the previous vendor of the DUC. Now it’s sold by Forsberg. Send our data sheet at the link above.
- **Shortcut to Model 1201 manual (1201-5001-0050) in Arena:** https://app.bom.com/items/detail-spec?item_id=1203165703&version_id=10221246328
- **Raven contact information:** Refer to: [** \(“StarLink”\) “Raven Link” system](#) (in next section down)

Part Numbers associated with the DUC:

- **Our P/N:** Refer to the “DUC Kit, “**1201-KIT-RF1-DUC**” section further below

NSN numbers assigned to DUCs

- Refer to case 206141

Email below from Dave Lorah (19 Aug KW) regarding case 206141

I believe the NSN for the Down/Up Converter system consists of three parts.

- **The Down Converter/Antenna: MP33R-0000-0003**, 5895-01-574-2108
- **The UP Converter: MP33R-0000-0002**, 5895-01-574-2109
- **The Power supply for the Up Converter**, 6130-01-599-0137

RMA's/repairs of the DUC

Email from Dave Lorah (9 Dec 15) The GPS Down/Up Converters Antenna Systems can be repaired if under one year old. In the event one has failed after that date, we cannot repair them, they must be replaced.

The Down/Up Converters do carry a five (5) year warranty for manufacturing defects and component failures. Lightning and surge damage is not covered however.

Spectracom can evaluate these units and check their operation. There is a \$200 evaluation fee per order for the equipment. If there is something simple we can repair we will make all attempts to do so, but any component type failures would mean new replacement of the entire module is necessary. If the module is not lightning/surge damaged and needs replacement it will be replaced at no charge. RMA's with no problems found are subject to the \$200 evaluation fee.

CE and Declaration of Conformity/ PSE (for Japan), RoHS and FCC compliancy



CE certification and DoC

- Refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Declaration of Conformity>

Note: The Declaration of Conformity for the GPS Down/up converter is included in the SecureSync's Declaration of Conformity Certificate

Per Dave Sohn (15 Jun 15): it includes EN 60950-1:2006/A11:2009 for safety. We don't test to EN61000-6-1:2007 or EN 61000-6-3:2007, instead testing against EN 55022:2006/A1:2007 for Class A emissions, and EN55024:1998/A2:2003 for immunity.

RoHS and FCC compliancy

- Refer to labels in the pictures above (as of at least Jan, 2018, the Forsberg data sheet doesn't provide ratings info)

Email from Dave L (16 Jan 18) The GPS Down/UpConverter 1201-KIT-RF1-DUC specs do indicate it is ROHS compliant. It also is FCC and CE compliant.

PSE Rating (for Japan)

Up converter and its associated power pack (PSU)

Q I noticed that perhaps the AC adaptor had already passed Japanese safety regulation and have a PSE printing. It seems there are some printing of the mark and Japanese importer. I cannot assert it because the drawing has not enough resolution.

A Email from Jean-Arnold (5 Feb 18) I don't think there is the printing, I know this has all the EU/US (CE, UL, FCC) standards, but I can't confirm as we don't have stock here.

Anyway, this is a simple AC/DC convert that you can replace with any compatible PSU with same characteristics, should this be a very strong requirement.

Supported GPS/GNSS bands

not compatible with Glonass

- GPS L1 only (not L2 which is required for SAASM)
- **Note:** Not Compatible with Glonass
- **Q.** Will we have the GLONASS capabilities with our Antenna Down Up converter systems for cable runs over 1000ft? 1201-KIT-RF1-DUC & 1201-KIT-FIB1-DUC systems?
- **A.** The DUC and fiber kit don't work for Glonass (or any other constellations, besides GPS L1 band)

BOM (list of items included)

- **Bill of materials (1201-0002-0600) in Arena:** https://app.bom.com/items/detail-bom?item_id=1202845076&version_id=10404383268

201-0002-0600 In Production 0 0 0 0 0 0

201-KIT-RF1-DUC

VISION 4 - In Production Effective as of 01/29/2016 09:14:30 AM, Unshared

Bill of Materials Files Revisions Sourcing Costing Compliance Where Used Projects Quality Tra

Identified Flat Sourcing Costing Purchasing Custom Redline Compare Lookup

contains 7 first-level Items, 7 line Items, 7 unique Items, 0 of which are shared.

#	ITEM NUMBER	ITEM NAME	CATEGORY
1	1201-1002-0800 rev 5	1201-KIT-RF1-DUC Kit Label	Label
2	1201-5001-0050 rev 4	Manual, GPS RF/Coax DUC Instructions	Manual
3	CP08-0007-5001 rev 1	ADAPTER, BNC (F) - TNC (M)	Adapter
4	CP09-0007-5001 rev 1	ADAPTER, N (F) - TNC (M)	Adapter
5	E025-0007-0002 rev 1	Antenna Surge Arrestor, TNC-TNC, 50 MHz	Integrated Circu
6	MP02-0003-0002 rev 2	LABEL STOCK, 6 UP	Label
7	MP33R-0000-0001 rev 2	DUC, Coaxial, with Power Supply	Miscellaneous Mechanical

Installation info

- **(very basic info)** https://www.navtechgps.com/assets/1/7/DUC-1-v1-01_DS.pdf
- Even better doc (1205-5001-0050 manual) in Arena: https://app.bom.com/items/detail-spec?item_id=1203165703&version_id=10221246328
- <https://forsbergpnt.com/wp-content/uploads/2018/11/A0501-09-0026-DUC-Quick-Start-Guide-v1.00.pdf>

Q Do you have an installation manual for GPS Antenna RF Down-Up Converter Kit?

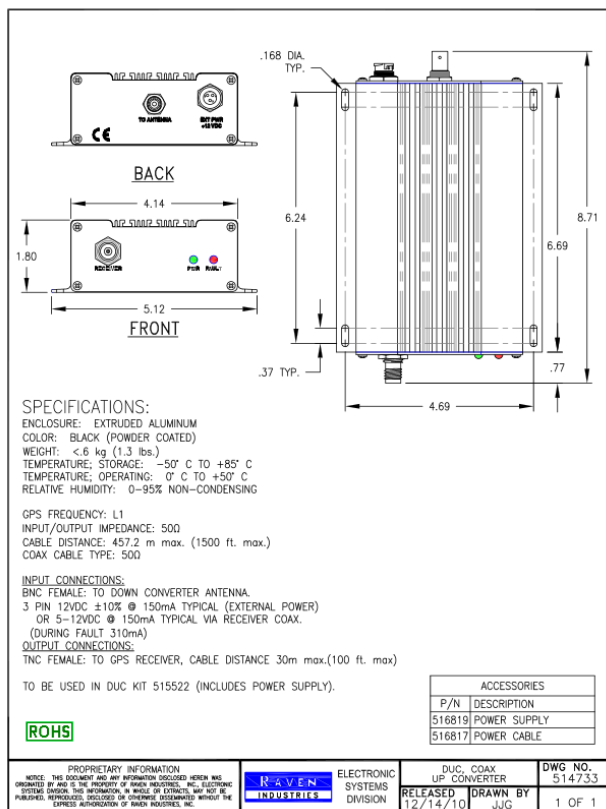
I need it to submit to customer for their approval. Or anything that shows its operation in a Spectracom GNSS setup with pictures or diagrams

A Datasheet: https://spectracom.com/sites/default/files/document-files/gps_antenna_rf_down-up_converter_kit_0.pdf

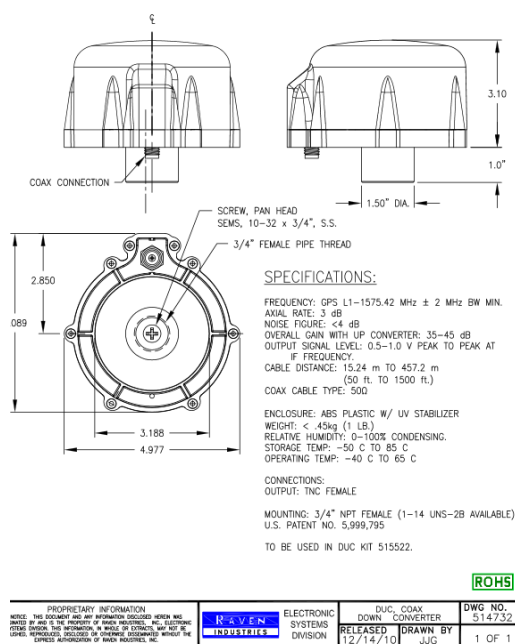
Here is something from the Forsberg (formerly Raven) website: https://www.navtechgps.com/assets/1/7/DUC-1-v1-01_DS.pdf

This is all I could find as far as documentation for this product.

Up Converter



GPS antenna / Down converter



Up Converter



GPS antenna / Down converter



Coax cable connectors on Antenna/Up converter/Surge suppressor



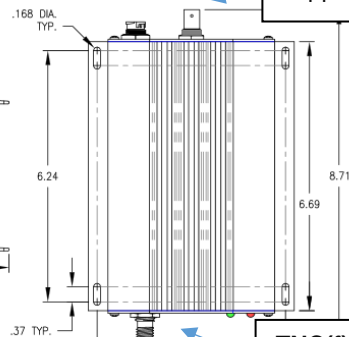
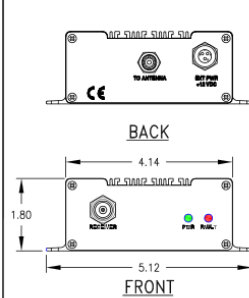
TNC(f) connector on bottom of antenna/down converter

'TNC(M)' to 'BNC(F)' adapter, (Spectracom P/N **CP08-0007-5001** (provided in kit). TNC end attaches to the bottom of the antenna and BNC end attaches to customer supplied coax cable going to the Surge suppressor



TNC(f) connectors on both sides of PolyPhaser P/N AGXZ+15TTF-A (Spectracom P/N E025-0007-0002) surge suppressor

BNC(f) connector (input from DUC Antenna/supplied surge suppressor, via customer-supplied BNC to BNC cable)



TNC(f) connector on edge of Up converter (output to the time server/GNSS receiver)

SPECIFICATIONS:
ENCLOSURE: EXTRUDED ALUMINUM
COLOR: BLACK (POWDER COATED)
WEIGHT: <.6 kg (1.3 lbs.)
TEMPERATURE, STORAGE: -50° C TO +85° C
TEMPERATURE, OPERATING: 0° C TO +50° C
RELATIVE HUMIDITY: 0-95% NON-CONDENSING

GPS FREQUENCY: L1
INPUT/OUTPUT IMPEDANCE: 500
CABLE DISTANCE: 457.2 m max (1500 ft. max)
COAX CABLE TYPE: 500

INPUT CONNECTIONS:
BNC FEMALE: TO DOWN CONVERTER ANTENNA.
3 PIN 12VDC ±10% @ 150mA TYPICAL (EXTERNAL POWER)
OR 5-12VDC @ 150mA TYPICAL VIA RECEIVER COAX.
(DURING FAULT 310mA)
OUTPUT CONNECTIONS:
TNC FEMALE: TO GPS RECEIVER, CABLE DISTANCE 30m max.(100 ft. max)

TO BE USED IN DUC KIT 515522 (INCLUDES POWER SUPPLY)

ROHS

ACCESSORIES	
P/N	DESCRIPTION
516819	POWER SUPPLY
516817	POWER CABLE

'TNC(m)' to 'Type N(f)' adapter (Spectracom P/N **CP09-0007-5001** (provided in kit) to attach one end of the customer-supplied Type N(m) to Type N(m) coax cable to the Up converter. The other end of the coax cable attaches to the time server.

customer-supplied **Type N(m) to Type N(m)** coax cable

Type N(f) connector on NetClock/SecureSync.

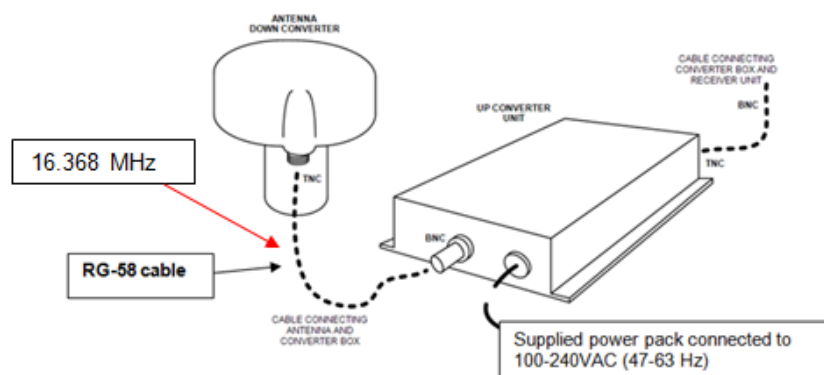
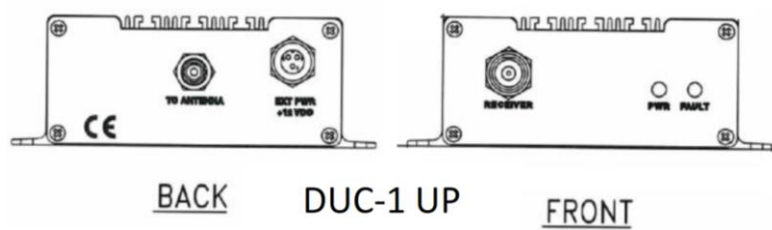
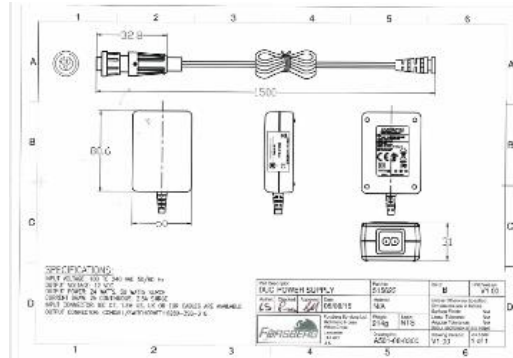


Figure 1: Down-Up Converter Connections

Note: Figure above is from the DUC manual (1201-5001-0050)

Provided Power supply (PSU) for the Up Converter (our P/N MP33R-0000-PS01)

- Forsberg P/N: 515623
- Our P/N for power supply/line cord: MP33R-0000-PS01 (in Arena): https://app.bom.com/items/detail-sourcing?item_id=1211922987&version_id=10368772228
- This appears to be the original Starlink/Forsberg adapter Forsberg now sending power pack/adapter with a standard IEC jack, instead of using a separate wall wart.
- The following diagram (MFG P/N **A0501-08-0300**) is stored in: <I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENDUC>



Newer 12vdc adapter with integrated IEC jack (no separate “wall wart”) (pictures taken Sept 2019)

- **MFG and MFG Model and P/N:** Stontronics Ltd. **Model:** DSA-42D-12.1 **P/N:** T3241ST

Bottom of adapter

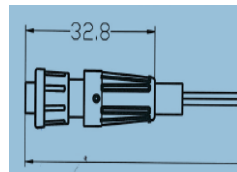


Connector on end of cable:

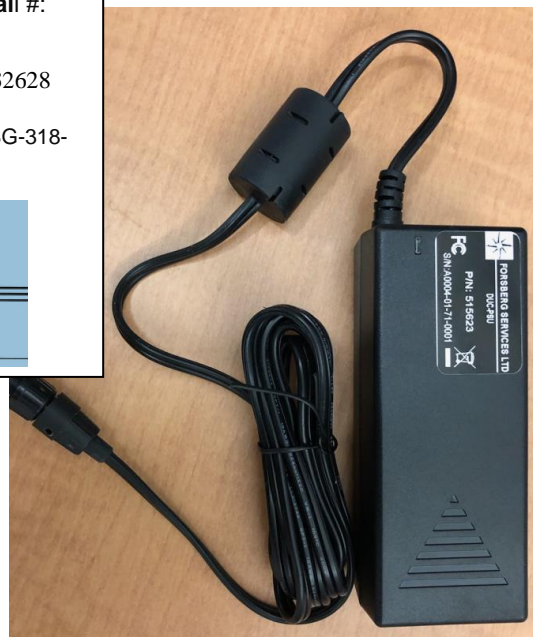
Switchcraft/Conxall #:
16280-3SG-318

Allied Stock #: 70932628

Digikey #: 16280-3SG-318-ND



Top of adapter



Side of adapter



IEC “C14” Power Connector

Pinout info

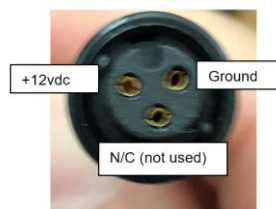


Side of Up Converter



End of adapter

Note: Only two conductors/wires out of adapter (not three). The third pin on the adapter output is not used/connected.



Dimensions and weights:

A) Up converter:

Size and Weight

- Dimensions: 6.675"D x 5.12"W x 1.75"H
- Weight: 20 ounces

B) Down converter:

Size and Weight

- Height: 3.5"
- Diameter: 4.5"
- Weight: < 1.3 lbs.

Partial Email from Tony DiFlorio to a customer (10/24/11)

The link below takes you to the product dimensions for the transmitter and receiver from Raven Industries. Please note this product is a purchased/resold product but we package it into a kit for the customer so that he can use it with our NetClock. <http://starlinkdgps.com/wp-content/uploads/2011/04/RVL-1-FIBER.pdf>.

Distance limitations / recommended antenna cable to use between antenna and up-converter

- **Copper DUC:** Optimized for RG-58/RG-59 cable for up to 1500 feet (457 meters).
- **Input power (to the Up converter):** 100-240VAC (47-63 Hz)
- **DC output (to the antenna/down converter):** +12VDC (2.1 Amps)
- **The DUC's IF output (low frequency) though the BNC cable is 16.368 MHz**

Cable impedance (50 ohms versus 75 ohm) such as using RG-59 instead of RG-58

Q Will RG-59 (75 ohm cable - not 50 ohm) work with the raw GPS signal and the down-converted GPS signal?

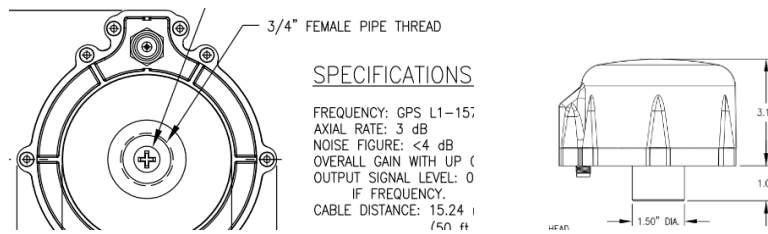
A Per Tom Richardson (9 May 16) "Short answer is yes. There might be some mismatch because of the different impedance but it should be minimal"

For more info on transmission line impedance, refer to sites such as:

<http://www.bluejeanscable.com/articles/impedance.htm>

DUC Antenna Mounting/Antenna mast/ANT-KT bracket

- We don't supply an antenna mast with the DUC antenna (can be created locally by the customer)
- The antenna/Down converter has a threaded $\frac{3}{4}$ inch Female Pipe thread connector



Email from Tom Richardson to Sadie (29 Nov 17) Takes a $\frac{3}{4}$ inch male pipe thread. We used to offer a piece of plastic pipe with an adapter. I forget the number.



This should be available at their local hardware store or Amazon:

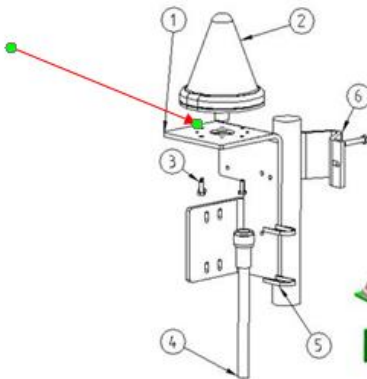
[https://www.amazon.com/Genova-Products-30407CP-4-Inch-](https://www.amazon.com/Genova-Products-30407CP-4-Inch-Adapter/dp/B000BQNEI8/ref=pd_sim_86_3?encoding=UTF8&psc=1&refRID=KKAPCYT631YPYP3WGNYZ)

[Adapter/dp/B000BQNEI8/ref=pd_sim_86_3?encoding=UTF8&psc=1&refRID=KKAPCYT631YPYP3WGNYZ](https://www.amazon.com/Genova-Products-30407CP-4-Inch-Adapter/dp/B000BQNEI8/ref=pd_sim_86_3?encoding=UTF8&psc=1&refRID=KKAPCYT631YPYP3WGNYZ)

Follow-up from TR to Sadie: My point is that they would need a $\frac{3}{4}$ inch male pipe fitting to mount the antenna. Whether it is a piece of pipe or an adapter doesn't matter. Because of the different situations that can occur I believe we leave it up to the customer.

Desire to use the ANT-KT bracket (Epsilon bracket) with the Raven/Forsberg DUC down-up converter's antenna

- (9 Jan 17) Dave L and Sadie confirmed the DUC down converter antenna is not compatible with this aluminum bracket, without modification of the bracket. There is no way to attach the DUC antenna to the bracket, because the hole at the top of the bracket is too small for the antenna to go through, and there is no way to fasten the antenna to this bracket.



Special Surge suppressor for the down-up converters (included in the kit)

Note: The Model 8226 is not compatible with the DUC.

- The DUC low frequency is **16.368 MHz**, so the surge suppressor should be specified for the frequency
- The DC voltage is 12V, so a 15V Surge Suppressor is good.
- We provide a PolyPhaser P/N AGXZ+15TFTF-A (Spectracom P/N E025-0007-0002, in Arena at: https://app.bom.com/items/detail-spec?item_id=1202836773&version_id=10221219168&orb_msg_single_search_p=1&redirect_seqno=8641560847)



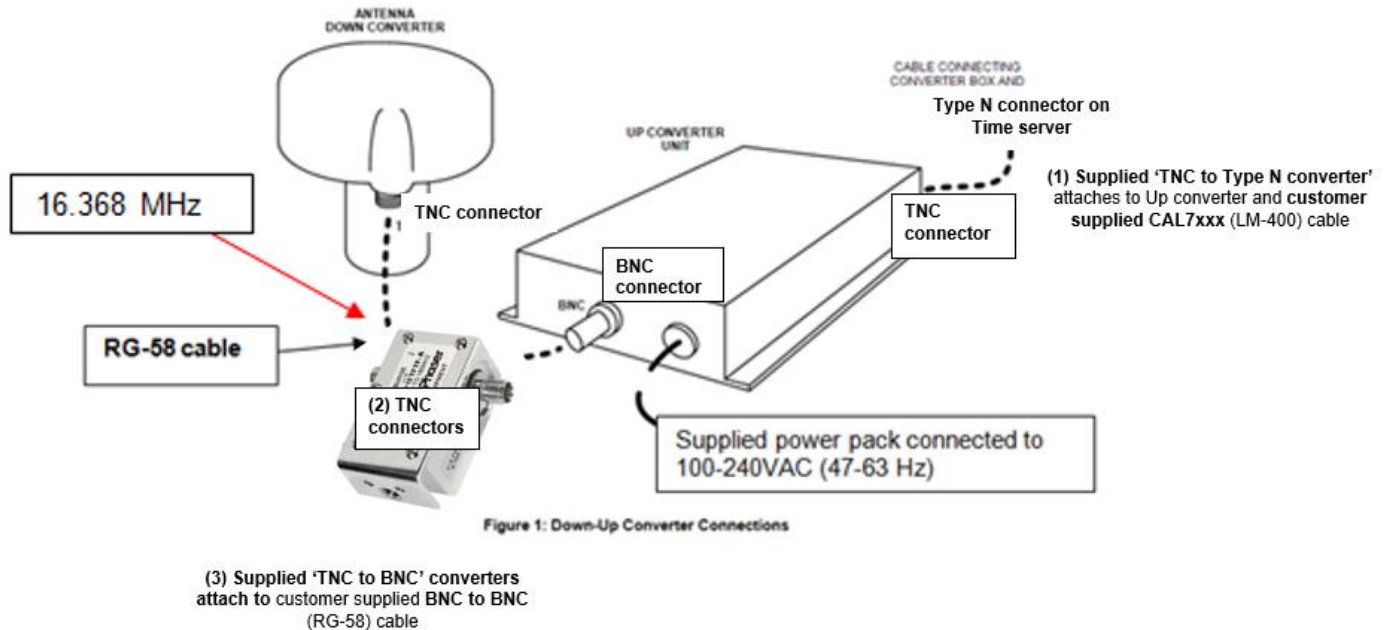
- Polyphaser Product data sheet: <http://polyphaser.com/products/rf-surge-protection/agxz-plus-15tftf-a>
- This device has two (2) TNC Female connectors on it.
- This surge suppressor is included in the DUC kit (1201-KIT-RF1-DUC, as indicated below):

Bill of Materials

DUC Kit, 1201-KIT-RF1-DUC (P/N: 1201-0002-0600)

in Arena: [https://app.bom.com/items/detail-](https://app.bom.com/items/detail-spec?item_id=1202845076&version_id=10404383268&orb_msg_single_search_p=1&redirect_seqno=8641538899)

[spec?item_id=1202845076&version_id=10404383268&orb_msg_single_search_p=1&redirect_seqno=8641538899](https://app.bom.com/items/detail-spec?item_id=1202845076&version_id=10404383268&orb_msg_single_search_p=1&redirect_seqno=8641538899)



(DUC kit includes the following items)

- 1 GPS antenna, with built-in down converter (Our P/N MP33R-0000-0001)



- 1 Up converter (MP33R-0000-0002)



- 1 surge protector (E025-0007-0002) (Polyphaser P/N: AGXZ+15TFTF-A)



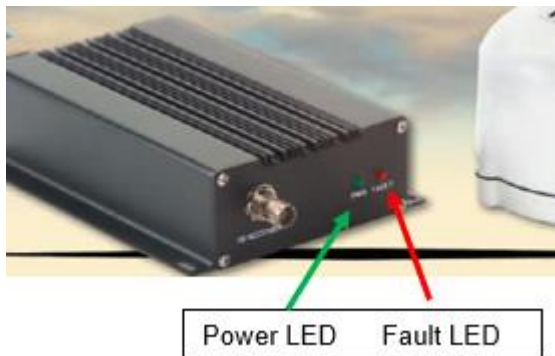
- **3 TNC to BNC adaptors (CP08-0007-5001)**

- (1) For connection to the bottom of the antenna/down converter
- (2) For each side of surge suppressor

- **1 TNC to type N adaptor (CP09-0007-5001)**

To attach the output of the Up converter to the customer-supplied cable going to the SecureSynchs

Green/Red LEDS on the edge of the Up converter:



Red Fault LED: Indicates a short or open being detected between the up converter and the GPS antenna.

Green “PWR” LED: Indicates power is applied to the Up converter (see important Note below):

NOTE: When the Up Converter Unit is connected to a receiver, the power LED on the unit may illuminate if the receiver is set up to power the antenna. This is a FALSE power-connect indication. The supplied external Converter Box Power Cable must still be connected for the unit to function properly and for the GPS receiver to track satellites.

Troubleshooting the DUC system

- 1) Make sure the GPS antenna/down converter assembly is outdoors with good view of the sky
- 2) Verify there is “near 12vdc” present at the antenna-end of the RG-58 cable.
- 3) Make sure there isn’t a Spectracom Model 8226 surge suppressor installed with this system. The Model 8226 is NOT compatible with the DUC. due to the lower frequency of the DUC.
- 4) Check the Power and Fault LEDS on the Up Converter:

- 5) The Fault LED lit indicates a likely open or short is occurring in the cable between DUC and Up converter.
- 6) See the Note above discussing how the Power LED can give a false indication of external 12vdc input being present, because of the 5vdc being supplied by the GPS receiver into the Up converter.
- 7) **GNSS receiver tracking only a few satellites (no more than 12):** the DUC is **GPS only** (not compatible with any other constellation) so only GPS satellites can be tracked.,

**** (“StarLink”) “RavenLink” 1201-KIT-FIB1-DUC Fiberlink system Kit (Discontinued)**

Note: Discontinued- replaced by Optical Zonu fiber converter

- Refer to Optical Zonu section for this replacement)
- Link to Optical Zonu system (replacement to the Raven Fiberlink) in this document: [Optical Zonu Fiber Optic GPS Signal Distribution System](#)

Please Note (29 Jan 2015) Raven has discontinued this product (with no alternative available from them). So it's no longer available.

- Refer to ECO 0287 (https://app.bom.com/changes/detail-summary?change_id=2384747104)

Note: This kit is for fiber only- not for coax cable. If coax cable is desired, refer to: [** \(“StarLink”\) Raven/Forsberg DUC - Down-Up coax cable converters for GPS \(Long distance coax cable runs\)](#)

Shortcuts

- Shortcut to Spectracom Model 1201 datasheet/manual: Don't believe there is one yet
- Update to this: March 2013, Product Management decided not to release one.
- Shortcut to Manufacturer's datasheets: [I:\Engineering\GPS Antennas](#) (look for “Raven”)

Declaration of Conformity

Refer to: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Declaration of Conformity](#)

Note: The Declaration of Conformity for the GPS fiber optic converter is included in the SecureSync's Declaration of Conformity Certificate.

Per Dave Sohn (15 Jun 15): it includes EN 60950-1:2006/A11:2009 for safety. We don't test to EN61000-6-1:2007 or EN 61000-6-3:2007, instead testing against EN 55022:2006/A1:2007 for Class A emissions, and EN55024:1998/A2:2003 for immunity.

Refer to: <http://starlinkdgps.com/products/fiber-link/raven-link-fiber-connection/>

Contact info

Raven's phone number: 1-314-656-2277 (this is the number for Donna Stengel- don't know their main number)

Email: starlink@ravenind.com

POCs:

- ~~Tony Zuzzio (Engineering)~~ Tony.Zuzzio@ravenind.com
- ~~Donna Stengel (RMA/Support)~~ Donna.Stengel@ravenind.com 1-314-656-2277
- ~~Mike Hillman (Repairs)~~ mike.hillmann@ravenind.com

Raven warranty: 1 year from date of purchase

Supported GPS bands: L1 only (not L2 which is required for SAASM)

Note: This system is not a DUC system (Down/Up Converter). The raw 1.5GHz GPS signal is received on a standard GPS antenna and then converted to fiber cable via a transmitter located near where the GPS signal enters the building. Then it's converted back to coax at the other end (before it's connected to the GPS receiver)

Raven P/Ns and our P/Ns

Fiber Optic Kit 1201-KIT-FIB1-DUC (Our P/N: 1201-0003-0600)

Kit consists of:

- (1) Fiberlink kit with power supply (Raven P/N 515522, RVL-1-FIBER)
- (2) Female to TNC Male adapter (Our P/N CP09-0007-5001, RF Industries P/N RFT-1234)
- (1) DUC (Our P/N: MP33R-0000-0004)

Individual Spectracom/ Starlink Part Numbers

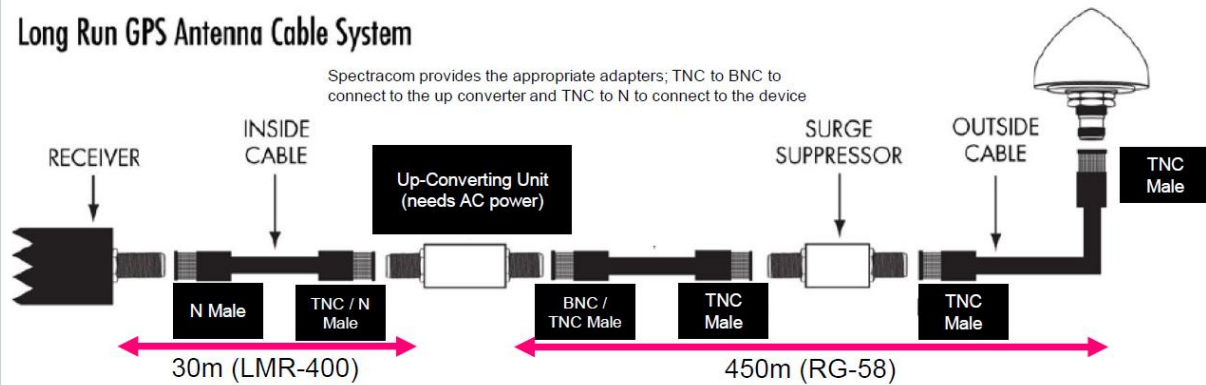
Our Part Number	Description	Starlink's Part Number
CA31-0001-0152	CAF7-1500 fiber optic cable, SX 1500'	518236
MP33R-0000-0004	FiberLink Kit (fiber transmitter and fiber receiver)	515522 (RVL-1-Fiber)
	RavenLink fiber transmitter	516059
	RavenLink fiber receiver	516060

2) Generic RG-58 (50ohm) low frequency coaxial RF cable (for 1201-KIT-RF1-DUC kit)

- When used with Spectracom 1201-KIT-RF1-DUC kit (needs AC power),
- Maximum distance from GPS antenna to Up-Converter unit is approximately 450m.
- Maximum distance from Up-Converter unit to GNSS receiver is approximately 30m
- Spectracom surge protector to be placed as near as possible to the antenna and in a weatherproof box. Surge protector is not weatherproof.
- Up-Converting to be placed near or in the rack, connected to its AC/DC adapter.

Long Run GPS Antenna Cable System

Spectracom provides the appropriate adapters; TNC to BNC to connect to the up converter and TNC to N to connect to the device



6

GPS Antenna RF Down-Up Converter Kit p/n: 1201-KIT-RF1-DUC Surge Protector p/n: E025-0007-0002

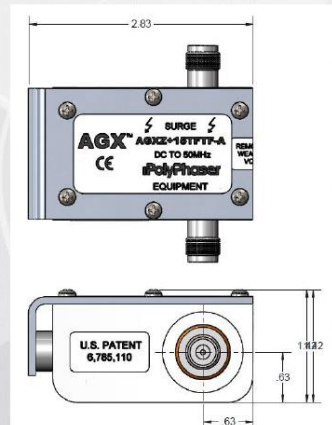
GPS Antenna and
Down-Converter



RF Up-Converter



Surge Protector

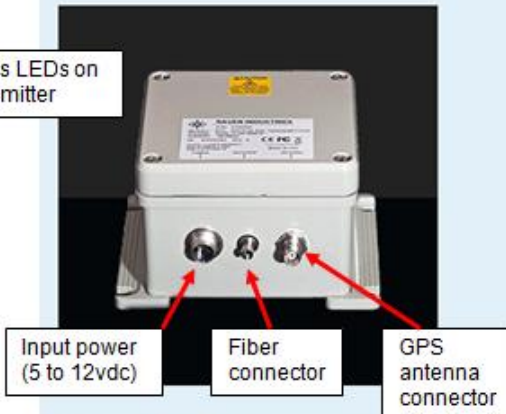


Lit- Power from GPS receiver is applied.
Green- Good
Red - Fault (no signal from the transmitter)

RAVEN LINK SYSTEM

System MODEL Number: RVL-1-FIBER

No Status LEDs on the transmitter



RAVENLINK TRANSMITTER

Product Overview

Product Name: RVL, Ravenlink Transmitter
Input Connection: TNC GPS From Antenna – Designed for Antenna Gain of 34dB \pm 6/3 dB; 2 Pin 12-24V AC or DC
Output Connection: ST Type Fiber Optic Connector for Simplex Multimode 50/125 Micron Cable
Frequency: 800MHz to 1800 MHz
Fiber Length: System allows Fiber Runs of up to 1524 meters (5000 feet) of 50/125 Fiber Optic Cable
Input Voltage: Voltage: AC/DC 12-24V 50/60 Hz; Current: 100-600mA
Input/Output Impedance: 50 Ω
Enclosure: Diecast Aluminum
Color: Beige (Powder Coated)
Weight: <1.36kg (3.0lbs)
Relative Humidity: 0-100% Condensing
Storage Temp: -50°C to +85°C
Operating Temp: -40°C to +70°C
Accessories: Power Supply (516816), Power Cable (516818)
Altitude: 6,096m (20,000 ft)

RAVENLINK RECEIVER

Product Overview

Model Number: SN 001; REV -A
Product Name: RVL, Ravenlink Receiver
Input Connection: ST Type Fiber Optic Connector for Simplex Multimode 50/125 Micron Cable
Output Connection: BNC 50 OHM Female
Frequency: 800MHz to 1800 MHz
Enclosure: Extruded Aluminum
Color: Natural
Weight: <0.92kg (0.21 lbs)
Relative Humidity: 0-95% Non-Condensing
Storage Temp: -40°C to +85°C
Operating Temp: 0°C to +50°C
Accessories: Antenna Fault Reporting LED: Green – Good; Red – Fault
Altitude: 6,096m (20,000 ft)

Function: Fiber optic converter for GPS

Frequency range: 800MHz to 1800 MHz

GPS bands:

- L1 (1575.42 \pm 15) MHz
- L2 (1227.60 \pm 15) MHz

Transmitter's output voltage to the GPS antenna: should be 5vdc.

Fiber cable needed to be used with the fiber converters: ST Type Fiber Optic Connector for Simplex Multimode 50/125 Micron Cable.

Here is the current description we are using. As you can see we have ST connections, and require Multimode cable.

1201-KIT-FIBL-DUC	Down-Up Converter system, Fiber-optic <i>Includes Down-Up Fiber-optic converters and connectors. Requires 115VAC 2A power (power adaptor with wall-plug included) for the Down-Converter in proximity to the GPS Antenna (up to 100 ft. maximum). Must add fiber-optic cable (Type ST Fiber, Simplex Multimode 50/125microns) between down and up-converter; GPS Antenna, Surge Protector, and (2) CAL7xxx Cables (1 between GPS Antenna system and down converter up to 100 ft., 1 between up-converter and time server – CAL7010, 10 ft.).</i>
-------------------	--

Desire to install Fiberlink transmitter outdoors

Email from Donna Stengel with Raven (26 Jun 2013) The Fiberlink Transmitter is a weatherproof enclosure. Putting it inside another enclosure is optional but by putting the transmitter inside another enclosure, it is protected from direct sunlight and should stay under the 70C limit inside the transmitter box.

158F is rather hot even for direct sunlight. If there is still concern about the temperature, then perhaps putting the enclosure in some shade is a possibility?

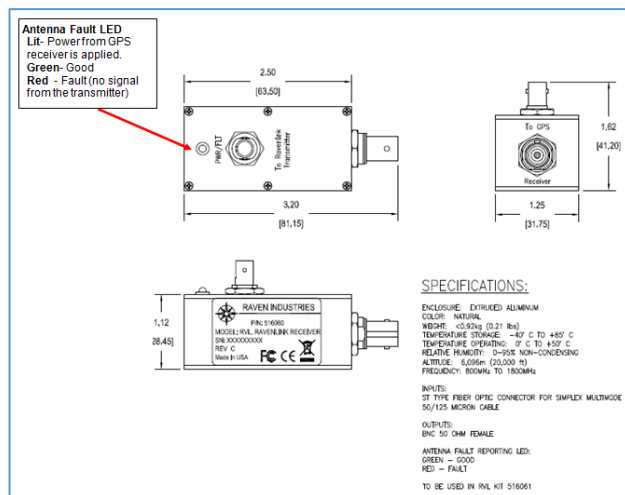
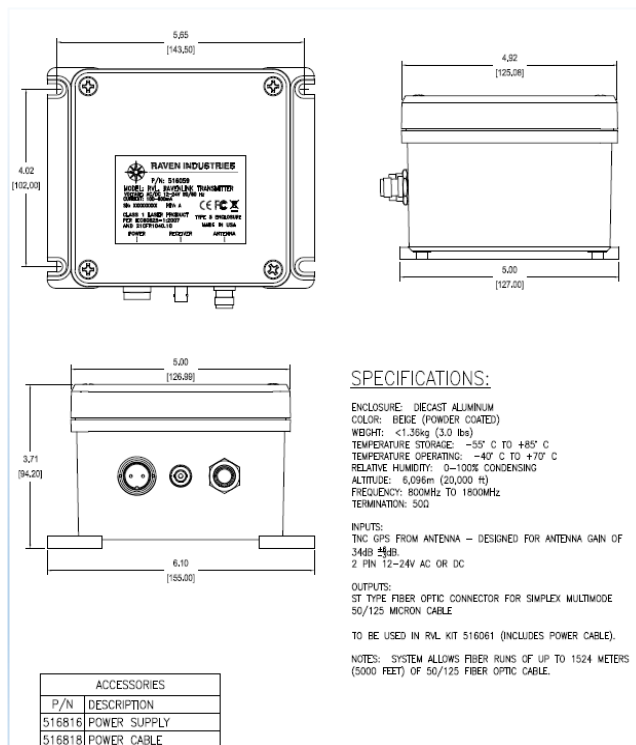
Use of a Model 8226 GPS surge suppressor with the Fiberlink converters/Cable from antenna to Fiber transmitter

- Can use a Model 8226 in conjunction with these converters.
- The 8226 needs to be installed between the GPS antenna and the Ravenlink transmitter (not between the Ravenlink transmitter and receiver).

Email from Dave Lorah (6 May 2013) The total cable length from the GPS Antenna thru the 8226 and ending at the FiberLink Transmitter should not exceed 30 Meters if using RG-5/RG-59. If you use a LMR 400 equivalent the total distance can go up to 250 feet.

Please note the antenna coaxial cable connection on the FiberLink Transmitter is a TNC type. The GPS Signal output connector on the Fiberlink Receiver is a BNC type. The FiberLink Kit contains adapters to convert these to type "N". The cable connection on the 8225 GPS Antenna, the 8226 Surge Suppressor and the SecureSync are all Type "N" connectors. So, all cables connecting these devices will need type "N" Male connectors.

Functional description



Email from Tom Richardson (5/21/12)

See attached for picture and data sheet. (I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\Raven GPS converters)

Antenna is supplied by us or customer, i.e. 8225. Antenna is connected to Fiber optic transmitter by coaxial cable. Fiber optic transmitter puts out 5V DC to power antenna. Fiber optic transmitter is powered by AC-DC power supply mounted at roof or wherever the transmitter is located.

The power supply is **NOT** weatherproof so should be in shelter somewhere.

The fiber optic transmitter sends GPS signal over fiber cable, 50/125 Micron Simplex Multimode with ST connectors, to fiber optic receiver where it is converted back to electrical GPS signal. There is no down convert in this fiber connection. Fiber optic receiver is powered by SecureSync 5V from antenna connector on SecureSync.

Connectors are TNC at transmitter to antenna and BNC at receiver to SecureSync. This is handled in Kit that Will made up 1201-KIT-FIB1-DUC. This has fiber link transmitter, receiver, power supply and connector adapters.

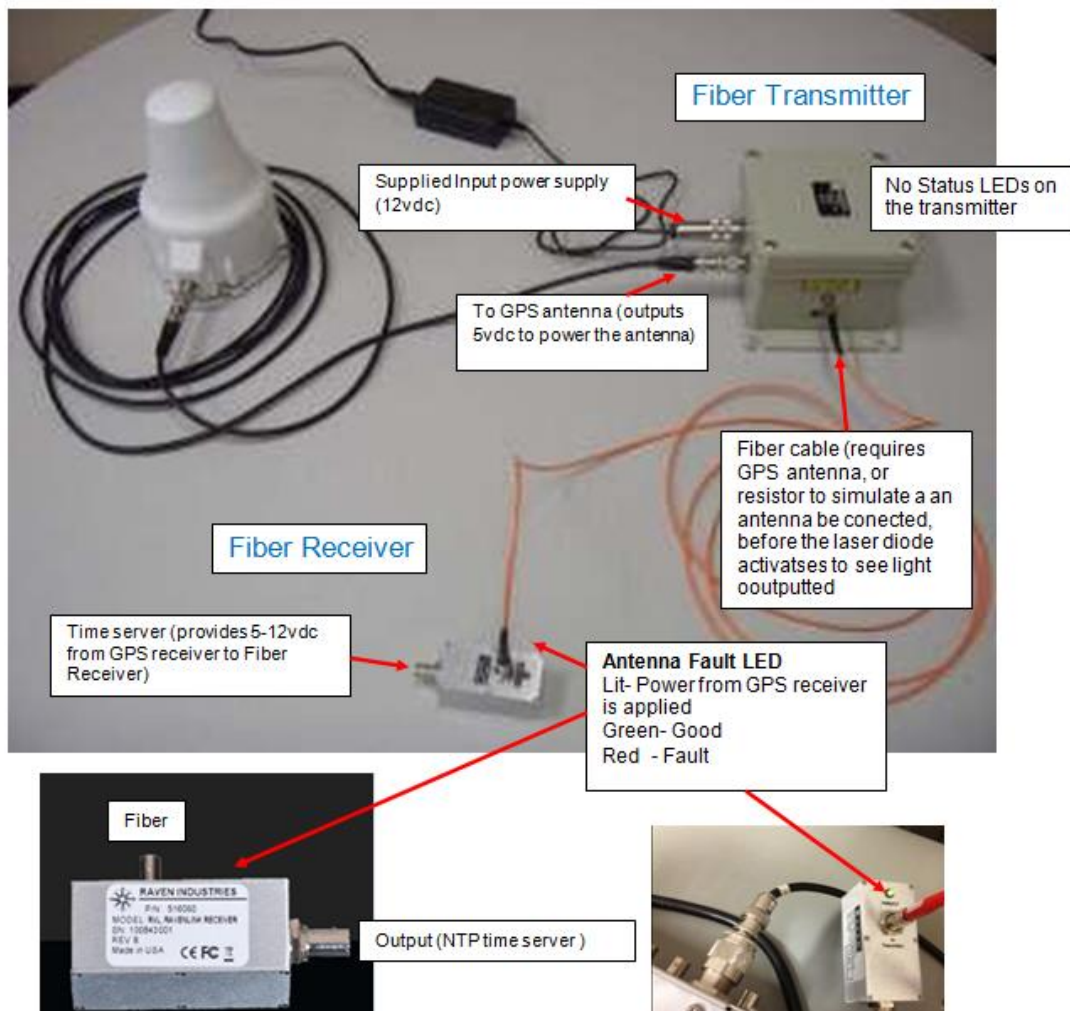
Surge arrestor is optional and probably unnecessary.

I think Will had something much better and Marcom can probably come up with some beautiful pictures.

Installation

A) Receiver:

- FiberLink receiver is intended to be powered by customer receiver.
- Power requirements are 5-12VDC. Typical current draw is 60mA.
- Connect the other end of the simplex multimode 50/125 micron fiber optic cable to the input labeled “FiberLink Transmitter” on the FiberLink receiver. (see picture below)



Operation:

The FiberLink works with all current GPS frequencies. It has a frequency range from 0.800 GHz to 1.8 GHz.

1. Connect the output of the FiberLink Receiver to the GPS Antenna connector on the Spectracom Time Server.
2. Connect the Fiber to the Fiberlink Transmitter and Fiberlink Receiver.
3. Connect the Fiberlink Transmitter to the GPS Antenna.
4. Connect the Power Supply to the Fiberlink Transmitter.

Note: There are no user serviceable parts internal to units and should not be opened under any condition.

Equipment List:

Model Number 1201-KIT-FIB1-DUC

- 1 - FiberLink Transmitter
- 1 - FiberLink Receiver
- 1- 12VDC 2A power supply and power cord for transmitter

Specifications:

Transmitter:

Antenna Requirements:

Connection: TNC

Gain: 34dB +6/-3 dB

Impedance: 50Ω

Power: 5 VDC (minimum 8mA)

Frequency: 800MHz to 1800 MHz

Power Connection: 2 Pin 12-24V AC or DC

Input Voltage: AC/DC 12-24V 50/60 Hz @ 100-600mA

Output Connection: ST Type Fiber Optic Connector for Simplex Multimode 50/125 Micron Cable

Fiber Length: System allows Fiber Runs of up to 1524 meters (5000 feet) of 50/125 Fiber Optic Cable

Enclosure: Diecast Aluminum

Color: Beige (Powder Coated)

Relative Humidity: 0-100% Condensing

Storage Temp: -50°C to +85°C

Operating Temp: -40°C to +70°C

Accessories: Power Supply (516816), Power Cable (516818)

Altitude: 6,096m (20,000 ft)

System Propagation Delay: 15ns (does not include fiber optic cable delay)

Receiver:

Input Connection: ST Type Fiber Optic Connector for Simplex Multimode 50/125 Micron Cable

Input Power: 5 to 12 VDC @ 85mA (powered from DC bias of GPS Receiver)

Output Connection: BNC 50 OHM Female

Frequency: 800MHz to 1800 MHz

Enclosure: Extruded Aluminum

Color: Natural

Relative Humidity: 0-95% Non-Condensing

Storage Temp: -40°C to +85°C

Operating Temp: 0°C to +50°C

Altitude: 6,096m (20,000 ft)

Input gain requirements

Email from Tom Richardson to Raven (July 15, 2011)

Hi Janice and Tony,

I see that your Ravenlink Transmitter is designed for Antenna with gain of 34dB +/- 6/3 dB. Would this be +/- 2 dB or +/- 6 dB?

Our antenna has a gain of 27 dB typ. Using cable with attenuation characteristics of 5.1 dB/100 feet at GPS frequency, what would the maximum cable length be from the antenna to the Fiber optic transmitter

Reply to Tom from Tony Zuzzio:

The gain range of the transmitter is 40 dB to 31 dB gain (or +6 and -3 from 34 dB). I would recommend a line amp between the antenna and the transmitter for an antenna with 27dB gain.

After 100 ft of cable your signal would be around 21.9 dB which would be too low for our transmitter to work. By boosting the signal up with a 12 dB Lineamp (<http://starlinkdgps.com/products/inline-amplifiers/>) you would be right around 34 dB gain, which our transmitter

needs.

Earlier references to GPS fiber kits (before we started selling the Model 1201 kits)

From an email sent to Ed O'Connor

➤ NEW link: <http://gpsnetworking.com/fiber-optic-network.asp>

"Per your request, I looked at the GPS networking website for their fiber antenna kit (http://www.gpsnetworking.com/cart.php?m=product_detail&c=16&p=68) and found that YES, the raw GPS data can be sent up to 10 kilometers before it is converted back to raw GPS data and inputted into an antenna. The spec says it converts raw GPS RF data to light and then back to RF again. This is incredible. This is unlike the Trimble version of the RS-485 antenna which had the GPS receiver built into the antenna and the GPS converted data sent through a twisted -pair cable. This functionality wasn't compatible with our systems. However, it looks like this new system would likely be compatible (The only question is what the dB gain is at the receiver input, but I am assuming that it is a common value for GPS receivers).

As shown below, it looks like there are several components to the system and I don't see pricing on the system located on the web-site (Besides the cost of running the fiber cable).

Propagation speed and cable delay for Fiber Optic cable

From: http://en.wikipedia.org/wiki/Optical_fiber_cable

Optical cables transfer data at the [*speed of light*](#) in glass (slower than vacuum). This is typically around 180,000 to 200,000 km/s, resulting in 5.0 to 5.5 microseconds of latency per km. Thus the round-trip delay time for 1000 km is around 11 ms.^[14]

Optical Zonu Fiber Optic Antenna Link kits (1201-KIT-FIB1-C kit and 1201-KIT-FIB2-C kit)

- Replacement for earlier Ravenlink fiber distribution: [** \("StarLink"\) "RavenLink" 1201-KIT-FIB1-DUC](#)

Links/shortcuts

Link to folder in the Customer Service drive: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\Optical Zonu GPS fiber converters>

Link to our data sheet on the website:

<http://spectracom.com/Desktopmodules/Bring2Mind/DMX/Download.aspx?EntryId=1748&PortalId=0>

- **Product brochure/info/specs**
<http://industrialpix.com/gps/pdf/GPS%20Distribution%20System%20V%202%20200.pdf>
- **GPS over Fiber products:** <http://www.opticalzonu.com/solutions/gpsoverfiber/>

Optical Zonu Tech Support

Phone Number: 1-818-780-9701

Website (submit a tech query with fast response): <http://www.opticalzonu.com/standalone/technical-inquiry-rfof-standalone-modules/>

Contacts

Greg Grimes

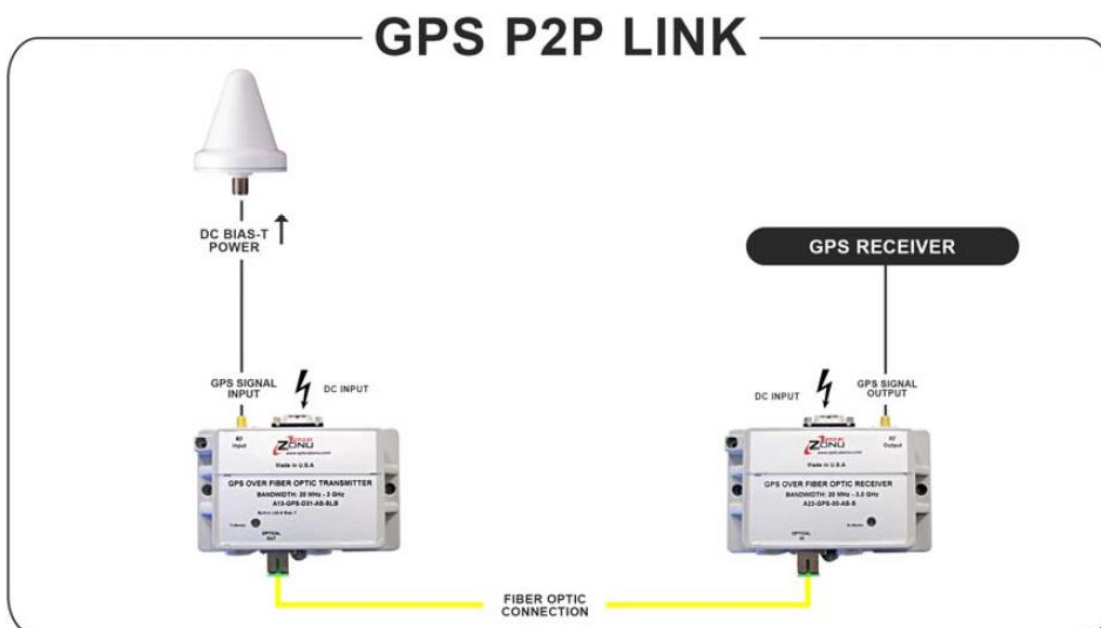
ggrimes@opticalzonu.com

Farzad Ghadooshahy

farzad@opticalzonu.com

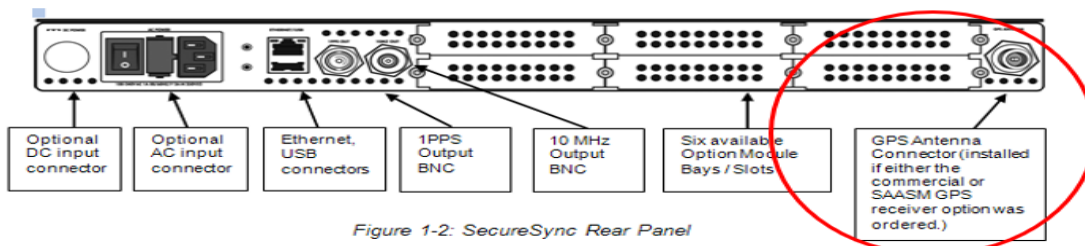
Britt McGinn (818) 452-5896

BMcGinn@opticalzonu.com



Q I need to know how to hook up a GPS Outdoor antenna to SecureSync 1200-013. Hook up the SecureSync to the network. What are slots J1 J2 J3 J4 on a 1204-06 (ser# 7200) used for? How to install a RF over fiber optic receiver and transmitter. Where do they plug into on the back of the SecureSync 1200-013?

A Reply from Keith (13 Dec 17) To begin (as shown in the following link to the online SecureSync user guide: http://manuals.spectracom.com/SS/Content/NC_and_SS/SS/Topics/INTRO/Rear_Panel.htm?Highlight=rear%20panel and below) the rear panel of every SecureSync has six available Option Bays/slots, which allow various "Model 1204-xx" Option Cards (such as the Model 1204-06 Gb Ethernet Option Card), to be installed in each SecureSync. Each purchased/installed Model 1204-xx Option Card adds a specific functionality to the SecureSync, which is not necessarily included in the base Model SecureSync (allowing customization of each SecureSync to pay for only what you need and not to include capabilities that you don't need). There are several different Model 1204-xx cards available for various purposes.



For instance, all base SecureSyncs have one Ethernet interface available ("eth0", located near the power and USB connector). The available Model 1204-06 GB ethernet Option card, when installed in the rear panel, adds three additional Gb Ethernet interfaces (eth1, eth2 and eth3). These additional interfaces allow the SecureSync to be connected to more than one isolated subnet.

When a SecureSync is purchased with a GPS/GNSS receiver installed, there is one external circular, threaded connector on the rear panel for applying the GPS RF signal to the SecureSync (as shown above). When using GPS RF to Fiber converters, the two fiber converters are connected to this rear panel GPS input connector.

The GPS RD signal is received by the Model 8230 GNSS antenna, which needs to be installed outdoors in a location where it has as much clear view of the sky as possible (preferably, but not essential, a 360 degree view around and up). Coax cable is attached to the bottom of the antenna and the cable run indoors. The RF to Fiber converter (the first of the two converters) is attached at this point. Fiber cable is then run to near the back of the SecureSync, where the Fiber to GPS converter (the second of the two converters) allows another coax connection to the GPS input threaded connector on the back of the SecureSync.

In summary, neither of the two fiber converters "directly" connect/attach to the back of the SecureSync. Instead, they are installed/attached to two lengths of coax cables. One of these coax cables also attaches to the Model 8230 antenna, and the other coax cable also attaches to the back of the SecureSync.

If you purchased/received from Spectracom the Optical Zonu converters (our P/N for the entire converter kit is either **1201-KIT-FIB1-C** or **1201-KIT-FIB2-C**) below is a basic diagram depicting this connection (with the connections to the antenna and the GPS receiver being the two lengths of coax cable).



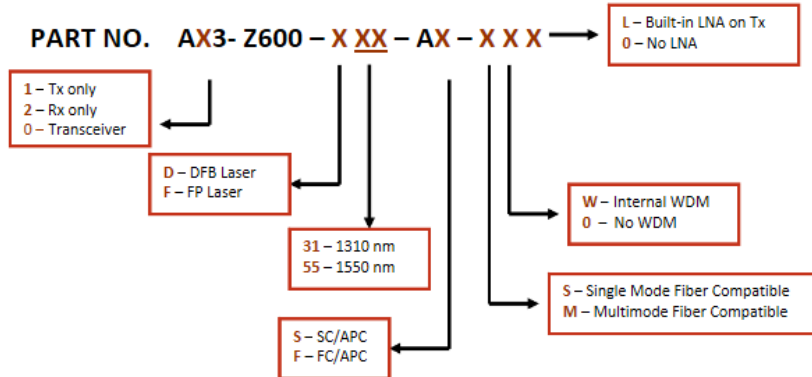
In this diagram, the GPS RF to Fiber converter is on the left (connected to the Model 8230 GNSS antenna, the Fiber to GPS converter is on the right (connected to the threaded GPS input on the back of the SecureSync) and the yellow line in between depicts the fiber cable.

OZ600 Part Numbering scheme



RF over Fiber Optic Transceiver OZ600 Series

ORDERING INFORMATION



General info

- ECO-00364 (Apr 2015) added these products to our “portfolio”

Email from John Fisher (12 June 2013)

FYI – interesting product. I can imagine some of our Financial Services and military customers might find this a useful companion product to our products. <http://www.gpsworld.com/optical-zonu-fiber-optic-gps-signal-distribution-system/>

System Specs

- From: <http://www.opticalzonu.com/standalone/oz600/>

OZ600 is a low-cost RF over Fiber transceiver. A pair of OZ600 transceivers will create a two-way bidirectional RF to Optical and Optical to RF link. OZ600 can also be configured as individual Transmitter (Tx) or Receiver (Rx) units if necessary. OZ600 is an excellent alternative to using coaxial cable systems and offer significant improvements in the transport of high frequency RF signals in their native format reliably across broad range of frequencies. It has low Noise Figure (NF) and high Spurious Free Dynamic Range (SFDR), with operational frequencies from 47 MHz to 3.0 GHz, or more.

The OZ600 is designed as a compact RF plug and play device that is easily integrated into your existing platform. It has a very low failure rate with an MTTF at room temperature of 20 years. Virtually any analog RF signal which falls within its bandwidth range can be transported over fiber optic cable using the OZ600 modules. Typical applications in which the OZ600 may be utilized include, but are not limited to, IF Satcom Band, L Band, GPS, PCS Cellular, UHF and VHF signal distribution over fiber.

Shock and vibe testing of the 1201-KIT-FIB2-C kit components

- Refer to Salesforce Case 243287 (Aug 2020)
- Refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\Optical Zonu GPS fiber converters\shock and vibe>

Attached is our compliance test report plus associated documentation.

I have also included a presentation showing PCBs.

The 1RU 19" rack mount chassis that was NEBS certified contains the OZ510 type PCBs. The flange mount enclosure that you use contain the OZ600 type PCB which has the same functionality as the OZ510 transmitter + OZ510 receiver.

When the OZ600 is used as a transceiver, both the laser diode (and associated transmitter circuitry) and the photodiode (and associated receiver circuitry) are populated. This board may also be used as a transmitter OR a receiver (This is how LMCO uses) in which case, half of the PCB is not populated.

Please treat the attached as confidential and proprietary (except for the datasheets which are in public domain).

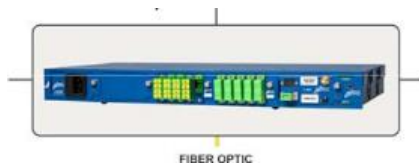
Regards,

Britt McGinn

Optical Zonu Corp.

(818) 452-5896

Master unit



- Not a required device
- As of at least February 2020, we are not currently offering this optional device

Fiber Optic cable delays

- ~5 nS for 1m fiber optic cable (from the Optical Zonu data sheet excerpted below)

SYSTEM SPECIFICATION

Frequency Range	1 GHz – 2 GHz.
Noise Figure P2P	3.3 dB (GPS antenna Gain not included)
IIP3	-10dBm
Link Gain	42 dB (GPS antenna Gain not included)
Group Delay	< 1nS
Fiber Optic Cable	~5 nS for 1m fiber optic cable
Power	Master Unit: 110-240V AC or 48VDC
RF Connector	50 Ohm SMA
Bias-T Option	+5V or +12V
Fiber Optic	SC/APC (LC/APC or FC/APC are optional)

ENCLOSURES

Master Unit	1U Modular Chassis 19" x 1U x 8
Remote Unit	Stand Alone Box 3" x 1.5" x 5"
Weight (Master Unit)	3.6 kg
Weight (Remote)	0.3 kg

MULTI-PORT DISTRIBUTION SYSTEM SPECIFICATIONS WITHOUT GPS ANTENNA GAIN

NUMBER OF OPTICAL RX	NF (dB)	GAIN (dB)
1	3.3	42
2	4.4	35
4	8.6	26.5
8	12.4	21.7
16	19.5	14.2
32	24	7.5

Manual Gain Control available on the Model OZ600s

From <http://www.opticalzonu.com/standalone/oz600/>

- All OZ600 modules are equipped with a Manual Gain Control (MGC) via a potentiometer accessible from the top of the box by a small screwdriver (or “twiker”) to ease field integrations.

Antenna Problem alarm fed back to the Spectracom device

Email from Dave L (15 Sep 17) The SecureSync sends a 5 VDC antenna power voltage from the antenna connector. The GPS Antenna is an active antenna that needs this power to supply a LNA. The antenna draws a nominal amount of current to power the LNA. If the current draw is above or below certain thresholds the receiver can indicate if there is a short or open circuit in the antenna line.

The Fiber transmitter/receiver system has the capability to send cable integrity status over the fiber connection so if the antenna became disconnected at the top end, the SecureSync could send an alarm indicating this condition

The fiber receiver has an internal circuit that will simulate an antenna failure to the SecureSync. **The Fiber Receiver has a circuit that will mimic the current draw based on a control signal coming from the fiber transmitter.**

You can test the SecureSync by connecting the GPS antenna directly to the cable that comes from the SecureSync antenna port. The LED should stop flashing and the GNSS status in the web UI should say OK if the Antenna Sense circuit is working properly.

Optical connector

from: <http://www.opticalzonu.com/standalone/oz600/>

- Standard optical connector is SC/APC for low back reflection, but FC/APC is also available. OZ600 Rx features a high performance InGaAs photodiode and Tx is based upon a linear Isolated FP Laser operating at 1.3 μm .

Power Control (AAPC) is incorporated for optimal optical power stability over the full temperature range.

RF interface is via a 50 Ohm SMA connector.

General Troubleshooting

Questions to ask/find out

1. What is the status of the “Tx Monitor” LED on both the TX and RX?
2. Is the DB9 cable attached to both the TX and RX?
3. Is there 5vdc at the antenna (verifying the 8226 and cable between antenna and TX is OK)

DB9 connector pin-out/power (to attach to both the Tx and Rx)

- Standard male DB-9 connector serves as an interface for alarm monitoring, RS232 port, and +12vdc power input
- From: <http://documents.mx/documents/oz600.html> (and an email from Danny Loke to TOYO (11 Jun 18)

DB-9 CONFIGURATION	
PIN	FUNCTION
1	Laser Enable (+12 v = Laser ON)
2	Data INPUT (Tx RS232)/ OR NC
3	Data OUTPUT (Rx RS232)/ OR NC
4	+12 volts (320 mA max)
5	Ground
6	Laser Bias Monitor (0.1 V = 10 mA)
7	Laser Bias Alarm (open collector, 25 mA)
8	Received Power Monitor (1V = 1mW)
9	Received Power Alarm (open collector, 25 mA)

1. Pin 1 is Laser Enable and must be pulled to +12 Volts for the module to be operational (Please ignore this only if you're using the manufacturer's original power supply with DB-9 plug). The +12 Volt enables the bias current to be supplied to the Laser and hence create output light. Be aware that if the Laser Enable is not supplied the LED indicator representing transmitter proper operation will remain GREEN. (Refer to Figure 3.)
2. Pins 2 and 3 of the DB-9 are RS232 Data Input and Output signals respectively. The RS232 logic levels are + 12 Volts.
3. Pin 4 provides +12 Volts to the module which typically draws less than 300 mA for the standard model with LNA or RS232 options.
4. Pin 5 is Ground. On the box there is also a Ground screw mount that can be used for even better grounding. Refer to FIGURE-2.
5. Pin 6 of the DB-9 connector is Laser Bias Monitor, which monitors Laser Bias Current. The output impedance of this port is 10K Ohms and may only be probed with a high impedance multimeter, otherwise a false measurement will result.
6. Pin 7 of the DB-9 connector is Laser Bias Alarm. The interface circuit is an Open Collector output, which is used to connect an external load such as a relay or LED. Care must be taken when connecting this port to an external load to limit the current to no more than 25 mA through the use of a limiting resistor. The threshold level for the alarm to trip is typically 110 mA.
7. Pin 8 of the DB-9 connector is Receiver Power Monitor, which is basically a built-in optical power meter. For every 1 mW of optical power, you should measure 1 Volt at this pin. The output impedance of this port is 10K Ohms and may only be probed with a high impedance multimeter, otherwise a false measurement will result.
8. Pin 9 of the DB-9 connector is Received Power Alarm. The interface circuit is an Open Collector output, which is used to connect an external load such as a relay or LED. Care must be taken when connecting this port to an external load to limit the current to no more than 25 mA using a limiting resistor. The Threshold level for the alarm to trip is typically -10 dBm input optical power.

+12vdc input power supply for both the Fiber Transmitter and Fiber Receivers



- The Anc kit for Both Fiber kits include one Optical Zonu +12vdc power supply for the Reciever and for the Transmitter.

Power supply attaches to Pin 4 of the DB9 connection

- “Pin 4 provides +12 Volts to the module which typically draws **less than 300 mA** for the standard model with LNA or RS232 options”

Our P/Ns for the Power Supply

A) US variant (MP33R-0000-0009)

- MP33R-0000-0009 in Arena: https://app.bom.com/items/detail-spec?item_id=1209402658&version_id=10324366538&orb_msg_single_search_p=1

Optical Zonu P/N for US power supply: 350-1212-02

Datasheet for power supply: refer to the Arena link above to obtain

Technical Specifications		
OUTPUT	DC VOLTAGE	12V
	RATED CURRENT	0.5A
	CURRENT RANGE	0 - 0.5A
	RATED POWER	6W
	RIPPLE & NOISE (max.)	100mVp-p
	VOLTAGE RANGE	11 - 13V; Fixed
INPUT	VOLTAGE RANGE	90 - 264VAC
	FREQUENCY RANGE	47 - 63Hz
	EFFICIENCY (Typ.)	76%
	AC CURRENT	0.2A / 100VAC
	INRUSH CURRENT (max.)	50A / 230VAC
PROTECTION	OVERLOAD	>110% rated output power Protection type : Hiccup mode, recovers automatically after fault condition is removed
	OVER VOLTAGE	>120% rated output voltage Protection type : Clamp by zener diode
ENVIRONMENT	WORKING TEMP.	0 to +40 (Refer to output load derating curve)
	WORKING HUMIDITY	20% to 90% RH non-condensing
	STORAGE TEMP., HUMIDITY	-20 to +85°C , 10 - 95% RH
SAFETY		UL60950-1, CSA22.2 approved
OTHERS	MTBF	500Khrs min. MIL-HDBK-217F(25)
	DIMENSION	32 x 66 x 42.5mm (L x W x H)
CONNECTOR	PLUG	DB-9
	CABLE	Standard type 20 AWG, 6ft
Ordering Information		
Description	Model Number	
+12 VDC AC-DC Power Adapter	350-1212-02	

B) EU (European) variant (MP33R-0000-0010)

MP33R-0000-0010 in Arena: https://app.bom.com/items/detail-sourcing?item_id=1218304793&version_id=10474778918

Optical Zonu P/N for EU power supply: 350-1212-02E

Datasheet for power supply: refer to the Arena link above to obtain

Two different Spectracom/Optical Zonu 'GPS to Fiber' kits are available:

Note: both kits use the same Fiber Optic transmitter. But they both use a different Fiber Optic receiver.

- **1201-KIT-FIB1-C (MultiMode kit)** (Refer to "A" below)
- **1201-KIT-FIB2-C (SingleMode kit)** (Refer to "B" below)

A) 1201-KIT-FIB1-C kit (MultiMode kit)

- **Our P/N:** 1201-0004-0600 in Arena: https://app.bom.com/items/detail-bom?item_id=1209896391&version_id=10334551698
- **A replacement for the obsolete 1201-0003-0600** (Raven FiberLink fiber converter), whose components went obsolete. This kit is **multimode**.
- Includes singlemode Transmitter, adapter cable, multimode Receiver and power supplies. (I suspect this is just re-using existing multimode fiber cable that was previously used with the Raven Fiberlink adapter)
- Uses Multimode fiber cable
- (As of at least Aug 2021) Includes **EU variant 12vdc power pack** (our P/N: MP33R-0000-0010) (not US variant)
 - In Arena: https://app.bom.com/items/detail-sourcing?item_id=1218304793&version_id=10474778918
 - Optical Zonu P/N for EU power supply: 350-1212-02E
 - Not sure if US variant power supply(MP33R-0000-0009) is still available/can be purchased separately
- **Data sheet in Marketing folder:** [I:\Marketing\ Product Data Sheets \(archive\)\GPS Antennas & Accessories](I:\Marketing\ Product Data Sheets (archive)\GPS Antennas & Accessories)
 - **Note:** as of Jan 2017, looks like there is only a datasheet for the other kit (1201-kit-fib2-C)
- **Data sheet on our website:** As of Jan 2017, looks like there is only a datasheet for the other kit (1201-kit-fib2-C)
- This kit is a Special and must be quoted as such

Link between the fiber transmitter and fiber receiver with this particular kit

- The link between the fiber transmitter and receiver is via multimode fiber cable.
 - **fiber-optic cable:** Type SC, Simplex Multimode 50/125microns to cover the distance between transmitter and receiver
- Max recommended cable length is 2 km.

Customer desire to use LC style Fiber connectors (along with the SC/APC connectors) via separate media converters

- Refer to Salesforce Case 271157 (Aug 2021)

Customer requirements:

- (1) 100-240VAC 50/60Hz 0.2A power for the transmitter within 50 ft of the GPS Antenna;
- (2) fiber-optic cable, Type SC, Simplex Multimode 50/125microns to cover the distance between transmitter and receiver;
- (3) GPS Antenna and Surge Protector;

- (4) RF cables 2 x CAL7xxx recommended (one between GPS Antenna system and transmitter up to 50 ft), one between receiver and time server/master clock – CAL7010, 10 ft. suggested).

This kit consists of the following items (Singlemode Transmitter, Multimode receiver, adapters, etc.)

1201-0004-0600

In Production

0

0

0

0

0

0

1201-KIT-FIB1-C

REVISION

»4 - In Production

Effective as of 08/24/2016 09:06:21 AM, Unshared

Specs

Bill of Materials

Files

Revisions

Sourcing

Costing

Compliance

Where Used

Projects

History

Indented

Flat

Sourcing

Costing

Purchasing

Custom

Redline

Compare

Lookup

Contains 8 first-level Items, 8 line Items, 8 unique Items, 0 of which are shared.

		#	ITEM NUMBER	ITEM NAME	CATEGORY	P
<input type="checkbox"/>	1		1201-1004-0800 rev 4	1201-KIT-FIB1-C Kit Label	Label	
<input type="checkbox"/>	2		CA01R-0NSA-8001 rev 2	CABLE,N JACK,SMA PLUG,RG-316,12in	Wire / Cable	
<input type="checkbox"/>	3		CA31-S1S1-0003 rev 2	CABLE, SC/APC, SC/UPC, Fiber Optic, MODE CONDITIONING, 1M	Cable Assembly	
<input type="checkbox"/>	4		CP12R-SCSC-0001 rev 1	Adapter, Fiber Optic, SC to SC, Multimode, Simplex, Metal	Adapter	
<input type="checkbox"/>	5		MP02-0003-0002 rev 2	LABEL STOCK, 6 UP	Label	
			MP33R-0000-0006 rev 1	GPS FO TX,SINGLEMODE,SMA,SC/APC	Electrical Hardware	
			MP33R-0000-0008 rev 1	GPS FO RX,MULTIMODE,SMA,SC	Electrical Hardware	
			MP33R-0000-0010 rev 2	POWER SUPPLY, OZ600 GPS FO, EU Version	Power Supply	

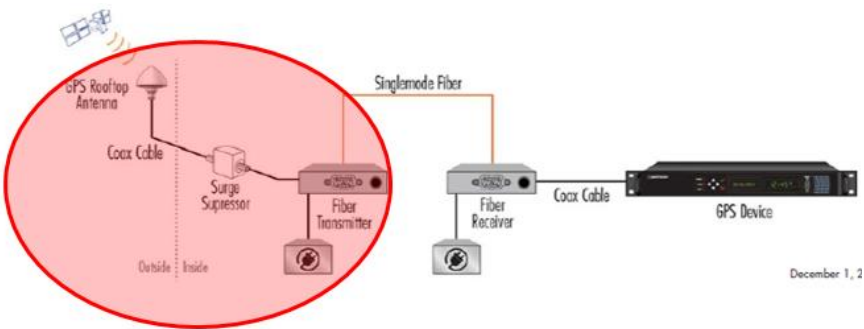
Add to Request

Fiber transmitter

Fiber receiver

(1) EU power pack

GPS antenna coax cable (between GPS antenna and the Fiber transmitter)



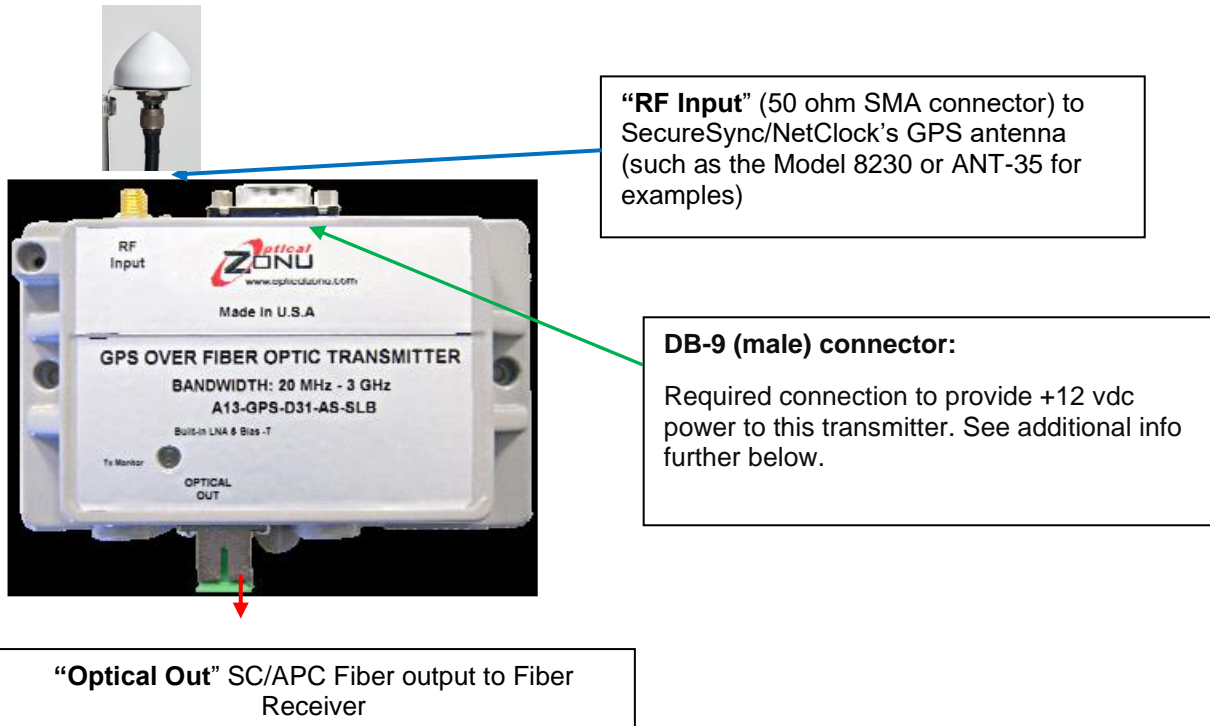
Max distance limitation for the coax cable

- 50 ft per Salesforce, but Tom Richardson believes 150ft should be OK

Q Hi Tom, could you assist us in determining max cable length (CAL7-LMR400) between the 8230 antenna and the fiber xmitter in the 1201-Kit-Fib2-C kit? I believe that's the Zonu system we're using now. Salesforce states 50ft., but is that the max? On the fiber-Rcvr end the cable length is stated 10 ft. recommended to the time server, which is satisfactory.

A Reply from Tom R (2 May 17) I think 150' should be OK also.

MP33R-0000-0006: Fiber Transmitter, singlemode (GPS antenna-end of the fiber cable)



- OZ600 series GPS Link Transmitter
- **Mfg. P/N:** A13-GPS-D31-AS-SLB
- **Our P/N:** MP33R-0000-0006 (in Arena): https://app.bom.com/items/detail-sourcing?item_id=1209397373&version_id=10324250378&orb_msg_single_search_p=1

Fiber Optic Transmitter

Input Connection	SMA Female (N to SMA adapter included)
Gain	20 dB +/- 1 dB
Impedance	50 ohm
Power for Antenna	5 VDC, 50 mA
Frequency	1 to 2 GHz
Power Connection	DB-9 12VDC (12VDC, 0.5 A power supply included)
Input Voltage	DC 12VDC @ 240 mA
Output Connection	SC/APC Type Fiber Optic Connector for Simplex Singlemode 9/125 Micron Cable
Fiber Length	System allows Fiber Runs of up to 5 miles (8 km) of 9/125 Fiber Optic Cable
Delay	< 1 ns + 3.3 ns/m fiber length
Storage Temp	-40°C to +50°C
Operating Temp	-40°C to +75°C
LEDs	Green: OK; Yellow: Antenna Fail; Red: Tx Fail; OFF: Power Supply Fail

LEDs / Antenna Sense for the Transmitter

Fiber Optic Transmitter

LEDs	Green: OK; Yellow: Antenna Fail; Red: Tx Fail; OFF: Power Supply Fail
-------------	--

- Unlike the Raven Fiberlink system, this system allows the GPS receiver to report an open or short being detected in the cable.
- The Master Unit monitors the current drawn by the antenna to confirm proper operation. Refer to information further below pertaining to the LEDs for the transmitters and receivers.

TX LEDs (update via email from Farzad, 23 Jan 17)

- **GREEN**: when the Laser of optical transmitter is functioning, the antenna is connected properly and is also functioning properly.
- **Flashing GREEN/YELLOW** (may look orange): The Antenna is failed or not connected. Optical power comes ON/OFF with approximately 50% duty cycle.

Email Keith sent (1 Nov 2018) Please first check for near +5vdc at the antenna end of the cable (disconnect the Model 8230 GNSS antenna from the cable and measure the DC voltage between the center pin of the cable and the outer shell of the connector). There should be about 4.8vdc present on the cable (to power the GNSS antenna).

If there is about 5vdc present on the end of the cable, the antenna was likely damaged by surge/lightning and may need to be replaced.

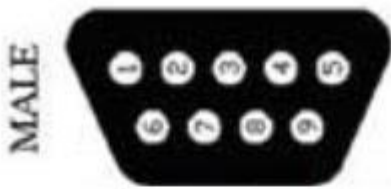
If there is no/low DC voltage on the antenna cable, there is likely an issue with the antenna cabling (a loose connection or an open/short in the cable/connectors between the antenna and the “**RF input**” connection on the Fiber transmitter.

Please let us know if you happen to find a bad connection between the antenna and the “RF input” connector on the fiber transmitter (and are now all set) or what the DC voltage is at the antenna-end of the cable. Then we can go from there!

- **RED**: Laser of optical transmitter failed. No optical power coming out of the optical transmitter.

DB-9 Configuration/power

- Alarm monitoring and power input is via male DB-9 connector and +12 Volts DC is required to operate this device.
- +12 Volts DC is provided to Optical Zonu's GPS over Fiber Optics Link via the DB-9 (male) connector with the pin-out configuration shown in this figure.

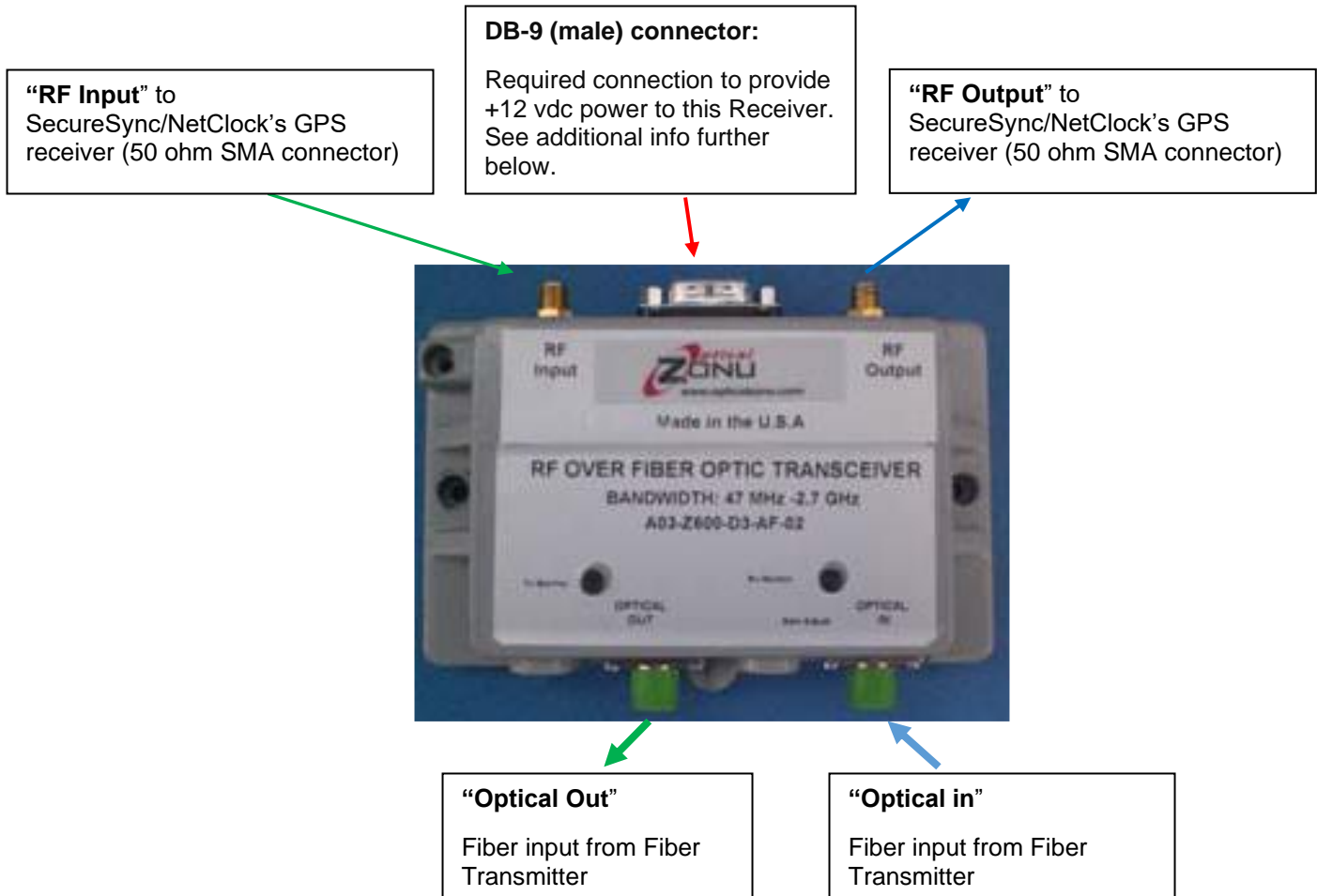


DB-9 CONFIGURATION	
PIN	FUNCTION
1	Laser Enable (+12 v = Laser ON)
2	Data INPUT (Tx RS232)/ OR NC
3	Data OUTPUT (Rx RS232)/ OR NC
4	+12 volts (320 mA max)
5	Ground
6	Laser Bias Monitor (0.1 V = 10 mA)
7	Laser Bias Alarm (open collector, 25 mA)
8	Received Power Monitor (1V = 1mW)
9	Received Power Alarm (open collector, 25 mA)

9. Pin 1 is Laser Enable and must be pulled to +12 Volts for the module to be operational (Please ignore this only if you're using the manufacturer's original power supply with DB-9 plug). The +12 Volt enables the bias current to be supplied to the Laser and hence create output light. Be aware that if the Laser Enable is not supplied the LED indicator representing transmitter proper operation will remain GREEN. (Refer to Figure 3.)
10. Pins 2 and 3 of the DB-9 are RS232 Data Input and Output signals respectively. The RS232 logic levels are + 12 Volts.
11. Pin 4 provides +12 Volts to the module which typically draws less than 300 mA for the standard model with LNA or RS232 options.
12. Pin 5 is Ground. On the box there is also a Ground screw mount that can be used for even better grounding. Refer to FIGURE-2.
13. Pin 6 of the DB-9 connector is Laser Bias Monitor, which monitors Laser Bias Current. The output impedance of this port is 10K Ohms and may only be probed with a high impedance multimeter, otherwise a false measurement will result.
14. Pin 7 of the DB-9 connector is Laser Bias Alarm. The interface circuit is an Open Collector output, which is used to connect an external load such as a relay or LED. Care must be taken when connecting this port to an external load to limit the current to no more than 25 mA through the use of a limiting resistor. The threshold level for the alarm to trip is typically 110 mA.
15. Pin 8 of the DB-9 connector is Receiver Power Monitor, which is basically a built-in optical power meter. For every 1 mW of optical power, you should measure 1 Volt at this pin. The output impedance of this port is 10K Ohms and may only be probed with a high impedance multimeter, otherwise a false measurement will result.
16. Pin 9 of the DB-9 connector is Received Power Alarm. The interface circuit is an Open Collector output, which is used to connect an external load such as a relay or LED. Care must be taken when connecting this port to an external load to limit the current to no more than 25 mA using a limiting resistor. The Threshold level for the alarm to trip is typically -10 dBm input optical power.

MP33R-0000-0008: Fiber Receiver, multimode (receiver-end of the fiber cable)

- OZ600 series GPS Link Receiver
- **Mfg. P/N:** A23-GPS-00-AS-M
- **Our P/N:** MP33R-0000-0008 (in Arena): https://app.bom.com/items/detail-sourcing?item_id=1209402588&version_id=10324365338&orb_msg_single_search_p=1



LEDs

Fiber Optic Receiver

LEDs	Green: Rx optical power good; OFF: Rx optical power < -10 dBm
-------------	---

- Also refer to information further below pertaining to the LEDs for the transmitters and receivers.

DB-9 Configuration/power

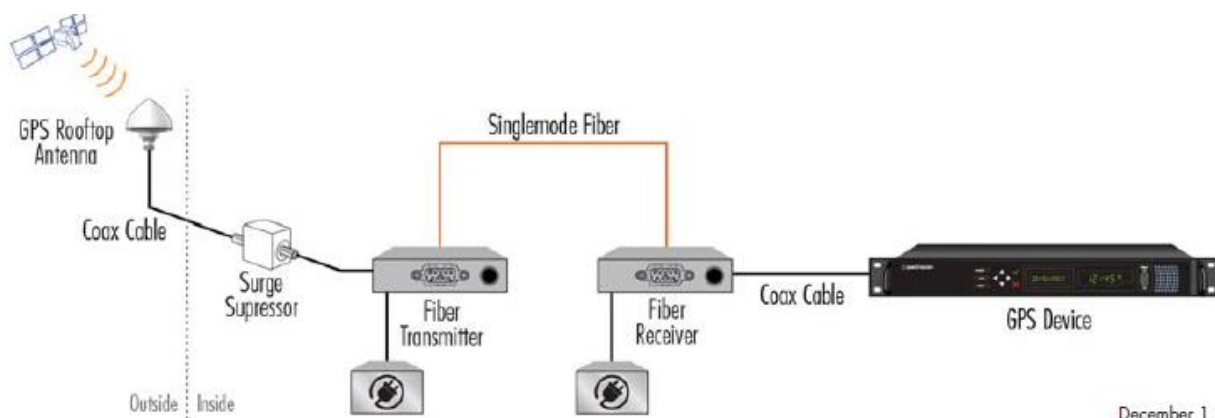
- Alarm monitoring and power input is via male DB-9 connector and +12 Volts DC is required to operate this device.
- +12 Volts DC is provided to Optical Zonu's GPS over Fiber Optics Link via the DB-9 (male) connector with the pin-out configuration shown in this figure.



DB-9 CONFIGURATION

PIN	FUNCTION
1	Laser Enable (+12 v = Laser ON)
2	Data INPUT (Tx RS232)/ OR NC
3	Data OUTPUT (Rx RS232)/ OR NC
4	+12 volts (400 mA max)
5	Ground
6	Laser Bias Monitor (0.1 V - 10 mA)
7	Laser Bias Alarm (open collector, 25 mA)
8	Received Power Monitor (1V - 1mW)
9	Received Power Alarm (open collector, 25 mA)

B) 1201-KIT-FIB2-C Kit (SingleMode kit)



December 1, 2016 - FIB1-C(C)

- **Our P/N:** 1201-0005-0600 (in Arena): https://app.bom.com/items/detail-attach?item_id=1209979033&version_id=10404383298&orb_msg_single_search_p=1
- A new kit for singlemode.
- Includes single mode TX, single mode RX and power supplies. (This kit is not replacing any previously run fiber cable. like the other kit is for).
- This kit uses **singlemode** fiber cable
- (As of at least Aug 2021) Includes **EU variant 12vdc power pack** (our P/N: MP33R-0000-0010) (not US variant)
 - In Arena: https://app.bom.com/items/detail-sourcing?item_id=1218304793&version_id=10474778918
 - Optical Zonu P/N for EU power supply: 350-1212-02E
 - Not sure if US variant power supply(MP33R-0000-0009) is still available/can be purchased separately
- **Refer to in Arena** https://app.bom.com/items/detail-bom?item_id=1209979033&version_id=10335671728
- **Link to 1201-KIT-FIB2-C data sheet:** [I:\Marketing\ Product Data Sheets \(archive\)\GPS Antennas & Accessories](I:\Marketing\ Product Data Sheets (archive)\GPS Antennas & Accessories)
- **Data sheet on our website:** <https://spectracom.com/admin/product-models/gps-fiber-converter>

Description for this kit:

The link between the fiber transmitter and receiver is via 9/125 micron singlemode simplex fiber via SC/APC connectors up to 5 miles (8 km). Use a standard Spectracom GPS RF antenna, surge suppressor, and coax cable system to connect to the fiber transmitter. The transmitter requires power (external supply included) which also supplies the 5V thru the RF cable to the antenna. At the end of the fiber link, the receiver requires power (external supply included) and is connected to the GPS device with a coax cable. Spectracom provides the appropriate adapters between the coax cable and fiber optic devices; SMA to N. The fiber receiver includes an active DC load on the RF connector center pin to prevent the antenna failure alarm in the GPS device. However, if the fiber detects antenna failure, it opens the active DC load at the RF output which triggers the alarm

This kit consists of the following items (Singlemode Transmitter, singlemode Receiver, adapters, etc)

1201-0005-0600

In Production

0

0

0

0

0

1201-KIT-FIB2-C

REVISION

»4 - In Production

Effective as of 08/24/2016 09:06:21 AM, Unshared

Specs

Bill of Materials

Files

Revisions

Sourcing

Costing

Compliance

Where Used

Proje

History

Indented

Flat

Sourcing

Costing

Purchasing

Custom

Redline

Compare

Lookup

Contains **6** first-level Items, **6** line Items, **6** unique Items, **0** of which are shared.☐

▼

#

ITEM NUMBER

ITEM NAME

CATEGORY

☐

1

1201-1005-0800 rev 5

1201-KIT-FIB2-C Kit Label

Label

☐

2

CA01R-0NSA-8001 rev 2

CABLE, N JACK, SMA PLUG, RG-316, 12in

Wire / Cable

☐

3

MP02-0003-0002 rev 2

LABEL STOCK, 6 UP

Label

Fiber transmitter

MP33R-0000-0006 rev 1

GPS FO TX, SINGLEMODE, SMA, SC/APC

Electrical Hardware

Fiber receiver

MP33R-0000-0007 rev 1

GPS FO RX, SINGLEMODE, SMA, SC/APC

Electrical Hardware

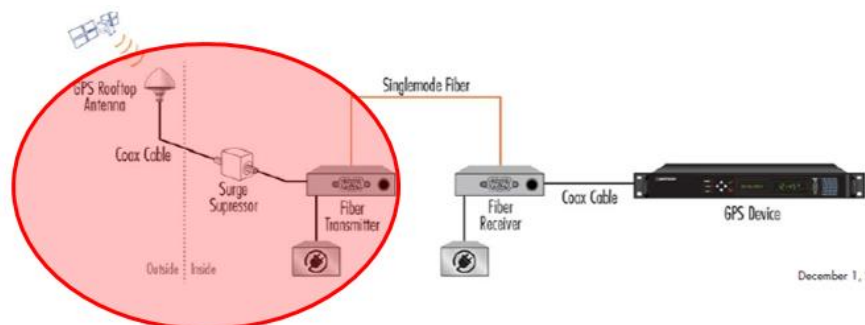
(2) EU power packs

MP33R-0000-0010 rev 2

POWER SUPPLY, OZ600 GPS FO, EU Version

Power Supply

GPS antenna coax cable (between GPS antenna and the Fiber transmitter)



Max distance limitation for the coax cable

A) Using LMR-400/RF-400 cable

- 50 ft per Salesforce, but Tom R believes 150ft should be OK

Q Hi Tom, could you assist us in determining max cable length (CAL7-LMR400) between the 8230 antenna and the fiber xmitter in the 1201-Kit-Fib2-C kit? I believe that's the Zonu system we're using now. Salesforce states 50ft., but is that the max? On the fiber-Rcvr end the cable length is stated 10 ft. recommended to the time server, which is satisfactory.

A Reply from Tom R (2 May 17) I think 150' should be OK also.

B) Using RG-58 cable instead (Based on Tom Richardson's comment of 150 ft of RF-400 being fine)

Email from Keith to a customer (28 April 2021) We state that up to 150 feet of LMR-400/RF-400 coax cable can safely be installed between the Antenna and the Fiber transmitter without signal strength issues. 150ft of this low-loss cable equates to about **8.25dB** of cable loss.

8.25db cable loss equates to about (worst-case) 27 feet of RG-58 (at 32dB per 100 feet of loss, or 0.32dB loss per foot). So, I would say that **about 25 to 30 feet of RG-58 cable between the existing GNSS antenna and the Fiber transmitter should be fine.** I wouldn't recommend exceeding about 30 feet of RG-58 cable in between the two devices.

Fiber cable to use / Link between the fiber transmitter and fiber receiver with this particular kit

- The link between the fiber transmitter and receiver is via 9/125 micron singlemode simplex fiber via SC/APC connectors up to 5 miles (8 km).

Fiber Transmitter (singlemode) (GPS antenna-end of the fiber cable)
(our P/N MP33R-0000-0006)



“RF Input” (50 ohm SMA connector) to SecureSync/NetClock’s GPS antenna (such as the Model 8230 or ANT-35 for examples)

DB-9 (male) connector:
 Required connection to provide +12 vdc power to this transmitter. See

“Optical Out” Fiber output to Fiber Receiver

- OZ600 series GPS Link Transmitter
- **Mfg. P/N:** A13-GPS-D31-AS-SLB
- **Our P/N:** MP33R-0000-0006 (in Arena): https://app.bom.com/items/detail-sourcing?item_id=1209397373&version_id=10324250378&orb_msg_single_search_p=1

Fiber Optic Transmitter

Input Connection	SMA Female (N to SMA adapter included)
Gain	20 dB +/- 1 dB
Impedance	50 ohm
Power for Antenna	5 VDC, 50 mA
Frequency	1 to 2 GHz
Power Connection	DB-9 12VDC (12VDC, 0.5 A power supply included)
Input Voltage	DC 12VDC @ 240 mA
Output Connection	SC/APC Type Fiber Optic Connector for Simplex Singlemode 9/125 Micron Cable
Fiber Length	System allows Fiber Runs of up to 5 miles (8 km) of 9/125 Fiber Optic Cable
Delay	< 1 ns + 3.3 ns/m fiber length
Storage Temp	-40°C to +50°C
Operating Temp	-40°C to +75°C
LEDs	Green: OK; Yellow: Antenna Fail; Red: Tx Fail; OFF: Power Supply Fail

Input Power

- The transmitter requires +12vdc power (external supply included to the DB9 connector) which also supplies the 5V thru the RF cable to the antenna.

LEDs/ Antenna Sense

Fiber Optic Transmitter

LEDs	Green: OK; Yellow: Antenna Fail; Red: Tx Fail; OFF: Power Supply Fail
-------------	--

- Unlike the Raven Fiberlink system, this system allows the GPS receiver to report an open or short being detected in the cable
- The Master Unit monitors the current drawn by the antenna to confirm proper operation. Refer to information further below pertaining to the LEDs for the transmitters and receivers.

RX LEDs (update via email from Farzad, 23 Jan 17)

- **GREEN:** when the optical receiver receives light and the antenna at the TX side is connected and working properly.
- **Flashing RED/OFF** The Antenna is failed or not connected at the TX site . Optical power received by receiver ON/OFF with approximately 50% duty cycle.

Email Keith sent (1 Nov 2018) Please first check for near +5vdc at the antenna end of the cable (disconnect the Model 8230 GNSS antenna from the cable and measure the DC voltage between the center pin of the cable and the outer shell of the connector). There should be about 4.8vdc present on the cable (to power the GNSS antenna).

If there is about 5vdc present on the end of the cable, the antenna was likely damaged by surge/lightning and may need to be replaced.

If there is no/low DC voltage on the antenna cable, there is likely an issue with the antenna cabling (a loose connection or an open/short in the cable/connectors between the antenna and the “**RF input**” connection on the Fiber transmitter.

Please let us know if you happen to find a bad connection between the antenna and the “RF input” connector on the fiber transmitter (and are now all set) or what the DC voltage is at the antenna-end of the cable. Then we can go from there!

- **RED:** no optical power received, possibly bad or dirty fiber or failed optical transmitter.

DB-9 Configuration/power

- Alarm monitoring and power input is via male DB-9 connector and +12 Volts DC is required to operate this device.
- +12 Volts DC is provided to Optical Zonu's GPS over Fiber Optics Link via the DB-9 (male) connector with the pin-out configuration shown in this figure.



DB-9 CONFIGURATION	
PIN	FUNCTION
1	Laser Enable (+12 v = Laser ON)
2	Data: INPUT (Tx RS232)/ OR NC
3	Data: OUTPUT (Rx RS232)/ OR NC
4	+12-volts (400 mA max)
5	Ground
6	Laser Bias Monitor (0:1 V = 10 mA)
7	Laser Bias Alarm (open collector, 25 mA)
8	Received Power Monitor (1V = 1mW)
9	Received Power Alarm (open collector, 25 mA)

MP33R-0000-0007: Fiber Optic Receiver, Singlemode (receiver-end of the fiber cable)
(our P/N MP33R-0000-0007)



“RF Output” to
SecureSync/NetClock’s GPS
receiver

DB-9 (male) connector:

Required connection to provide
+12 vdc power to this Receiver.
See additional info further
below.

“Optical In” Fiber input
from Fiber Transmitter

- OZ600 series GPS Link Receiver
- **Mfg. P/N:** A23-GPS-00-AS-S
- **Our P/N:** MP33R-0000-0007 (in Arena):

(Single mode receiver only)

Fiber Optic Receiver

Input Connection	SC/APC Type Fiber Optic Connector for Simplex Singlemode 9/125 Micron Cable
Power Connection	DB-9 12VDC (12VDC, 0.5 A power supply included)
Input Voltage	DC 12VDC @ 310 mA
Output Connection	SMA Female (SMA to N adapter included)
Storage Temp	-40°C to +85°C
Operating Temp	0°C to +50°C
LEDs	Green: Rx optical power good; OFF: Rx optical power < -10 dBm

Function

- At the end of the fiber link, the receiver requires power (external supply included) and is connected to the GPS device with a coax cable.
- Spectracom provides the appropriate adapters between the coax cable and fiber optic devices; SMA to N. The fiber receiver includes an active DC load on the RF connector center pin to prevent the antenna failure alarm in the GPS device. However, if the fiber detects antenna failure, it opens the active DC load at the RF output which triggers the alarm

LEDs

Fiber Optic Receiver

LEDs	Green: Rx optical power good; OFF: Rx optical power < -10 dBm
-------------	---

- Refer to information further below pertaining to the LEDs for the transmitters and receivers.

RX LEDs (update via email from Farzad, 23 Jan 17)

- **GREEN**: when the optical receiver receives light and the antenna at the TX side is connected and working properly.
- **Flashing RED/OFF** The Antenna is failed or not connected at the TX site. Optical power received by receiver ON/OFF with approximately 50% duty cycle.
- **RED**: no optical power received, possibly bad or dirty fiber or failed optical transmitter.

DB-9 Configuration/power

- Alarm monitoring and power input is via male DB-9 connector and +12 Volts DC is required to operate this device.
- +12 Volts DC is provided to Optical Zonu's GPS over Fiber Optics Link via the DB-9 (male) connector with the pin-out configuration shown in this figure.



DB-9 CONFIGURATION	
PIN	FUNCTION
1	Laser Enable (+12 v = Laser ON)
2	Data INPUT (Tx RS232)/ OR NC
3	Data OUTPUT (Rx RS232)/ OR NC
4	+12-volts (400 mA max)
5	Ground
6	Laser Bias Monitor (0.1 V = 10 mA)
7	Laser Bias Alarm (open collector, 25 mA)
8	Received Power Monitor (1V = 1mW)
9	Received Power Alarm (open collector, 25 mA)

Status LEDs

Excerpted below from our datasheet

Fiber Optic Transmitter

LEDs	Green: OK; Yellow: Antenna Fail; Red: Tx Fail; OFF: Power Supply Fail
-------------	--

Fiber Optic Receiver

LEDs	Green: Rx optical power good; OFF: Rx optical power < -10 dBm
-------------	--

“TX Monitor” LED status indications

- Same Model Transmitter is included in both the 1201-KIT-FIB1-C and 1201-KIT-FIB2-C kits



“TX Monitor” LED Status	Indication	Recommendation
Green	OK	None
Yellow	Antenna Fail	
Red	TX Fail	
flashing green and red (single LED)	No antenna detected by the fiber transmitter	Potential Causes: 1) no antenna or dead antenna LNA, 2) lightning arrestor blocking DC power, 3) coaxial cable between the Tx and the antenna too long 4) fiberoptic Tx bias-T shorted out
Off	Power supply fail	Verify if 12vdc input is present on DB9 pin 4

“RX Monitor” LED status indications

Multimode Receiver (part of 1201-KIT-FIB1-C)

Mfg. P/N A23-GPS-00-AS-M



Singlemode Receiver (part of 1201-KIT-FIB2-C)

Mfg. P/N: A23-GPS-00-AS-S



“TX Monitor” LED Status	Indication	Recommendation
Green	OK	
Yellow	Antenna Fail	
Solid Red	TX Fail (No light received)	Potential Causes: 1) fiber cable broken, disconnected or routed incorrectly 2) fiberoptic Tx dead or not powered
Off	Power supply fail	Verify if 12vdc input is present on DB9 pin 4

Note: A software change to the product has since changed LED status indications.

Below in blue (reported symptoms from Open Access): in red (responses from Gary Grimes, 14 Apr 16)

TX – flashing green and red (single LED) – No antenna detected. Causes:

- 1) no antenna or dead antenna LNA,
- 2) lightning arrestor blocking DC power,
- 3) coaxial cable between the Tx and the antenna too long (+5 VDC PCTel antenna can take a minimum +3.3 VDC),
- 4) fiberoptic Tx bias-T shorted out

RX – solid red – RX is closer to the GPS antenna. No light received. Causes:

- 1) fiber cable broken, disconnected or routed incorrectly
- 2) fiberoptic Tx dead or not powered (Tx LED solid red or off)

General Troubleshooting

- 1) What is the status of the “Tx Monitor” LED (on both the TX and RX?)
- 2) Is the DB9 cable attached to both the TX and RX?

- 3) Is there 5vdc at the antenna (verifying the 8226 and cable between antenna and TX is OK)
- Refer to the applicable GPS reception tech note

Manual Gain Control (MGC)

- Info below from: <http://www.opticalzonu.com/standalone/oz600/>

All OZ600 modules are equipped with a Manual Gain Control (MGC) via a potentiometer accessible from the top of the box by a small screw driver (or “twiker”) to ease field integrations.

Standard optical connector is SC/APC, for low back reflection- but FC/APC is also available.

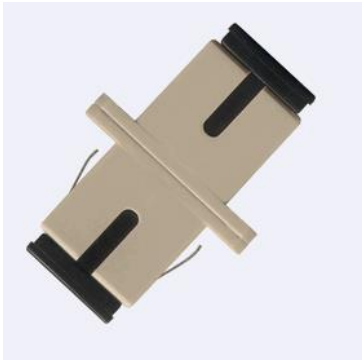
OZ600 Rx features a high performance InGaAs photodiode and Tx is based upon a linear Isolated FP Laser operating at 1.3 μm . Average Automatic Power Control (AAPC) is incorporated for optimal optical power stability over the full temperature range.

DB9 connector pin-out/power

- Standard male DB-9 connector serves as an interface for alarm monitoring, RS232 port, and +12vdc power input
- From: <http://documents.mx/documents/oz600.html>

DB-9 CONFIGURATION	
PIN	FUNCTION
1	Laser Enable (+12 v = Laser ON)
2	Data INPUT (Tx RS232)/ OR NC
3	Data OUTPUT (Rx RS232)/ OR NC
4	+12 volts (320 mA max)
5	Ground
6	Laser Bias Monitor (0.1 V = 10 mA)
7	Laser Bias Alarm (open collector, 25 mA)
8	Received Power Monitor (1V = 1mW)
9	Received Power Alarm (open collector, 25 mA)

Fiber Optic Adapter



- **Description:** SC to SC, multimode, Simplex, Meta;
- **Our P/N:** CP12R-SCSC-0001
- **In Arena:** https://app.bom.com/items/detail-spec?item_id=1209909854&version_id=10334701078

Pendulum FL-15 GPS Antenna Fibre link (not available from Spectracom)

Data sheet: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\Pendulum equipment\Pendulum FL-15 GPS antenna Fiber link>

- We believe this product / system was discontinued prior to Spectracom purchasing the Pendulum product line.
- We do not support or accept this product back for repair and have little info about it.
- If the device has the manufacturer's name indicated on it, the customer can contact them directly to see if they will still support/repair it.

Pendulum P/N was: 4031 600 15101

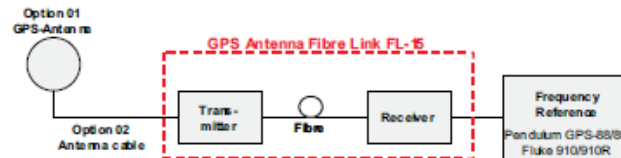


Figure 1: Cross-site connection.

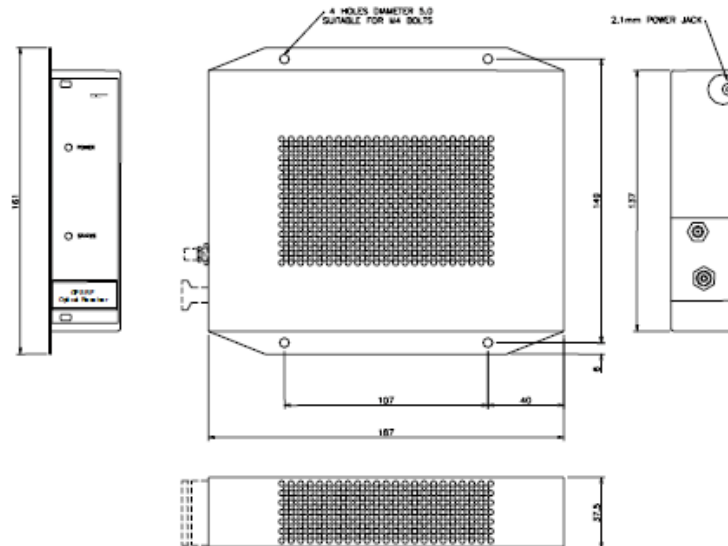


Figure 2: Mechanical dimensions.

“The system consists of the frequency reference, the FL-15 fiber link, and GPS antenna and antenna coax cable interface.

Other GPS Fiber converters (not available from Spectracom)

Refer to: I:\Customer Service\GPS\GPS Fiber converters

Email from Dave Sohn (13 June 2013) I spoke with Optical Zonu company a year and a half ago when PMRF asked about 50km fiber optic links for GPS. Specifically, for that application, I came across these two other vendors as well that do RF over fiber. An Optical Zonu product supporting the 50km link was ~\$4000.

ViaLite (they mentioned them): >50km
<http://www.vialite-usa.com/>

Microwave Photonic Systems: >50km
<http://www.b2bphotronics.com/>

GPS/GNSS RECEIVERS

Distinguishing Glonass satellites versus GPS satellites

- GPS satellites have a Satellite ID number range of 0 to 59 and are reported as “GP”
- Glonass satellites have a Satellite ID number range of 60 and above and are reported as “GL”

Noise Figure

From wikipedia

Noise figure (NF) and **noise factor** (F) are measures of degradation of the signal-to-noise ratio (SNR), caused by components in a radio-frequency (RF) signal chain. It is a number by which the performance of an amplifier or a radio receiver can be specified, with lower values indicating better performance.

The noise factor is defined as the ratio of the output noise power of a device to the portion thereof attributable to thermal noise in the input termination at standard noise temperature T_0 (usually 290 K). The noise factor is thus the ratio of actual output noise to that which would remain if the device itself did not introduce noise, or the ratio of input SNR to output SNR.

The noise *figure* is simply the noise *factor* expressed in decibels (dB)

Noise figures of various GNSS devices

GNSS Antennas

- Noise Figure of 8230 antenna, 1dB typical
- Noise Figure of 8225S antenna, 3dB

GPS Amps

- Noise figure of Model 8227 inline amplifier, 3.5 dB

Maximum noise figure for reliable operation of the ublox receiver is

Email from Tom Richardson (29 Jan 18) For a system including 8230 antenna, (+40 dB), 400 feet of cable, (-20 dB), an 8227, (+20 dB) and another 400 feet of cable (-20 dB) the Noise figure is 1.042 dB and the gain is 20 dB so it falls within the requirements of less than 1.5 dB of noise figure and gain between 5 and 20. Current draw would be 19 mA for the antenna and 15 mA for the inline amplifier for 34 mA total. Max DC loss would be 34 mA * 1.39 ohms ~ 0.05V DC.

TRAIM (Timing Receiver Autonomous Integrity Monitoring)

- TRAIM is not the same as anti-spoofing.
- RAIM requires an abundance of satellites, because it compares one satellite measurement to the consensus of the other available satellite measurements.
- When more satellites are available than needed to produce a position fix, the extra pseudoranges should all be consistent with the computed position. A pseudorange that differs significantly from the expected value (i.e., an [outlier](#)) may indicate a fault of the associated satellite or another signal integrity problem (e.g., ionospheric dispersion).
- RAIM compares each GPS measurement to the consensus of the other available GPS measurements. In this way, RAIM detects the presence of a faulty satellite within the current set of in-view satellites. In some circumstances, RAIM can also isolate which satellite is faulty or inconsistent with the other satellites in-view.
- Traditional RAIM uses fault detection (FD) only, however newer GPS receivers incorporate fault detection and exclusion (FDE) which enables them to continue to operate in the presence of a GPS failure.

From Wikipedia: Receiver autonomous integrity monitoring (RAIM) provides integrity monitoring of GPS for aviation applications. In order for a GPS receiver to perform RAIM or fault detection (FD) function, a minimum of five visible satellites with satisfactory geometry must be visible to it. RAIM has various kind of implementations; one of them performs consistency checks between all position solutions obtained with various subsets of the visible satellites. The receiver provides an alert to the pilot if the consistency checks fail.

RAIM availability is an important issue when using such kind of algorithm in safety-critical applications (as the aeronautical ones); in fact, because of geometry and satellite service maintenance, RAIM is not always available at all, meaning that the receiver's antenna could have sometimes less than five satellites in view.

Availability is also a performance indicator of the RAIM algorithm. Availability is a function of the geometry of the constellation which is in view and of other environmental conditions. If availability is seen in this way it is clear that it is not an on-off feature meaning that the algorithm could be available but not with the required performance of detecting a failure when it happens. So availability is a performance factor of the algorithm and characterizes each one of the different kinds of RAIM algorithms and methodologies.

TRAIM:

TRAIM ([Time Receiver Autonomous Integrity Monitor](#)). TRAIM is not, in any way, an anti-spoof functionality. This GPS receiver feature provides monitoring to allow a GPS satellite that is transmitting bad data to not be used by the GPS receiver for positional fix (as long as the GPS receiver is tracking at least three satellites). It helps the GPS receiver provide a better GPS 1PPS output to the SecureSync. Once a positional fix has been computed from any satellite data the GPS receiver reads, TRAIM automatically continues to detect and reject any faulty GPS satellites.

General Information on TRAIM (from <http://www.cotsjournalonline.com/articles/view/100205> as it applies the SecureSync's GPS receiver)

For precision timing/frequency applications (recall that frequency is the reciprocal of time), some commercial GPS receiver manufacturers modify their software to make a typical receiver a better precision timing product. Since timing applications are mostly stationary, the receiver's local signal processing power is focused on producing a very precise 1 pps (pulse per second) output with a signal integrity capability, hence defining the accuracy level of the receiver. This is referred to as the TRAIM function (Time Receiver Autonomous Integrity Monitoring). Although designed for timing, the receiver does self-surveying to find its location automatically so that true UTC (Universal Time Coordinated) can be obtained.

Contrary to navigation, which needs four satellites to compute a solution, a receiver used only for timing applications needs only one satellite to maintain precision time and frequency, once its position is established. However, to enhance the optional TRAIM integrity, a minimum of three satellites is required. In case of GPS signal loss (such as a lightning strike disabling the antenna) or GPS-related failures, designers of time/frequency systems add external precision oscillators to back up the receiver for a period of time. Such oscillators provide hold-over performance until the antenna is replaced or repaired and the receiver switches back to "GPS locked" operation. The performance that can be achieved from the receiver alone without external aid.

The most detailed, available information on TRAIM in the SecureSync's GPS below (From

Timing operation

The Resolution T automatically outputs a PPS and time tag. With an accurate reference position, the receiver automatically switches to an overdetermined clock mode, activates its TRAIM algorithm and outputs a precise PPS. Using a simple voting scheme based on pseudo-range residuals, the Resolution T integrity algorithm automatically removes the worst satellite with the highest residual from the solution set if that satellite's residual is above a certain threshold.

Email from Dick Fox to TOYO regarding TRAIM (12/5/12)

We met with Trimble today and received some additional information on how Traim works

Here is the answer we received from Trimble

Time Receiver Autonomous Integrity Monitoring (TRAIM) requires at least THREE SV, it will automatically drop the SV with the largest (only one) range residual, if its greater than 150 meters and one additional SV with the largest range rate greater than 15 meters per second.

Please note TRAIM only drops the worst case of each parameter type. It does not drop all the SV that violate either parameter.

As you can see from the explanation Trimble has a language of their own when it comes to explaining GPS receiver operations

- for example SV refers to satellites
- range residual – refers to the change in the position as determined by the GPS receiver
- range rate – refers to the speed – as determined by the GPS receiver

So TRAIM can use to use eliminate up to a maximum of 2 satellites from the GPS calculation

Here are some use cases and what Traim does

1. None of the satellites change the calculated position by more than 150 Meter
 - a. Result –GPS receiver will use all the satellites to calculate the position, speed and time
2. None of the satellites change the calculated speed by more than 15 meters per second
 - a. Result – GPS receiver will use all the satellites to calculate the position, speed and time
3. One of the satellites change the calculated position by more than 150 Meter
 - a. Result – that satellite is ignored in the calculation of position, speed and time
4. One of the satellites change the calculated speed by more than 15 meters per second
 - a. Result – that satellite is ignored in the calculation of position, speed and time
5. One of the satellites changes the calculated speed by more than 15 meters per second and another satellite changes the position by more than 150 meters
 - a. Result – both these satellites are ignored in the calculations of position, speed and time
6. Two satellites change the calculated speed by more than 15 meters per second and three satellites change the position by more than 150 meters
 - a. Results
 - i. The satellite that change the speed the most is ignored
 - ii. The satellite that changed the position the most is ignored
 - iii. All the other satellites are used in the calculations
 1. including the one the change the speed by more than 15 meters per second
 2. Including the two that changed the position by more than 150 meters are used
 3. Only two satellites are eliminated from the calculation

With this as background we believe Traim has limited ability to detect sophisticated spoofing.

It can detect one abnormal satellite based its effect on speed

It can eliminate one abnormal satellite based its effect on position

Clearing Antenna problem alarm when GPS antenna is not connected:

Note: For SecureSync and 9483/9489, Archive software version 4.8.7 (late Sept 2012 time-frame) added "Mask alarm" capability which can "hide" an undesired Antenna Problem alarm.

As a matter of fact, there certainly is a way to prevent the Fault LED from blinking. This is an indication that the Antenna Problem alarm is asserted, because the GPS sense circuit is detecting an open in the GPS port.

To clear this alarm, you just need to simulate a GPS antenna being connected. The output voltage of the rear panel antenna jack (used to power the antenna) is a nominal +5vdc. To simulate a GPS antenna being connected to this jack, simply put a 50 to 200 ohm resistor from the center of the antenna jack to the outer- threaded portion of the same jack. This resistive load will simulate a GPS antenna being connected, therefore clearing the Antenna Problem alarm (the LED will no longer blink).

The specific resistor value doesn't really need to be a specific value. The sense circuit is pretty wide open in order to support GPS antennas with varying impedance values. We have used antennas with 67 ohm impedance as well as around 200 ohm impedance. Any value in this general range will simulate the GPS antenna being connected.

Type N connector with 50 ohm load

Email from Tom Kilbourne to one of his customers:

I recommended that the customer buy some cheap 50 Ohm Type N terminations for this use. The GPS antenna port provides +5 VDC to drive the amp in the antenna and with a 50 Ohm DC load this will draw 0.1 A and the load will dissipate 0.5 Watts. I found this 1 GHz 2W N Male termination for less than \$20: <https://www.pasternack.com/2-watts-n-male-rf-load-up-to-1-ghz-pe6152-p.aspx> This is a much more elegant and far less costly solution than having an antenna hanging off the end of the SecureSync

Desire to block DC voltage output from the GPS receiver

For unknown reasons, TOYO in Japan desires to block the GPS receiver's 5vdc output. Dave Sohn sent the following to Dick Fox:

You can purchase DC blocks that will allow the RF signal to go through, but blocks the DC voltage. GPS Networking offers one for about \$75 USD.

<http://gpsnetworking.com/attenuators.asp>

Rockwell Collins GB-Gram SAASM receiver (MPE-S receiver)

- Refer to: <U:\Engineering\SAASM-FOUO\CustomerService\SecureSync>

uBlox Model M8T GNSS receiver (used in SecureSyncs,TSync boards and Versas)

- **MFG. data sheet:** <https://www.u-blox.com/en/product/neolea-m8t>
- GPS/QZSS, Glonass and BeiDou capable receiver
- 72 channel receiver

u-Blox info

- <https://www.u-blox.com/en>
- u-blox was founded in 1997 and is headquartered in Thalwil, Switzerland.
- **u-blox America Inc. (u-blox USA Sales Office)**

uBlox manual

- in Arena at: https://app.bom.com/items/detail-spec?item_id=1215115639&version_id=10415914428&orb_msg_single_search_p=1
- or also at: <..\..\GPS\GPS receivers\ublox M8T>

Associated Part Numbers

- Receiver consists of the receiver chipset and a carrier board

1. Carrier board required for SecureSyncs/9400s to use the u-blox receiver:

- **1240-1000-0200** (bare carrier board for ublox receiver) in Arena at: https://app.bom.com/items/detail-spec?item_id=1215137017&version_id=10420470768
- **1240-0000-F001** (carrier board, no battery) in Arena at: https://app.bom.com/files/detail-summary?file_master_id=1238771766&file_id=1752262382

2. Complete M8T receiver (carrier board with chipset installed)

- **MFG/ MFG P/N:** ublox America, Inc., Model LEA-M8T-0
- **Mfg. Data sheet:** <https://www.u-blox.com/en/product/neolea-m8t>
- **Our P/N:** **MP30R-0GNS-0005** (ublox Model M8T GNSS receiver) in Arena at: https://app.bom.com/items/detail-spec?item_id=1215115639&version_id=10415914428&

Product Selection

Model	Type					Supply	Interfaces			Features							Grade												
	GPS / QZSS	GLONASS	Galileo	BeiDou	Timing	Dead Reckoning	Precise Point Positioning	Raw Data	1.65 V – 3.6 V	2.7 V – 3.6 V	Lowest power (DC/DC)	UART	USB	SPI	DDC (I/C compliant)	Programmable (Flash)	Data logging	Additional SAW	Additional LNA	RTC crystal	Internal oscillator	Active antenna / LNA supply	Active antenna / LNA control	Antenna short circuit detection / protection pin	Antenna open circuit detection pin	Frequency output	Standard	Professional	Automotive
NEO-M8T	•	•	R	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	T	•	•	•	•	•				
LEA-M8T	•	•	R	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	T	•	•	•	•	•	•			

○ = Optional, not activated per default or requires external components
C = Crystal / T = TCXO

R = Galileo ready

Features - GNSS		Package	
Receiver type	12-channel u-blox M8 engine GPS/GNSS L1 CA, GLONASS L1OF, BeiDou B1 SBAS L1 CA, SBAS, EGNOS, MSAS Galileo-ready E1BC (subject to firmware upgrade)	NEO-M8T 26-pin LCC leadless Chip Carrier 12.2 x 16.0 x 2.4mm, 1.6 g LEA-M8T 28-pin LCC leadless Chip Carrier 17.0 x 22.4 x 2.4mm, 2.6 g	Product
Nav. update rate	Continuous (RTT) - up to 2 Hz	Pinouts	
Position accuracy	2.5 m CEP (A) Autonomous		
Acquisition	GPS & GLONASS GPS & BeiDou		
	Cold start: 26 s 17 s Aided cold start: 2 s 3 s		
Sensitivity	Tracking & Nav: -147 dBm -145 dBm Cold start (aided): -137 dBm -135 dBm (Autonomous): -148 dBm -146 dBm Reacquisition: -160 dBm -158 dBm		
Assistance	AssistNow GNSS Online AssistNow GNSS Offline (up to 35 days) AssistNow Autonomous (up to 6 days) CMAS SARA, S-GPP compliant		
Oscillator	TCXO		
RTC crystal	BufoH		
Noise figure	On-chip LNA (LEA-M8T) Extra LNA for passive antenna (NEO-M8T)		
Anti-jamming	Active CW detection and removal. On-board SAW band pass filter		
Memory	Internal QSPI Flash for firmware updates		
Supported antenna	Active and passive		
Features - Timing		Features - Raw data and IMES	
Timing accuracy	Clear sky: < 50 ns	Measurement data	GPS, GLONASS, BeiDou, SBAS and QZSS Carrier phase, Code phase & pseudo-range, Doppler
Time-to-first-fix	0.25 Hz - 10 MHz	Message data	GPS, GLONASS, BeiDou, SBAS, QZSS, L1/L2 and IMES 1 message (ISO200 base auto-band)
Time-to-acquisition	< 11 Hz		
Integrity reports	RAIM active, phase uncertainty, time-pulse rate/offset reports		
Environmental data, quality & reliability		Features - Power management	
Operating temp.	-40° C to 85° C	Power save modes	On/Off low duty-cycle
Storage temp.	-40° C to 85° C	On control	Hardware, message interface
RoHS compliant (lead-free)		On control	Hardware, wake-on UART activity, Timer, Latching low power (RTC)
Qualification according to ISO 16750		Automatic on/off with configurable period (GPS-only)	
Manufactured and fully tested in ISO 9001:2015 certified production sites			
Uses u-blox M8 chips qualified according to AEC-Q100			
Electrical data		Features - Antenna management	
Supply voltage	2.7 V to 3.6 V	NEO-M8T	External with logic level antenna switching output, filtered continuous supply
Power consumption	18 µA (Battery back-up) 80 µA (Full-power back-up) 34 mA @ 3.0 V (Operational, NEO-M8T) 80 mA @ 3.0 V (Operational, LEA-M8T)	LEA-M8T	Internal antenna bias supply with switching, overcurrent protection and alarm. Optional input for external over-current detection
Backup supply	1.4 to 3.0 V		
		Interfaces	
		Serial interfaces	SP or UART and QDC I²C compliant USB, I²C, I²S, SPI, 12-MHz
		Protocols	NMEA, UBX binary, RTCM
		Time-pulse outputs	2
		Time-mark inputs	2
		Support products	
		EVA-M8T	u-blox M8 Timing GNSS Evaluation Kit
		Product variants	
		NEO-M8T	u-blox M8 GNSS LCC module in NEO form factor, Timing, TCXO, Ref, SAW, LNA
		LEA-M8T	u-blox M8 GNSS LCC module in LEA form factor, Timing, TCXO, Ref, SAW

Country of Origin (COO) for ublox M8T receiver (Chinese components)

- M8T receiver we purchase for Ublox (from a US contractor) apparently consists of the ublox receiver chipset and an adapter board.
- Per Mike Steele (3 March 2020) **Re the huawei and associated banned list there is nothing of concern**

Per Mike Steele (3 March 2021) "The Ublox card is an assembly produced in the US by our contractor and we do not normally buy it standalone so i don't have COO" The bare PCB and most electronic components come from china.

Email Keith sent to FAA (3 March 2021) As for your question about County of Origin for the ublox receiver, we work with a US contractor to produce a carrier PCB board, which the uBlox receiver is installed on. This carrier board allows the receiver to be mounted/attached inside the SecureSync.

The carrier PCB board, and many of the electronic components installed on the carrier board, are manufactured in China. However, NONE of the components in the NetClock (including the ublox receiver and its associated carrier board) is from Huawei, or any other US-banned organization.

Firmware version info for ublox M8T receivers

A) ublox firmware version info for SecureSync/9400s

SecureSync version	Ublox firmware version	Cut-in info	Changes incorporated	Notes
5.4.1	2.3.0	Refer to info further below for ublox receiver cut-in dates	N/A	First ublox firmware we have used.
5.6.0	Release 3.01 TIM 2.2.0	April, 2017	Added support for Galileo constellation and performance improvements	We started receiving ublox receivers with 3.0.1 installed ~Nov 2016.

Note (for both SecureSyncs and TSynC boards) A Ublox receiver reporting it's at version 2.01 (instead of 2.3.0 or higher) is stuck in either its bootloader of default/"unprogrammed" state. It needs to be first placed into its programmed state using one of the following steps, to be updated to a newer firmware version,

via a hard power-down/power-up (not just a warm reboot)

Select the "Receiver Reset" checkbox (Interfaces -> GNSS 0-page of the browser)

Or use the **gpsreset clean** CLI command.

B) ublox firmware version info for TSynC boards

TSynC firmware Version	Ublox firmware version	Cut-in info	Changes incorporated	Notes
	2.3.0	Refer to info further below for ublox receiver cut-in dates	N/A	First ublox firmware we have used
3.0.1	Release 3.01 TIM 2.2.0	~ Nov/Dec 2016?	Added support for Galileo constellation and performance improvements	We started receiving ublox receivers with 3.0.1 installed ~Nov 2016.

Our cut-in info/minimum software version requirements for M8T receiver

A) SecureSyncs

- **ECO cut-in for SecureSync:** ECO-000781 in Arena (~14 March, 2016): https://app.bom.com/changes/detail-summary?change_id=2385971714&orb_msg_single_search_p=1

Per Jill, SecureSync/NetClock S/N cut-over from REs-SMT-G to ublox M8T receiver **S/N 11719 (~28 Mar 2016)**

- **Description:** Replace Trimble receiver, MP30R-0GNS-0001, with UBLOX GNSS receiver, 1240-0000-F001, in SecureSync products

Minimum software requirements: SecureSync/9400s series require software version 5.3.2 or higher be installed (cut-into SecureSync with v5.4.1 being shipped). Earlier versions of software can't talk to the ublox receiver.

Carrier board required for SecureSyncs to use the u-blox receiver:

- **1240-1000-0200** (bare carrier board for ublox receiver) in Arena at: https://app.bom.com/items/detail-spec?item_id=1215137017&version_id=10420470768
- **1240-0000-F001** (carrier board, no battery) in Arena at: https://app.bom.com/files/detail-summary?file_master_id=1238771766&file_id=1752262382

B) TSync series timing boards

- ECO cut-in for TSync timing boards (ECO-00699) https://app.bom.com/changes/detail-summary?change_id=2385698104
- Cut-in for TSync boards: ~24 Mar 2016 (**S/N 4601**, per Jill)

FAQs about the ublox M8T receiver/Specs

Max altitude

- Per U-blox, Max altitude for M8T receiver is **50,000 meters (164,041 feet)**
- Per the u-Blox M-8T datasheet https://www.u-blox.com/sites/default/files/NEO-LEA-M8T-FW3_DataSheet_%28UBX-15025193%29.pdf

Operational limits ⁹	Dynamics	≤ 4 g
	Altitude	50,000 m
	Velocity	500 m/s

20 Year rollover counter

- Refer also to separate section in this document specific to 20 YEAR GPS week rollover
 - Last 20 year rollover occurred in **2016**
 - Next 20 year rollover occurs in **2036**

uBlox M8T 2036 year rollover

- **Based on firmware version. Refer to (uBlox document):** <https://www.u-blox.com/en/docs/UBX-19039990>

➤ Excerpt below

In a continuous effort to offer excellent technical support to the customers, u-blox has evaluated all u-blox 5, 6, 7, 8 and M8 receivers and listed the GPS week number roll-over compensation value for each u-blox GNSS receiver firmware version as shown in **Table 1**.

Generation	Firmware	Week number	Start date	End date
u-blox 5	5.x	1460	2007-12-30	2027-08-14
	6.x	1528	2009-04-19	2028-12-02
	6.x	1528	2009-04-19	2028-12-02
u-blox 6	7.x	1603	2010-09-26	2030-05-11
	1.x	1691	2012-06-03	2032-01-17
	7.x	1603	2010-09-26	2030-05-11
u-blox 7	1.x	1691	2012-06-03	2032-01-17
	2.0x	1756	2013-09-01	2033-04-16
	3.0x	1867	2015-10-18	2035-06-02
u-blox 8/M8	3.5x	1936	2017-02-12	2036-09-27

Table 1: Default GPS week number roll-over compensation values of u-blox GNSS receivers

Need to resurvey after sync/movement of the receiver to another location while in Stationary mode

A) Work-around for SecureSyncs/9400s

- Update **version 5.4.5** is implementing a software change that causes the ublox receiver to resurvey if it's relocated after completing a survey in Standard/Stationary mode - alleviating the need to manually delete the position.
- Software versions **5.4.4 and below** need position manually cleared if relocated after initial sync to GPS

Email from Dave Sohn to Derek Darling (3 Jun 16) Here was a statement I put together for service on this:

One of the characteristics of the new ublox receiver is that it does not automatically "resurvey" its position in standard (stationary) mode if the unit is relocated. Stationary mode provides some improved timing stability, operation down to a single satellite, and is able to employ a T-RAIM algorithm that can exclude satellite signal measurements that fall outside expected values. Normally, this behavior is not problematic, however when pre-staging deployments or redeploying systems, the system will survey at the staged location and won't resurvey again at the deployed location, which will prevent the system from synchronizing. The system may show tracked satellites, but will not synchronize to the constellation.

The Spectracom factory has always cleared location (and history) on all SecureSyncs before shipping them to any of our customers, so delivered units will always perform a survey on location.

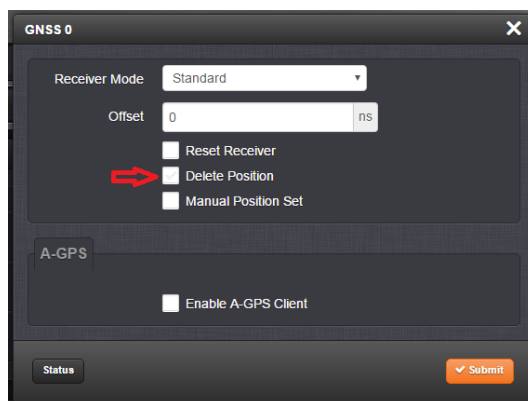
There are two options to minimize any noticeable impact on systems due to staging prior to a move to final install site

change the staging process to perform a "Delete Position" as part of the system power down (details below)

as part of the configuration done during staging, enable mobile mode, which does not perform the survey process. This will not have any appreciable effect on 1PPS (or 10MHz) accuracy. We only saw a difference of 3 ns between the 1 sigma 1PPS synchronization accuracy over 24 hours between the two modes.

To clear position:

Launch a web browser and load the web user interface of the unit
 Navigate to the GNSS status page (Interfaces -> REFERENCES -> GNSS Reference -> GNSS 0)
 On the "Main" tab, click the "Edit" button
 Check the "Delete Position" selection and click the "Submit" button
 The survey will automatically restart
 Shut down the unit prior to survey completion (~33 minutes)



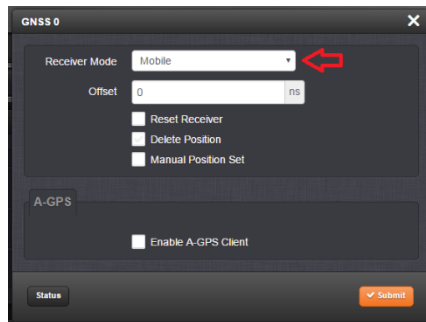
To enable mobile mode:

Launch a web browser and load the web user interface of the unit

Navigate to the GNSS status page (Interfaces -> REFERENCES -> GNSS Reference -> GNSS 0)

On the "Main" tab, click the "Edit" button

Change the "Receiver Mode" selection to "Mobile" and click the "Submit" button



The screenshot shows a web interface window titled "GNSS 0". Inside, there is a "Receiver Mode" dropdown menu currently set to "Mobile", with a red arrow pointing to it. Below this is an "Offset" input field with the value "0" and a unit selector set to "ms". There are three checkboxes: "Reset Receiver", "Delete Position", and "Manual Position Set", all of which are currently unchecked. Below these is a section labeled "A-GPS" with an "Enable A-GPS Client" checkbox, which is also unchecked. At the bottom left is a "Status" button, and at the bottom right is an orange "Submit" button with a checkmark icon.

B) Work-around for TSync series timing boards to resurvey every boot-up is implemented starting in firmware version 3.4.7 (ECO 1625 released 29 March 2018)

- Per the v3.4.7 release notes: “**GNSS receiver will now restart survey on power-up or board reset**”
- The work-around for SecureSyncs/9400s to delete position/resurvey after each reboot was implemented in the network processor software.
- The same work-around for SecureSyncs/9400s to delete position/resurvey after each reboot was implemented in TSync firmware upgrade version 3.4.7 (~29 March 2018)
- TSync boards with firmware versions prior to v3.4.7 firmware, which are synced to GPS after shipment from our factory and then relocated elsewhere will need the GPS position manually cleared before it can sync at the new location.

~~Email from Keith to Tony DiFlorio (20 Feb 17) Tim T just clarified that the work-around that we are using for SecureSyncs and NetClock 9400s with a ublox receiver installed (clearing the position hold after each boot-up for a new survey to be performed) is not available as a work-around for the TSync boards with a ublox receiver (or for a Res-SMT-GG receiver with version 1.0.9 firmware installed).~~

~~The work-around that was added to the SecureSyncs and 9400s needed to be implemented in the “network processor software” (not in the KTS Timing system software). The TSync boards share the KTS timing system software with the SecureSyncs/9400s. But unlike the SecureSyncs/9400s, the TSync boards don’t contain the Network processor software, preventing this work-around from being able to be added to the TSync boards.~~

~~The GNSS receiver is cleared of its position before its shipped from our factory. But if the TSync board is synced to GPS at a location after the board had been received and then relocated thereafter, the TSync board will continue to need its position manually cleared before it can sync at the new location. Unlike SecureSyncs, there are no expected work-arounds/changes expected for the TSync series boards to be able to clear their position automatically.~~

NMEA-0183 outputs for ublox M8T receiver (such as GPGGA, GPRMC and GMZDA)

- Refer to ublox Protocol document: http://ec-mobile.ru/user_files/File/ublox/ublox5_Protocol_Specifications.pdf

Mobile operation (instead of the default Standard/Stationary mode)

Speed over ground / Track angle

We have recently purchased a Spectracom SecureSync time server and had several questions about the GPS positional information.

1. **What is the update rate of the GPS position information, assuming access through the CLI on SNMP?**
2. **Is there any way to access the ground speed or track angle information through either the CLI or SNMP?**
3. **Would the unit moving at moderate speeds (25 knots / 39 mph / 46kph) have any effect on the timing accuracy?**

Reply from Paul Myers (31 Aug 16) They cannot get Speed over ground or track angle. They should have good mobile performance. It will be Mobile Land. I recommend they update AS SOON AS POSSIBLE to Release 5.4.5 because they can see the dynamics.

- What is the update rate of the GPS position information, assuming access through the CLI on SNMP?

PEM: The Receiver updates position at 1 Hz.

- Is there any way to access the ground speed or track angle information through either the CLI or SNMP?

PEM: The Front Panel, command line interface gpsloc command and the SNMP MIB variables for Latitude, Longitude and Altitude can be read. We do **NOT** recommend walking the MIB, however, reading these values at **no faster** than 1Hz is possible.

- Would the unit moving at moderate speeds (25 knots / 39 mph / 46kph) have any effect on the timing accuracy?

PEM: If the user places the SecureSync in Mobile mode, it can be used in mobile operation. The use of timing receivers in low speed, low dynamic (meaning slow turns) motion will be the lowest risk in degrading Time/1PPS signal performance depending on GNSS/GPS Receiver type installed.

The Trimble receivers will experience degraded 1PPS performance 3x worse than our stated specification in the best case. The recommended receiver type to use is the Ublox M8T which should suffer little to no performance loss under these conditions. It is recommended the customer use Release 5.4.1 firmware until Release 5.4.5 is available. Release 5.4.5 will display Land/Sea/Air Dynamics selection for Mobile Mode users.

Thanks for clarifying you have a newer model UBLOX. Here are the answers to your questions:

- What is the update rate of the GPS position information, assuming access through the CLI on SNMP?

Reply from Paul Myers (1 Sept 16) The Receiver updates position at 1 Hz.

- Is there any way to access the ground speed or track angle information through either the CLI or SNMP?

Reply from Paul Myers (1 Sept 16) The Front Panel, command line interface "gpsloc" command and the SNMP MIB variables for Latitude, Longitude and Altitude can be read. We do **NOT** recommend walking the MIB to read the data, however, reading these values at **no faster** than 1Hz is possible.

- Would the unit moving at moderate speeds (25 knots / 39 mph / 46kph) have any effect on the timing accuracy?

Slightly edited Reply from Paul Myers (1 Sept 16) If the user places the SecureSync in Mobile mode, it can be used in mobile operation. The use of timing receivers in low speed, low dynamic (meaning slow turns) motion will be the lowest risk in degrading Time/1PPS signal performance depending on GNSS/GPS Receiver type installed.

The Trimble receivers (Res-T and Res-SMT-GG) will experience degraded 1PPS performance 3x worse than our stated specification in the best case.

The recommended receiver type to use is the ublox M8T which should suffer little to no performance loss under these conditions. It is recommended the customer use Release 5.4.1 firmware until Release 5.4.5 is available. Release 5.4.5 will display Land/Sea/Air Dynamics selection for Mobile Mode users.

Noise Figure for ublox M8T receivers: Noise figures of various GNSS devices

GNSS Antennas

- Noise Figure of 8230 antenna, 1dB typical
- Noise Figure of 8225S antenna, 3dB

GPS Amps

- Noise figure of Model 8227 inline amplifier, 3.5 dB

Maximum noise figure for reliable operation of the ublox receiver is 1.042 dB

Email from Tom Richardson (29 Jan 18) For a system including 8230 antenna, (+40 dB), 400 feet of cable, (-20 dB), an 8227, (+20 dB) and another 400 feet of cable (-20 dB) the Noise figure is 1.042 dB and the gain is 20 dB so it falls within the requirements of less than 1.5 dB of noise figure and gain between 5 and 20. Current draw would be 19 mA for the antenna and 15 mA for the inline amplifier for 34 mA total. Max DC loss would be 34 mA * 1.39 ohms ~ 0.05V DC.

Sensitivity/Gain for the ublox M8T receiver

	ublox receiver min sensitivity		Res-SMT-GG sensitivity (for comparison)	Notes
	(GPS and Glonass)	(GPS and Beidou)		
Acquisition	-148 dBm	-148 dBm	-155 dBm	
Tracking/Navigation	-167 dBm	-165 dBm	-160 dBm	-136 dBm (-160dBW) at surface of the Earth. (Need min 16 dB gain)
Reacquisition	-160 dBm	-160 dBm		

dB Gain

The recommended minimum to recommended maximum dB gain (Antenna/GPS preamp dB gains, minus the antenna cable loss) at the input to the GPS receiver is 16dB. This can also be stated as the following:

The GPS signal at the surface of the earth is -136dBm. The minimum sensitivity for the GPS receiver in the SecureSyncs/TSync boards which have a ublox receiver installed is **-148 dBm**. There has to be enough antenna gain (and inline GPS amps, if needed) to account for the antenna cable loss, for the signal to be at least -145 dBm. The antenna cable loss for Belden RF400 or Time Microwave LMR-400 cable is about 5.5 dB loss/100 feet of cable.

Recommended gain at the GPS receiver (per the receiver manufacturer): 5 dB to 20dB gain

The NEO-M8T includes a SAW filter and an additional LNA and is suitable for use with both passive ¹³ and active ¹⁴ antennas. The LEA-M8T includes a SAW filter and is suitable for use with active antennas and antenna distribution systems. Within the recommended range below, lower overall gain can improve immunity to interference in most situations; higher gain offers slightly better sensitivity.		
Antenna Type		
Active Antenna Recommendations		
Minimum gain	5 dB (at module input)	
Maximum gain	20 dB (at module input)	
Maximum noise figure	1.5 dB	

ublox M8T current specs

The antenna's protect/detect circuit will:

- **short circuit** at around 100 mA.
- **An open circuit** is determined if the antenna current falls below approximately **6 mA**.

Constellation support/configuration

- As of at least March 2016, this receiver supports: GPS, Glonass, BeiDou and QZSS (Galileo support is expected via software update ~ Q4-2016)

Can configure:

1. **GPS only**
2. **Receiver allows only two constellations (or QZSS + up to two other constellations)**

A) SecureSyncs/9400s:

- GPS only (unless **SS-OPT-GNS** option is purchased)
 - refer to (<https://na28.salesforce.com/01tC0000003IGr1?srPos=9&srKp=01t>)
- SS-OPT-GNS option adds Glonass, Beidou and QZSS to GPS
 - **Galileo**: the ublox M8T receiver is hardware compatible with the Galileo constellation, but a firmware update for the Receiver/SecureSync will be needed- expected around Q4-2016)

Difference between Trimble and ublox receivers regarding Standard mode (ublox doesn't re-survey)

Email from Dave Sohn to Derek (3 Jun 16) Here was a statement I put together for service on this:

One of the characteristics of the new ublox receiver is that it does not automatically "resurvey" its position in standard (stationary) mode if the unit is relocated. Stationary mode provides some improved timing stability, operation down to a single satellite, and is able to employ a T-RAIM algorithm that can exclude satellite signal measurements that fall outside expected values. Normally, this behavior is not problematic, however when pre-staging deployments or redeploying systems, the system will survey at the staged location and won't resurvey again at the deployed location, which will prevent the system from synchronizing. The system may show tracked satellites, but will not synchronize to the constellation.

The Spectracom factory has always cleared location (and history) on all SecureSyncs before shipping them to any of our customers, so delivered units will always perform a survey on location.

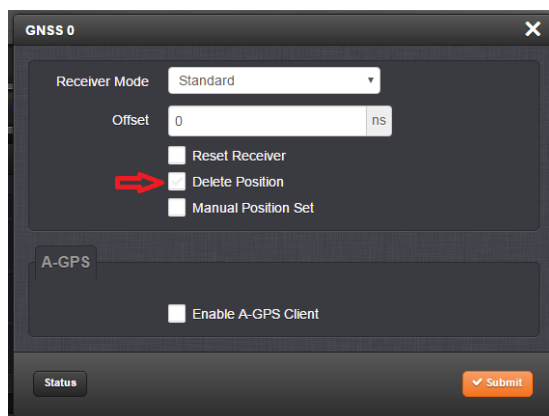
There are two options to minimize any noticeable impact on systems due to staging prior to a move to final install site

1) Change the staging process to perform a "Delete Position" as part of the system power down (details below).

2) As part of the configuration done during staging, enable mobile mode, which does not perform the survey process. This will not have any appreciable effect on 1PPS (or 10MHz) accuracy. We only saw a difference of 3 ns between the 1 sigma 1PPS synchronization accuracy over 24 hours between the two modes.

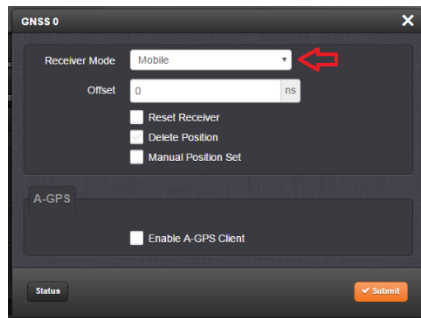
To clear position:

- A) Launch a web browser and load the web user interface of the unit
- B) Navigate to the GNSS status page (Interfaces -> REFERENCES -> GNSS Reference -> GNSS 0)
- C) On the "Main" tab, click the "Edit" button
- D) Check the "Delete Position" selection and click the "Submit" button
- E) The survey will automatically restart
- F) Shut down the unit prior to survey completion (~33 minutes)



To enable mobile mode:

- A) Launch a web browser and load the web user interface of the unit
- B) Navigate to the GNSS status page (Interfaces -> REFERENCES -> GNSS Reference -> GNSS 0)
- C) On the "Main" tab, click the "Edit" button
- D) Change the "Receiver Mode" selection to "Mobile" and click the "Submit" button



B) ublox receivers on TSync timing boards

- All satellite constellations (**GPS**, **Glonass**, **Beidou** and **QZSS**- as well as **Galileo** starting with ublox firmware version 3.0.1) are available without the need to purchase any additional options

Ublox UBX output messages:

- Refer to ublox docs (such as): https://www.u-blox.com/sites/default/files/products/documents/ublox8-M8_ReceiverDescrProtSpec_%28UBX-13003221%29_Public.pdf (also saved in: I:\Customer Service\GPS\GPS receivers\ublox M8T

Groups of message types outputted from ublox receivers

31.7 UBX Class IDs

A class is a grouping of messages which are related to each other. The following table lists all the current message classes.

Name	Class	Description
NAV	0x01	Navigation Results Messages: Position, Speed, Time, Acceleration, Heading, DOP, SVs used
RXM	0x02	Receiver Manager Messages: Satellite Status, RTC Status
INF	0x04	Information Messages: Printf-Style Messages, with IDs such as Error, Warning, Notice
ACK	0x05	Ack/Nak Messages: Acknowledge or Reject messages to CFG input messages
CFG	0x06	Configuration Input Messages: Set Dynamic Model, Set DOP Mask, Set Baud Rate, etc.

UBX-13003221 - R13

Early Production Information

Page 134 of 371



u-blox 8 / u-blox M8 Receiver Description - Manual

UBX Class IDs continued

Name	Class	Description
UPD	0x09	Firmware Update Messages: Memory/Flash erase/write, Reboot, Flash identification, etc.
MON	0x0A	Monitoring Messages: Communication Status, CPU Load, Stack Usage, Task Status
AID	0x0B	AssistNow Aiding Messages: Ephemeris, Almanac, other A-GPS data input
TIM	0x0D	Timing Messages: Time Pulse Output, Time Mark Results
ESF	0x10	External Sensor Fusion Messages: External Sensor Measurements and Status Information
MGA	0x13	Multiple GNSS Assistance Messages: Assistance data for various GNSS
LOG	0x21	Logging Messages: Log creation, deletion, info and retrieval
SEC	0x27	Security Feature Messages
HNR	0x28	High Rate Navigation Results Messages: High rate time, position, speed, heading

All remaining class IDs are reserved.

“ublox receiver data” reported in Timing log

Fields/values

PPS SYNC= x (0= PPS not in sync) (1= PPS is in sync)

H=x (0= Time not in sync) (1= Time is in sync)

Mode=x (0= Single Satellite mode) (1= Standard/Stationary mode) (2= Mobile/Continuous mode)

Note: VersaSync's factory default mode is **Mobile** mode

tAcc=x (where "x" is Time Accuracy Estimate– reported in nanoseconds)

tAccClk= x (where "x" is Time Accuracy Estimate– reported in nanoseconds???)

indoor=0 (I believe this indicates the "indoor messaging service" -IMES- being disabled in the ublox receiver)

Note: "IMES" (associated with Japan's QZSS) appears to be a mode of operation for indoor positioning using low power transmitters

GPS Fix:

None (GPS survey has not yet been completed)

TIMEONLY (5) (GPS survey has completed)

3D (3) (3D fix- with four or more satellites being tracked?)

Oct 5 13:18:11 2017 278 13:18:11 000 PPS SYNC=0 H=1 Mode=1 tAcc=2 tAccClk=6 indoor=0 GPS Fix: NONE (0)
Oct 5 13:18:30 2017 278 13:18:30 000 GNSS FIX CHANGE: NONE (0) to TIMEONLY (5)
Oct 5 13:18:30 2017 278 13:18:30 000 PPS SYNC=1 H=1 Mode=1 tAcc=14 tAccClk=44 indoor=0 GPS Fix: TIMEONLY (5)
Oct 5 13:18:33 2017 278 13:18:33 000 GNSS FIX CHANGE: TIMEONLY (5) to NONE (0)
Oct 5 13:18:33 2017 278 13:18:33 000 PPS SYNC=0 H=1 Mode=1 tAcc=13 tAccClk=16 indoor=0 GPS Fix: NONE (0)
Oct 5 13:18:34 2017 278 13:18:34 000 GNSS FIX CHANGE: NONE (0) to TIMEONLY (5)
Oct 5 13:18:34 2017 278 13:18:34 000 PPS SYNC=1 H=1 Mode=1 tAcc=12 tAccClk=13 indoor=0 GPS Fix: TIMEONLY(5)
Oct 5 13:43:10 2000 001 00:00:05 000 GNSS FIX CHANGE: TIMEONLY (5) to NONE (0)
Oct 5 13:43:10 2000 001 00:00:05 000 PPS SYNC=0 H=1 Mode=1 tAcc=4556 tAccClk=3 indoor=0 GPS Fix: NONE (0)
Oct 5 13:43:10 2000 001 00:00:05 000 GNSS Source of UTC-GPS Offset from Unknown(255) to GPS(2) V=3
Oct 5 13:43:10 2000 001 00:00:05 000 Changing GNSS Source of Leap Second from None(0) to GPS(2) V=3
Oct 5 13:43:10 2000 001 00:00:05 038 GR antenna fault.
Oct 5 13:43:10 2000 001 00:00:06 000 GNSS FIX CHANGE: NONE (0) to 3D (3)
Oct 5 13:43:10 2000 001 00:00:06 000 GR antenna ok.
Oct 5 13:43:10 2000 001 00:00:08 000 PPS SYNC=1 H=1 Mode=1 tAcc=30 tAccClk=56 indoor=0 GPS Fix: 3D (3)
Oct 5 13:43:10 2017 278 13:43:03 000 GNSS FIX CHANGE: 3D (3) to NONE (0)
Oct 5 13:43:10 2017 278 13:43:03 000 PPS SYNC=0 H=1 Mode=1 tAcc=2555 tAccClk=4 indoor=0 GPS Fix: NONE (0)
Oct 5 13:43:10 2017 278 13:43:03 038 GR antenna fault.
Oct 5 13:43:10 2017 278 13:43:03 000 GR antenna ok.
Oct 5 13:43:10 2017 278 13:43:04 000 GNSS FIX CHANGE: NONE (0) to 3D (3)
Oct 5 13:43:10 2017 278 13:43:04 000 PPS SYNC=1 H=1 Mode=1 tAcc=420 tAccClk=36 indoor=0 GPS Fix: 3D (3)
Oct 5 13:43:10 2017 278 13:43:05 000 PPS SYNC=0 H=1 Mode=1 tAcc=118 tAccClk=420 indoor=0 GPS Fix: 3D (3)
Oct 5 13:43:10 2017 278 13:43:06 000 PPS SYNC=1 H=1 Mode=1 tAcc=67 tAccClk=118 indoor=0 GPS Fix: 3D (3)
Oct 5 13:47:44 2017 278 13:47:44 000 GNSS FIX CHANGE: 3D (3) to NONE (0)
Oct 5 13:47:44 2017 278 13:47:44 000 PPS SYNC=0 H=1 Mode=1 tAcc=4 tAccClk=4 indoor=0 GPS Fix: NONE (0)
Oct 5 13:48:04 2017 278 13:48:04 000 GNSS FIX CHANGE: NONE (0) to 3D (3)
Oct 5 13:48:04 2017 278 13:48:04 000 PPS SYNC=1 H=1 Mode=1 tAcc=165 tAccClk=49 indoor=0 GPS Fix: 3D (3)
Oct 5 14:15:31 2017 278 14:15:31 000 GNSS FIX CHANGE: 3D (3) to TIMEONLY (5)
Oct 5 14:15:31 2017 278 14:15:31 000 Standard Survey completed in 2000 sec with 3D-Variance 877643 mm^2
Oct 5 15:20:33 2017 278 15:20:32 000 Empty UBX FIFO
Oct 5 15:26:25 2017 278 15:26:25 000 Empty UBX FIFO
Oct 8 02:41:02 2017 281 02:41:02 000 PPS SYNC=0 H=0 Mode=1 tAcc=3 tAccClk=3 indoor=0 GPS Fix: TIMEONLY (5)
Oct 8 02:42:06 2017 281 02:42:06 000 PPS SYNC=1 H=1 Mode=1 tAcc=2 tAccClk=2 indoor=0 GPS Fix: TIMEONLY (5)

“GPS0 UBX Message receive Checksum Error”/ “GPS0 UBX Message receive buffer overflow” (observed in SecureSync logs)

- Suspect these are associated with the initial start-up of the uBlox receiver.

A) Both error messages above asserted

- Refer to Salesforce Case 274882

Report from customer We had a weird problem that we are unable to reproduce. We booted up the SecureSync 1200 (with a u-blox 8) connected to a GPS antenna and it started getting two error messages:

046 GPS0 UBX Message receive Checksum Error

031 GPS0 UBX Message receive buffer overflow

The errors persisted through one hardware reboot and did not through a second.

B) Just “GPS0 UBX Message receive Checksum Error” asserted

- Refer to Salesforce Case 232034

Email from Ron Dries (8 May 2020) Looking in the timing.log file there are a lot of checksum error messages:

May 7 11:38:50 Spectracom Spectracom: [system] 2020 128 11:38:50 046 GPS0 UBX Message receive Checksum Error

May 7 11:38:53 Spectracom Spectracom: [system] 2020 128 11:38:53 046 GPS0 UBX Message receive Checksum Error

May 7 11:38:57 Spectracom Spectracom: [system] 2020 128 11:38:56 046 GPS0 UBX Message receive Checksum Error

May 7 11:38:59 Spectracom Spectracom: [system] 2020 128 11:38:59 046 GPS0 UBX Message receive Checksum Error

May 7 11:39:00 Spectracom Spectracom: [system] 2020 128 11:39:00 046 GPS0 UBX Message receive Checksum Error

This indicates to me that there is communication issues between KTS and the GPS receiver, but I don't see any indications of other communication issues so KTS is still functioning correctly.

My feeling is that it is something with the receiver but I think we will need to RMA it to diagnose what happened for sure.

Update (2 Aug 2021) for RMA 232034, Repair team found faulty/replaced GNSS receiver

ublox receiver used in Legacy VelaSyncs (Smart GXClock-500 from SpectraTime)

- PCB/oscillator/receiver assembly is the **Smart GXClock-500** from SpectraTime
- Our P/N: **MP34R-0004-0001** (in Arena): https://app.bom.com/items/detail-attach?item_id=1203441444&version_id=10254028448&orb_msg_single_search_p=1&redirect_seqno=7551326510
- **Datasheet** <http://www.spectratime.com/products/isync/gps-ocxo/>
- At time of Legacy VelaSync product release, the assembly uses a **ublox Model LEA-6T-001** GPS receiver
- **Refer to:** <http://www.ublox.com/en/gps-modules/ublox-6-timing-module/lea-6t.html>
- ~~<http://www.ublox.com/en/lea-5t.html>~~ (earlier Model LEA-5T-001 receiver)
- GPS Receiver sensitivity:

Tracking: -162 dBm
Cold starts: -148 dBm
Reacquisition (hot start): -157dBm

Receiver performance data

Receiver type	50-channel u-blox 6 engine GPS L1 C/A code SBAS: WAAS, EGNOS, MSAS	
Navigation update rate	up to 5 Hz (2 Hz for LEA-6T-1)	
Accuracy	Position	2.5 m CEP
	SBAS	2.0 m CEP
Acquisition	Cold starts:	26 s
	Aided starts:	1 s
	Hot starts:	1 s
Sensitivity	Tracking:	-162 dBm
	Cold starts:	-148 dBm
	Hot starts:	-157 dBm

Environmental data, quality & reliability

Operating temp.	-40° C to 85° C
Storage temp.	-40° C to 85° C
RoHS compliant (lead-free)	
Qualification according to ISO 16750	
Manufactured in ISO/TS 16949 certified production sites	

	Ublox receiver sensitivity	Res-SMT-GG sensitivity (for comparison)	Notes
Acquisition	-148 dBm	-155 dBm	
Tracking	-162 dBm	-160 dBm	-136 dBm (-160dBW) at surface of the Earth (Need 16 dB gain)

Recommended gain at the GPS receiver: **22dB to 30dB gain**

For power conversion: refer to <http://www.radiomar.net/convDBWen.htm>

Note: GPS signal strength is -136 dBm at surface of the Earth (-160dBW).

The Sensitivity spec for the ublox receiver states Acquisition = -148 dBm, Tracking = -162dBm. I would subtract about 3 dB for the internal cable so the minimum should be -145 dBm.

- **Recommended minimum signal strength:** -145 dBm

The recommended minimum to recommended maximum dB gain (Antenna/GPS preamp dB gains, minus the antenna cable loss) at the input to the GPS receiver is 17 dB. This can also be stated as the following:

The GPS signal at the surface of the earth is -136dBm. The minimum sensitivity for the GPS receiver in the Legacy VelaSyncs, which have a ublox receiver installed, is -148 dBm. There has to be enough antenna gain (and inline GPS amps, if needed) to account for the antenna cable loss, for the signal to be at least -145 dBm. The antenna cable loss for Belden RF400 (RG-8) or Times Microwave LMR-400 cable is about 5.5 dB loss/100 feet of cable.

Trimble Tech support contact info

Trimble_Support@Trimble.com Your password is: R1WvGrJlpW

Support for Resolution-T (Res-T) receivers (not SAASM)

Primary contact
Brad Lynch
Trimble Navigation - Advanced Devices Division
North American Sales Manager - Technology Sales Group
GPS, GNSS and RFID Solutions
Mobile: 408-242-3968
brad_lynch@trimble.com

Secondary contact for Res-T receivers (not SAASM)

Christian Voit
(Sales Engineer & FAE, Germany)
Christian_Voit@Trimble.com
+49 (2131) 133 9271

Julian Dortort
Trimble Navigation - Advanced Devices Division
Customer Support Manager - Technology Sales Group
GPS, GNSS and RFID Solutions
935 Stewart Drive
Sunnyvale, CA 94085-3913
Google Voice: +1 650 918 6848
email: julian_dortort@trimble.com

Support for SAASM (Force 22/22E) GPS receivers:

Bruce Swearingen
System/Application Engineer
Military Technical Support
bruce_swearingen@trimble.com
408 481 7568

Trimble Res-SMT-GG / Resolution SMT-GG Multi-GNSS receiver (Multi-GNSS GPS/Glonass)

- Our P/N: MP30R-0GNS-0001
 - (in Arena) at: https://app.bom.com/items/detail-spec?item_id=1202844940&version_id=10381202658
- Trimble P/N: 99974-00, 89999-00

Link to Trimble data sheet: http://www.trimble.com/timing/pdf/022542-039A_Resolution_SMT_GG_DS_0412_US_LR.pdf

Link to Trimble Res-SMT-GG user manual: <http://trl.trimble.com/docushare/dsweb/Get/Document-652340/>

Link to Trimble website: <http://www.trimble.com/timing/resolution-smt-gg.aspx>

Link to Engineering info (datasheet, user guide, etc): <I:\Engineering\GPS RCVRs\Trimble GPS\ResSMT> and <I:\Engineering\GNSS Receiver>

**Positional accuracy for the Res-SMT-GG receiver

- Specs below (from the Res-SMT-GG data sheet http://www.trimble.com/timing/pdf/022542-039A_Resolution_SMT_GG_DS_0412_US_LR.pdf) are for a stationary location.
- The GNSS receiver is updated at a 1 Hz rate (this rate is not configurable)
- Positional/timing accuracy while in motion is not specified by either Trimble or Spectracom:

PERFORMANCE SPECIFICATIONS	
Accuracy Horizontal Position	<6 meters (50%) <9 meters (90%)
Accuracy Altitude Position	<11 meters (50%) <18 meters (90%)
Time to First Fix (no stored position)	<46 sec. (50%) <50 sec. (90%)
Time to First PPS (stationary with stored position, e.g., recovery after power outage)	<14 sec. (50%) <18 sec. (90%)
Re-acquisition after 60-second signal loss	<2 sec. (90%)
Sensitivity	
Tracking	-160 dBm
Acquisition	-155 dBm
Dynamics	
Velocity	.600m/s
Acceleration	.4 g (39.2 m/sec ²)
Jerk	.20 m/sec ³

Q This is Kyle Huggins with ISA.... We would also like to make use of the position data, however. From looking at the card's position data (using GR_GetPosition from the examples), it appears that the position is only updated once every second (a little after the 1PPS it seems). So my question to you is this: Is the position reported by the GPS updated once per second? If it is, then my next question is: is it configurable? If not, then my question is: *when* precisely is that position data tied to? Immediately after the 1PPS? 10ms after?

A Reply from Keith, after talking to Paul Myers (19 Aug 15) Your observations are correct in that the receiver has a 1 Hz update rate. As long as the receiver is calculating fixes (tracking at least four satellites as needed for a 3D fix) the Tsync board reads its current position from the receiver each second. This position is read and updated in the TSync board very shortly after the 1PPS on-time point of each second.

How soon after each second the position is read and updated may vary each second, based on other processes running at that moment. But the best estimate is the position will be read/updated within the first 0.5 second and likely within the first 0.10 second, each second while the receiver is able to calculate a fix for that second.

Potential Draft email: With the TSync-PCIe board's onboard GNSS receiver reconfigured to operate in Continuous mode (instead of

the factory default Standard/stationary mode, there is some degradation of the timing accuracy capabilities for the GPS reference.

The actual degradation of its timing performance of the receiver while in motion is not specified by either the GNSS receiver manufacturer or by Spectracom, as the amount of degradation is dependent upon the dynamics of movement while it's in motion (such as the tightness of turns, velocity, etc). However, in general, it's likely to be in the nanoseconds range (not in the seconds range and not likely to be in the milliseconds range, for instance).

****Receiver 1PPS Timing accuracy for RES-SMT-GG/ Positional accuracy**

- **Standard/Stationary mode:** Synced to within 15 nanoseconds of UTC or GPS (1 sigma).
- **Mobile mode:** Unlike the Res-T GPS receiver, Trimble doesn't spec degradation of the Res-SMT-GG receiver while it's in motion (Res-T is 3 times worse in Mobile mode versus stationary accuracies). From the Trimble documentation, they assume the RES-SMT-GG receiver is being used in a stationary environment!
 - Positional/timing accuracy while in motion is not specified by either Trimble or Spectracom:
- **Per the Trimble manual,** the receiver is updated at a 1 Hz rate (this rate is not configurable)
- **Per the Trimble Res-SMT-GG user manual** "A position error of 100 meters corresponds to a time error of approximately 333 ns"

Potential Draft email: With the TSynC-PCIe board's onboard GNSS receiver reconfigured to operate in Continuous mode (instead of the factory default Standard/stationary mode, there is some degradation of the timing accuracy capabilities for the GPS reference.

The actual degradation of its timing performance of the receiver while in motion is not specified by either the GNSS receiver manufacturer or by Spectracom, as the amount of degradation is dependent upon the dynamics of movement while it's in motion (such as the tightness of turns, velocity, etc). However, in general, it's likely to be in the nanoseconds range (not in the seconds range and not likely to be in the milliseconds range, for instance).

****Bias voltage (output to antenna): 5vdc**

- The antenna's protect/detect circuit will short circuit at around 100 mA.
- Trimble recommends that you keep the antenna current below 75 mA. An open circuit is determined if the antenna current falls below approximately 2mA

****Receiver accuracy based on GPS/Glonass vs Glonass only operation**

Alignment of 1PPS output from receiver to system, based on the satellite constellation (GPS/Glonass) selected

- Refer to Mantis case 2938
- **Summary:** SecureSync 1PPS output can be offset (by up to 300ns) depending on which GNSS constellations are selected. Different timescales have different definitions of their 1PPS Signal

Q from Sylvain: I suppose the **NTP accuracy** is the same when you use GLONASS only or GPS/Glonass or GPS only with the SecureSync. So: **time accuracy < 10ms**.

A. After talking to Paul Myers, it sounds like if the RES-SMT-GG receiver is in Glonass only mode, the PPS is still very stable. But based on our testing, there appears to be several nanosecond differences between GPS only mode, Glonass only mode and combined GPS/Glonass mode. The PPS out isn't absolutely coincident in all three modes. There appears to be a slight shift in the PPS when switching between the three possible modes.

Environmental specs

****RES-SMT-GG Receiver Sensitivity**

- (-160dBW).
- Res-SMT-GG receiver is much more sensitive to weaker signals than the Res-T receivers

Comparison of RES-SMT-GG versus Res-T

Res-SMT-GG receiver sensitivity (and Res-T data sheet for comparison)

	Res-SMT-GG sensitivity	Res-T sensitivity (for Comparison)	Notes
Acquisition	-155 dBm	-136 dBm	
Tracking	-160 dBm	-141 dBm	-136 dBm (-160dBW) at surface of the Earth. (Need 30 dB gain)

Recommended gain at the GPS receiver: **22dB to 30dB gain**

For power conversion: refer to <http://www.radiomar.net/convDBWen.htm>

Minimum recommended signal strengths for RES-SMT-GG

- Recommended minimum signal strength for RES-SMT-GG -155dBm
- * Minimum signal strength for RES-T GPS receiver (for comparison): -136 dBm (-166dBW).

Note: GPS signal strength is -136 dBm at surface of the Earth (-160dBW).

The Sensitivity spec for the RES-SMT-GG receiver states Acquisition = -155 dBm, Tracking = -160 dBm. I would subtract about 3 dB for the internal cable so the minimum should be -152 dBm.

- **Recommended minimum signal strength:** -152dBm
- **Sensitivity for the Res-T receiver:** -155 dBm

The recommended minimum to recommended maximum dB gain (Antenna/GPS preamp dB gains, minus the antenna cable loss) at the input to the GPS receiver is 20 to 30 dB. This can also be stated as the following:

The GPS signal at the surface of the earth is -136dBm. The minimum sensitivity for the GPS receiver in the SecureSyncs that have the newer RES-SMT-GG receiver installed is -155 dBm. There has to be enough antenna gain (and inline GPS amps, if needed) to account for the antenna cable loss, for the signal to be at least -152 dBm. The antenna cable loss for Belden RF400 (RG-8) or Time Microwave LMR-400 cable is about 5.5 dB loss/100 feet of cable.

****Res-SMT-GG receiver firmware versions**

Q Two versions are reported by the receiver- which one do we care about??? **the first of the two (as confirmed by Keith with the screenshots below, 1 Aug 2019)**

Note: The Trimble receiver reports two versions (one after the other).

```
login as: spadmin
Using keyboard-interactive authentication.
Password:
Spectracom SecureSync Version 5.8.2
spadmin@Spectracom ~ $ version gps
GPS 0 Mfr/Mdl: Trimble RES-SMT GG

GR (0) Rcv Info (66 bytes):
-----
Serial #: 0 71135400
Date:      9/17/2014
-----
Appl Ver: 1.9
Date:      8/1/2016
-----
Core Ver: 1.6
Date:      8/1/2016
-----
```

Answer: as shown below in green, we care about the **bolded first** reported version – and not the **second** version (the green “1.9” value in the example below is the only one which matters to is)

Example report (from the manifest log, of the same unit as the CLI “version gps” command above)

GNSS Receiver GPS 0 Mfr/Mdl: Trimble RES-SMT GG

Versions: 0 71135400 9/17/2014 **1.9** 8/1/2016 **1.6** 8/1/2016 (this receiver is at version “1.9” or “1.09”)

(1 Aug 2019, as observed by Keith) apparent issue with SecureSyncs/9400s reporting the correct RES-SMT-GG version (two different versions, such as 1.6 and 1.9, being reported between corresponding Manifest.log and update.log entries)

I noticed in 5.7.1/ 5.8.4 units:

1) **Manifest.log** was reporting GG receiver as: “Versions: **1.6** 1.9 0 0”

2) Its corresponding (same Time/Date) **update.log** was reporting: “GNSS **1.9** 1.9 No Upgrade Needed (SWUE)”

So which version is actually correct- 1.6 per manifest, or 1.9 per update.log??

RES-SMT-GG receiver versions (ascending order)

v1.06 (1.6)

- First firmware rev we've used in our products

v1.07 (1.7)

- Improved issues with 1PPS
- Can cause receiver to periodically drop to 0 satellites for just a few seconds (or at least report its tracking 0 sats for a few seconds in the Qual log-not known if this is a reception issue or just a reporting issue)

v1.08 (1.8)

- Much improved performance with 1PPS and UTC offset not changing.
- Cut into SecureSync with **v5.3.0** upgrade, ~Sept 2015.
- Cut into TSync boards with a deviation, ~Aug 2015.

V1.09 (1.9)

- Refer to ECO 979 (Sept 2016), in Arena at: https://app.bom.com/changes/detail-summary?change_id=2386957641
- Fix for one second error caused by 2016 leap second pending issue (not cut-in yet, as of Aug, 2016)
- Expected to be cut-into the TSync boards ~Sept 2016.

V1.10 (1.10)

Note: info below as of 15 Oct 2019...

➤ Version 1.9 has intermittent 1PPS spikes
(per Trimble SMT-GG 1.10 Release notes):

2. During the time period of Oct 7, 2018 the PPS output on some units were exhibiting 1 millisecond PPS errors. This offset would continue for a couple of seconds, then return to the correct phase, only to repeat the issue again in about 30 seconds. These "bursts" of PPS error would continue for 60 to 300 seconds. The PPS then returned to normal operation.

In looking at the almanac data gathered from another, independent receiver, anomalies were observed in the data being transmitted in the almanac information for PRN27 which persisted until Oct 11, 2018. These anomalies contained different PRN 27 almanac information being transmitted from different satellites.

The methodology of the marking of the health, while allowed by the ICD, was slightly irregular. The almanac data containing orbital parameters being transmitted by the satellites for PRN27 included very large error in the clock offset for the satellite.

The module contains code for a false correlation locking routine that would disqualify a satellite if there was a large discrepancy between the orbital parameters, but it failed to take into account a false lock due to a large clock discrepancy.

The correlation locking routine was modified to correct that shortcoming by forcing use of the ephemeris parameters immediately upon detection of the error. This causes PRN27 to be reacquired, with proper phase and data correlation so that there is no longer a 1 millisecond error for that satellite.

3. Added robustness on system time correction and improved the management for the almanacs updates.

- fix for Res-SMT-GG associated with "bad satellite" PRN 24
- Believe shipped only to Hughes so-far, as a Special release
- Released to SecureSync/9400s production in update **version 5.8.6** (Oct 2019)
- Planned for TSync boards sometime in the future.

Software/firmware support for the newer Res-SMT-GG receiver (upward/downward compatibility with Res-T Receivers)

- The communication protocols for the Res-T and Res-SMT receivers are not exactly the same.
- Earlier software/firmware versions in our products are NOT upward compatible for the newer RES-SMT-GG receiver. So, newer versions of software / firmware ARE necessary when swapping a Res-T receiver for a Res-SMT receiver with earlier firmware.
- Installing a RES-SMT-GG on earlier firmware will cause the receiver to not be able to communicate (Antenna Sense=Unknown for example).
- Newer software/firmware versions that support RES-SMT receivers ARE downward compatible with the earlier Res-T receivers. They will work with either receiver.

A) SecureSync: Software versions 5.0.0 and above support the RES-SMT-GG (and RES-T) receivers.

- Earlier firmware versions need to be updated to v5.0.0 to be able to work with a RES-SMT-GG receiver (ECN 3244, June 2013)

Cut-in info for the Res-SMT-GG

A) SecureSync/9400 Cut-in info (SecureSync: Switching from Trimble Res-T to Res-SMT receivers)

- **Cut-in ECN to support receiver in SecureSyncs:** ECN 3228, 7 Nov 2013 (ECN closed)
- **Cut-in ECN to support receiver in NetClock 9483/9489:** ECN 3265, 7 Nov 2013 (ECN closed)
 - I believe we actually started shipping SecureSyncs/NetClock 9400s **with Res-SMT-GG** receivers **~2 Apr 2014**
 - Based on this best guess date of **2 Apr 2014**, best guess Cut-in Serial Number is **~5408**

Res-SMT-GG receiver versions for SecureSyncs

- Refer also to: [Software release dates.xlsx](#)
 - **1.10** applied in update [version 5.8.6](#) (patch available for versions 5.8.5 and below)
 - **1.09 (1.9)** applied in update [version 5.4.5](#)
 - **1.08 (1.8)** applied in update [version 5.3.0](#)
 - **1.07 (1.7)** applied in update [version 5.1.7](#).
 - **1.06 (1.6)** I believe this is the first version we have used since we started shipping Res-SMT receivers (Res-SMT-GG receiver started shipping ~2 Apr 2014 while we were shipping v5.1.3)

B) TSync Cut-in info (Switching from Trimble Res-T to Res-SMT receivers)

- Firmware **versions 2.2.1 and above** support the RES-SMT-GG (and RES-T) receivers.
- Earlier firmware versions need to be updated to be able to work with a RES-SMT-GG receiver.
 - **Cut-in ECN for TSynCs:** ECN 3436, ~28 March, 2014
 - Best guess cut-in Serial Number: **2247, 2251 and higher**

Temporary deviation to use up existing Res-T receivers before shipping Res-SMT to use up stock

This deviation was implemented after we had started shipping Res-SMT-GG receivers in SecureSync/9400s

Deviation 000047 (May 2015) to ship Res-T in place of Res-SMT-GGs (except for Harris and Skylight)

- Refer to: https://app.bom.com/changes/detail-summary?change_id=2385096515

**(Jul/Aug 2016) Leap second asserted upon GPS notification of Dec 2016 leap second

- One second offset (GPS to UTC offset went to 18 instead of remaining 17) caused when GPS asserted notification (~19 Jul, 2016) of pending leap second
- Refer to ECO-00986 (https://app.bom.com/changes/detail-summary?change_id=2386971148&) for hot patch of Res-SMT-GG receiver update to Trimble firmware version 1.09, or update the SecureSync/NetClock to version 5.4.5 software to fix.

****Desire to Blacklist (Mask/Unmask) a Satellite from being received by a Trimble RES-SMT-GG receiver**

- Refer to Salesforce case 179110
- Refer to the communication letter about PRN27 and the example email discussing this capability in: <..\..\GPS\GPS receivers\Res-SMT-GG receiver>

Partial email Keith sent (8 Feb 2019) (not in all red, as there is color-coding in this email)

For your information:

Blacklisting (masking) any desired satellite from the TSync board's GNSS receiver is the same process as could also be used to blacklist PRN27 (before a fix for the receiver was made available). The Satellite you wish to blacklist just needs to replace "PRN27" in the associated command, available to mask/unmask this particular satellite.

Attached you should find a copy of the communication we sent out last October, about satellite PRN27. Towards the bottom of the first page (under the header of "**For TSYNC products utilizing RES-SMT-GG receivers**") is a section discussing the commands used to either mask (blacklist) or unmask PRN27 (and to reset the receiver). These two mask/unmask commands can be slightly modified to mask/unmask any other desired satellite, as well.

The base TSync-PCIe-PCI Example program/API call used to mask/unmask a satellite is "**GR_SendCustom**"

The complete command to:

Mask PRN27 is: **GR_SendCustom 0 0 10 39 02 1B 10 03**

Unmask PRN27 is: **GR_SendCustom 0 0 10 39 01 1B 10 03**

In these two commands above, the "**02**" and "**01**" are the indicator to either **mask** or **unmask** the satellite. Just after the "**02**" and "**01**" is "**1B**", This is the Hex number for the satellite ID desired to be masked (or unmasked). "**1B**" in Hex correlates to "27" decimal (for PRN27).

So, to either mask or unmask any other satellite besides PRN27, just convert its ID number from Decimal to Hex, and replace the "**1B**" in the applicable command above. Refer to the bottom of page 1 for the complete process, including the resetting of the receiver.

Known firmware issues with Res-SMT receiver (SecureSyncs, TSyns, EC20S)

Version 1.9 has intermittent 1PPS spikes (per Trimble SMT-GG 1.10 Release notes):

2. During the time period of Oct 7, 2018 the PPS output on some units were exhibiting 1 millisecond PPS errors. This offset would continue for a couple of seconds, then return to the correct phase, only to repeat the issue again in about 30 seconds. These "bursts" of PPS error would continue for 60 to 300 seconds. The PPS then returned to normal operation.

In looking at the almanac data gathered from another, independent receiver, anomalies were observed in the data being transmitted in the almanac information for PRN27 which persisted until Oct 11, 2018. These anomalies contained different PRN 27 almanac information being transmitted from different satellites.

The methodology of the marking of the health, while allowed by the ICD, was slightly irregular. The almanac data containing orbital parameters being transmitted by the satellites for PRN27 included very large error in the clock offset for the satellite.

The module contains code for a false correlation locking routine that would disqualify a satellite if there was a large discrepancy between the orbital parameters, but it failed to take into account a false lock due to a large clock discrepancy.

The correlation locking routine was modified to correct that shortcoming by forcing use of the ephemeris parameters immediately upon detection of the error. This causes PRN27 to be reacquired, with proper phase and data correlation so that there is no longer a 1 millisecond error for that satellite.

3. Added robustness on system time correction and improved the management for the almanacs updates.

At least versions 1.6 through 1.9 have a sporadic minor math error issue with GPS week number resulting in a momentary 1PPS timing glitch (next event won't be until Sept 2021)

- RES-SMT-GG has math error causing PPS spike on certain GPS week numbers
 - Timing glitch magnitude can be around 200 ns to 1.1 microseconds.
- Applicable only to the Res-SMT-GG receiver (not Res-T)
- Refer to JIRA case number JIRA-SSS-161
- Refer to "06-02-1024-02-ACU_ResSMTGG.UTC-PPS.pdf: <I:\Customer Service\GPS\GPS receivers\Res-SMT-GG receiver>
- Harris observed alarms asserted in Oct, 2016 time-frame.
- At least Trimble firmware versions 1.6 through 1.9 are affected (not known at this time if Trimble intends to fix this).
- Next known event not expected to occur again, until Sept, 2021.

Version 1.09 (1.9 ~Sept 2016) not performing new GPS survey/won't resync after being relocated

- Refer to JIRA case SSS-137.
- Confirmed issue with receiver version 1.9. Possibly also an issue with version 1.8.
- Must delete position after relocating receiver before it will go into sync (even though its tracking just fine)

A) RES-SMT-GG in SecureSyncs/9400s

- GPS Time data will be valid (green) but GPS PPS will remain not valid (red) until position is deleted in the Interfaces -> GNSS 0 page of the browser
- The work-around for SecureSyncs/9400s to delete position/resurvey after each reboot was implemented in the network processor software.
- Firmware versions prior to v need to reset the receiver position to resurvey at a new location.

Email from Dave Lorah (15 Sept 16) Looks like we have an issue with the new Trimble GG receiver patch. The receiver will not resurvey if moved to a new location after the patch is applied.

So yesterday before I left work I deleted the position. The receiver tracked satellite fine and let the survey complete. All was well.

Then I took the SecureSync home and when I powered up it was not able to sync. No satellites were shown as being tracked even though I saw the bar graphs indicate satellites on the front panel display. I switched to Mobile mode and immediately it showed tracking 7 satellites. I then updated the firmware from 5.4.0 to 5.4.5 (receiver was already at v1.9 due to the patch previously applied) and switched to standard mode. I let the survey complete at home.

B) RES-SMT-GG with TSync timing boards

Resurvey every boot-up is implemented starting in firmware version 3.4.7 (ECO 1625 released 29 March 2018)

- Per the v3.4.7 release notes: **“GNSS receiver will now restart survey on power-up or board reset”**
- The same work-around for SecureSyncs/9400s to delete position/resurvey after each reboot was implemented in TSync firmware upgrade version 3.4.7 (~29 March 2018)
- TSync boards with firmware versions prior to v4.5.7 firmware, which are synced to GPS after shipment from our factory and then relocated elsewhere will need the GPS position manually cleared before it can sync at the new location.

~~Email from Keith to Tony DiFlorio (20 Feb 17) Tim T just clarified that the work-around that we are using for SecureSyncs and NetClock 9400s with a ublox receiver installed (clearing the position hold after each boot-up for a new survey to be performed) is not available as a work-around for the TSync boards with a ublox receiver (or for a Res-SMT-GG receiver with version 1.0.9 firmware installed).~~

~~The work-around that was added to the SecureSyncs and 9400s needed to be implemented in the “network processor software” (not in the KTS Timing system software). The TSync boards share the KTS timing system software with the SecureSyncs/9400s. But unlike the SecureSyncs/9400s, the TSync boards don’t contain the Network processor software, preventing this work-around from being able to be added to the TSync boards.~~

~~The GNSS receiver is cleared of its position before its shipped from our factory. But if the TSync board is synced to GPS at a location after the board had been received and then relocated thereafter, the TSync board will continue to need its position manually cleared before it can sync at the new location. Unlike SecureSyncs, there are no expected work-arounds/changes expected for the TSync series boards to be able to clear their position automatically.~~

**** (June 2015) Issues fixed in firmware version 1.0.8 (1.8), which was implemented in SecureSync software update version 5.3.0)**

A) Loss of GPS reception for just one or a couple of seconds

Email from Paul Myers (30 June 15): Results in testing thus far show the RES-SMT-GG v1.08 improves PPS Stability when using GPS+GLO. Also, our observation of Qualification Logs on SecureSync’s shows good tracking performance with multiple SecureSync’s showing no drops to 0 satellites when running v1.08, while a control unit running v1.07 does show a few drops to 0 satellites for 1-2 sec.

Tim T has been doing board testing with 1.08 and we should check to see if he is seeing any 0 satellites log entries.

V1.08 will be in the upcoming SecureSync 5.3.0 release.

B) Poor 1PPS performance when Glonass is enabled

- For SecureSyncs, this only applies with units that have Glonass license installed and have Glonass enabled
- **Short term fix (as of 30 Jun 2015) until a field update is available** is to disable Glonass, if possible. Or the GNSS receiver can be returned to us for update to 1.0.8 (added in version 5.3.0 update) if Glonass reception is necessary.

(Sept 2014) Issues fixed in RES-SMT-GG receiver firmware version 1.0.6

A) (Sept/Oct 2014) 1PPS jump of a few hundred milliseconds

- **Refer to** Mantis case 2935 <http://cvsmantis.int.rolia.com/mantis/view.php?id=2935>
- **Summary:** 1PPS Jump in RES-SMT-GG might be caused by a position change in receiver calculations
- **Description:** The unexpected 1PPS jump to a few hundred msec off of the GPS 1PPS 'might' be caused by an intermittent error in the position calculation causing the GNSS receiver to incorrectly adjust 1PPS.

B) (Sept/Oct 2014) Potential for Res-SMT-GG receiver to cause time jumps (several seconds) in certain SecureSyncs/9400s and TSyncl-PCIe boards

Potential Issue: Res-SMT-GG receivers can potentially start to output the wrong number of seconds of UTC offset for a period of time, resulting in System Time jumping by the error in this value, when the device is synced to GPS. The GNSS receiver automatically corrects the time with the next ephemeris download (within 12.5 minutes of the issue occurring).

Refer to the SecureSyncCustAssist or TsyncCustassist documents for additional information.

One customer observed a 12 second time jump occur on a SecureSync for about 6 minutes. Then it automatically corrected.

Reportedly fixed with the Res-SMT-GG version 1.0.7 firmware update, being made available in the SecureSync version 5.1.7 update (Nov, 2014)

C) (Sept/Oct 2014) Erratic leap second warning asserted

Reportedly fixed with the Res-SMT-GG version 1.0.7 firmware update, being made available in the SecureSync version 5.1.7 update (Nov, 2014). As of Jan 2015, TSyncl boards were still being shipped with 1.06 firmware. Will switch once Trimble uses up existing stock and sends them to us with 1.07 installed.

Note: This erroneous leap second being scheduled is not likely to be applied to the system. So it's highly unlikely to affect operation of the SecureSync. With versions 5.1.7 and below and as long as the System time scale is still set to UTC, the leap second is only applied if the amount of leap second to be applied is "+1" or "-1".

The erroneous scheduled leap second from version 1.06 receiver firmware is instead setting this to a much higher value than 1, such as +6 or +72 for examples. Even though the leap second is scheduled, this bad data won't result in a leap second correction occurring (unless its erroneously set to a 1). And the receiver is scheduling out the leap second, long after the one scheduled for June 2015. So, it will be cancelled out by the real leap second.

However, if the system is in GPS or TAI timescale with version 5.1.7 or below installed, the leap second will take if scheduled before June 2015. The Jan 2015 release is adding additional protection that the system will only accept a 1 second change no matter what the system timescale is set to.

The leap second scheduled for June 2015 will override/delete any erroneous scheduled leap seconds. Or a user can manually delete with the browser, if they wish.

Per Dave Sohn (8 Jan 15, referring to v5.1.7) Better protections for this are already in place and will be included in the next release (referring to 5.2.0 release in Jan 2015). However, despite the reporting of the leap second, a leap second of greater than one second will not occur if the unit is operating in a UTC timescale, which is the default for SecureSync. Also, a leap second can be removed from the system, if present, by using the delete mechanism from the Edit Leap Second window on the Management - > Time Management page of the browser.

D) (Sept/Oct 2014) GPS goes not valid every other second (if no other references, goes into Holdover every other second)

- Likely (but not confirmed) fixed with the Res-SMT-GG version 1.0.7 firmware update, being made available in the SecureSync version 5.1.7 update (Nov, 2014).
- Emmanuel observed this same issue with an Epsilon clock with a Res-SMT-GG receiver installed.

E) (Nov 2014) Cold reset of SecureSync with RES-SMT-GG results in return to last saved GNSS Receiver Mode

- Refer to Mantis case 2932 <http://10.30.1.21/mantis/view.php?id=2932>
- Summary: A Cold Reset deletes all RAM data and acts like a power cycle of the RES-SMT-GG (or RES-T).

Trimble RES-T (Resolution T) GPS receiver (NetClock, TSync, SecureSync)

- Link to Trimble data sheet: <http://www.trimble.com/timing/resolution-t.aspx>
- Link to Trimble receiver info: <I:\Engineering\GPS RCVRs>

Model/Part Numbers

- Our P/N: MP30-0GPS-002
 - Trimble P/N: 52664-05
-

Res-T software version info

A) Version 1.14 software ???

B) Version 1.17 software

- Refer to: <http://trl.trimble.com/docushare/dsweb/Get/Document-483433/Resolution%20T%20Firmware%20v1.17%20Update%20Procedure%20-%20revB.pdf>

C) Version 1.20 software

- **Added anti-jamming feature**

Email from Paul Myers (Dec 2013) Basically, the 1PPS signal from the RES-T can jump by 1msec during jamming.

Typically jamming interference is detected by lowered signal strength. I was assuming this meant satellites go away. However Trimble said in an email:

The anti-jamming code is suppressing the Timing output if it's potentially disturbed by jamming or other unusual conditions. A typical symptom of jamming are decreasing signal levels, therefore the receiver might assume the presence of jamming in your test scenario.

If Lynn county was seeing decreasing signal levels, it might have triggered the 1ms PPS jump.

Basically, the ANTI-JAM feature will let us coast between jamming events on the 1PPS of the receiver using the receiver's TCXO. Fixes require a minimum of 2 satellites and to reacquire after an outage of 9 minutes 3 or more satellites.

- **Released in April 2010**

Email from Tom Richardson (1/13/12) about our cut-in of v1.20 software

Probably P-47929 was first order with new software. Delivery was 3/2010 thru 7/2010, 100 a month. I believe all but that first order in 2009 is version 1.20. We had an issue with the next order, P-48300, where they shipped us wrong version and we updated here.

GPS Week roll over issue

Q. From Dick Fox to Dave Sohn: Do you know what is meant by GPS week counter roll over problem? Is this a known issue with other GPS receiver? Does the Res-T receiver have this issue?

A. Reply from Dave Sohn (2/21/13 KW) The GPS week rollover issue would be caused as the GPS week counter rolls over back to zero, indicating another GPS epoch. Some receivers may have issues responding to this, causing errant behavior on the year, day of year reported. The receiver we utilize in SecureSync does not have a GPS week rollover sue.

Note about Dave's response above: Dave asked Lisa Perdue to test a Res-T GPS receiver for the week roll over issue, using a GSG Simulator. The testing worked just fine. He did not experience any roll over issues.

****Minimum sensitivity/ Min/Max Signal strengths**

- Res-SMT-GG receiver is much more sensitive to weaker signals than the Res-T receivers
- For power conversion: refer to <http://www.radiomar.net/convDBWen.htm>

Recommended gain at the GPS receiver: 20dB to 30dB gain

Comparison of RES-SMT-GG versus Res-T

Res-SMT-GG receiver sensitivity (and Res-T data sheet for comparison)

	Res-T receiver sensitivity	Res-SMT-GG sensitivity (for side-by-side comparison)	Notes
Acquisition	-136 dBm (-166dBW)	-155 dBm	
Tracking	-141 dBm	-160 dBm	(-130 dBm at the surface of the earth. Need 14 dB gain)

Recommended gain at the GPS receiver: 20 to 30dB gain

Note: GPS signal strength is -130 dBm at surface of the Earth (-160dBW).

Email from Tom Richardson: Sensitivity for the Res-T is -136 dBm, I don't have a max signal spec, this has usually not been the problem. But I know that like any receiver you can give it too much signal and it won't work, I just don't know how much.

The Sensitivity spec for the Trimble Res-T receiver states Acquisition = -136 dBm, Tracking = - 141 dBm. I would subtract about 3 dB for the internal cable so the minimum should be -133 dBm.

The recommended minimum to recommended maximum dB gain (Antenna/GPS preamp dB gains, minus the antenna cable loss) at the input to the GPS receiver is 20 to 30 dB. This can also be stated as the following:

The GPS signal at the surface of the earth is -130dBm. The minimum sensitivity for the GPS receiver in the Model 9300s, 9400s and SecureSync is -136 dBm. There has to be enough antenna gain (and inline GPS amps, if needed) to account for the antenna cable loss, for the signal to be at least -136 dBm. The antenna cable loss for Belden RF400 (RG-8) or Time Microwave LMR-400 cable is about 5.5 dB loss/100 feet of cable.

Reported SNR (Signal Strengths) range for Res-T receivers: 0 to 55

Note: We typically qualify **30** or higher as a good SNR value. According to Paul Myers, it really needs to be above **28** to prevent adverse operation of the GPS receiver.

AMU versus the dB/Hz measurement

The Trimble Res-T receivers can be configured to output the SNRs for each channel in AMUs (a Trimble-specific measurement) or as dB/Hz measurement. As AMU is Trimble-specific and therefore the Motorola receivers are using dB/Hz, we chose to configure the Res-T to also provide SecureSync with dB/Hz, as well (so that the SNRs from both receivers would be comparable to each other).

The SecureSync just reports/displays the raw dB/Hz values that are provided directly from the GPS receiver. SecureSync doesn't scale the reported values.

Maximum recommended input signal, before damage may occur.

- Vendor says +10dBm max into receiver.

Email from Julian Dortort with Trimble

The maximum RF power input you can place on the front end is 10dBm. Obviously we normally expect levels of around -130dBm for satellite signals.

As Jim explained a little earlier there are also limits to the LNA gain in dB that can be placed on the device.

From a purely GPS standpoint, there is no practical maximum. The issue becomes that of handling out-of-band signals (and noise).

You can characterize the required gain as follows:

Minimum gain (dB) = 10 + cable loss + Rx noise figure*

$$\text{Max gain (dB)} = \text{minimum gain} + 10$$

- Refer to [GPS\Trimble Res-T manual\ResolutionT_UG_2B_54655-05-ENG.pdf](#) for Trimble document regarding min and max gain.

Known issues with Res-T GPS Receivers

- E) Res-T receiver dropping to 1 satellite for a short period of time (130 seconds), near UTC midnight on Saturday/Sunday
 - This is a potential issue with all firmware versions of the Res-T receiver (as of at least Nov 2015, SecureSync versions 5.3.1 and below- Res-T firmware versions 1.20 and below)
 - Only fix is to replace the Res-T receiver with a ublox receiver.
 - Doesn't affect "Q=" value. But if the user-defined min threshold is less than 130 seconds, will assert an alarm.

(9/10/12 KW) A few customers (NetClocks and SecureSyncs) with Res-T receivers have periodically reported losses of GPS reception occurring around midnight UTC on Saturday. The latest was Ty Bartels, who noticed the receiver dropping to just one satellite for two hours, on both their NetClock and their SecureSync.

On Sunday at 24:00 GMT when the week rolled over we received holdover alarms on 8 of our SecureSync and 9389 servers. We have this occur on occasion. I wanted to see if there has been any progress to resolve this issue?

Our current code versions are: SecureSync: v4.8 and v4.8.6; 9389: v3.4.5

Sep 2 01:00:02 DC3-SecureSync-NTP-01 spectracom: [system] GPS 0: 1 = 105 7 = 471 8 = 2196 9 = 828 Q = 3600

Sep 2 00:00:02 DC3-SecureSync-NTP-01 spectracom: [system] GPS 0: 1 = 25 8 = 2788 9 = 787 Q = 3600

Sep 1 23:00:02 DC3-SecureSync-NTP-01 spectracom: [system] GPS 0: 6 = 16 7 = 2137 8 = 1417 9 = 30 Q = 3600

Sep 2 02:00:02 ADC-SecureSync-NTP-02 spectracom: [system] GPS 0: 7 = 1730 8 = 1127 9 = 743 Q = 3600

Sep 2 01:00:02 ADC-SecureSync-NTP-02 spectracom: [system] GPS 0: 1 = 105 6 = 586 7 = 1218 8 = 1614 9 = 77 Q = 3600

Sep 2 00:00:02 ADC-SecureSync-NTP-02 spectracom: [system] GPS 0: 1 = 25 7 = 113 8 = 2755 9 = 707 Q = 3600

Sep 1 23:00:02 ADC-SecureSync-NTP-02 spectracom: [system] GPS 0: 5 = 17 6 = 397 7 = 2195 8 = 991 Q = 3600

Paul Myers had also been working earlier with Trimble on this condition. He noticed this issue happening on only some of our time servers (with versions 4.8.5, 4.8.6 and 4.8.7 installed). He mentioned that none of our receivers are using the latest Trimble release. But the receivers with our latest version of their software installed did not show this issue happening. He only noticed it with our units running an even earlier version of their firmware. The screenshot below was from a SecureSync that was showing the loss of GPS occurred this past Saturday/Sunday.


```

Spectracom NetClock 9483 Version 4.8.5
[spadmin@SalesDemo2 ~]$
[spadmin@SalesDemo2 ~]$
[spadmin@SalesDemo2 ~]$ version
Software      4.8.5
Timing System 2.8.5
[spadmin@SalesDemo2 ~]$ version gps
Mfr/Mdl: Trimble Resolution T

GR (0) Rcv Info (66 bytes):
-----
Serial #: 2048 41811084
Date:    10/28/2010
-----
Appl Ver: 1.20
Date:    4/21/2010
-----
Core Ver: 1.26
Date:    4/21/2010
-----

```

Example Email Keith sent to John Abdelsater, 30 Nov 15. I suspect the temporary loss of greater than four satellites occurred near midnight UTC time (on the UTC transition from Saturday to Sunday) for a very short period of time (130 seconds). This can be easily confirmed via either the SecureSync's Alarms log and/or the GPS Qualification log.

If you would like us to confirm for you that this condition only occurred at about UTC midnight, please send us the logs and we will be happy to review them for you. Here is info on capturing the logs as a single bundled file:

All of the SecureSync's logs (including those shown in the browser and also those in the background) can be easily bundled into one file and then exported from the SecureSync to send as an attachment.

Instead of copy/pasting all of the log entries into a Word document, starting in Archive software update version 5.1.2, the logs can be easily saved to single bundled file and exported into a networked PC. Earlier versions of software allowed the bundle to be created, but then the file still needed to be transferred out using an FTP/SCP connection. Now, a button in the web browser alleviates the need to create an FTP session to transfer this file out to a PC.

The log bundling and export to a PC is controlled in the **"Management"** -> **"Log Configuration"** page of the SecureSync's web browser. On the left-side of the browser, click on the **"Save and download all logs"** button. You can then select where to save the log bundle to. The default file name is "securesync.log".

Note this log bundle file can be rather large. If it's too large for you to email it to us, or if you prefer, please feel free to upload the file to the following sharefile site: <https://spectracom.sharefile.com/filedrop>. After entering your contact info, you will be taken to a new screen. Please select my name (**"Keith Wing"**) from the **"Send to"** dropdown, drag/drop the log bundle file into the empty field and then press **"Upload Files"**.

For your information, SecureSyncs with a Res-T GPS receiver installed can periodically observe a 130 second period of typically tracking 1 satellite, during the new GPS week rollover (which occurs Saturday at UTC midnight, rolling over into Sunday), if the GPS Wing has made any changes to the GPS signal. This seldom-observed temporary loss of greater than four satellites is a factor of the GPS receiver itself and of the changes incorporated into the GPS signal being transmitted by the constellation of the GPS satellites. The symptoms of the receiver being temporarily affected by the signal changes incorporated are the receiver tracking less than four satellites (typically only one satellite) for 130 seconds. As the GPS receiver continues tracking at least one satellite during this new week transition, this seldom observed anomaly does not affect the minimum system requirements that the GPS receiver needs to track at least one satellite at all times to prevent the SecureSync from going into Holdover mode. So the only effect on the SecureSync during this new week rollover transition is the user-defined min satellites alarm will be asserted if this available/optional alarm has been enabled by a user, and if the user has specified a "minimum threshold" of less than 130 seconds for the alarm to be asserted (or the user hasn't specified any threshold, so the threshold is set to "0").

If a user has enabled the available "User-defined Min satellites" alarm (which is disabled by factory default), the fix to this potential and rarely observed anomaly is to set the min threshold to a minimum of 130 seconds. The threshold for the Min Satellites alarm is configured in the **Management** -> **Notifications** page of the browser, at the bottom of the **GPS** tab. As shown below, if the Minimum Satellites for the Minor and/or Major alarms has been configured, the corresponding threshold should be set to a value such as 135 seconds for example

Minor Alarm Threshold	
Minimum Satellites	Duration Below Threshold (s)
4	135

Major Alarm Threshold	
Minimum Satellites	Duration Below Threshold (s)
4	135

Timing accuracy (to UTC)

- Extremely accurate 1-PPS output, synchronized to GPS or UTC within 15 ns (one sigma).
- **Per the Trimble Res-SMT-GG user manual:** “A position error of **100 meters** corresponds to a time error of **approximately 333 ns**”

RES-T GPS position (latitude/longitude/antenna height) update interval

- The Res-T receiver updates the GPS position at a 1 Hz rate (once-per-second).

Note: This value is not configurable.

Speed and Altitude limitations

- As far as speed (and altitude) limitations for the Res-T receiver (these are common limitations across all commercial GPS receivers due to export controls).
 - **Altitude** 18,000
 - **Velocity** 515 m/s

Note: Either limit may be exceeded, but not both!

Acquisition time

Per the Resolution T datasheet (http://www.ko4bb.com/Manuals/05%29_GPS_Timing/Trimble/Trimble_Resolution-T/13441+Resolution+FA2.pdf) , the typical acquisition/reacquisition times (and the percentage of times it will occur in this amount of time) are below:

Reacquisition: <2 sec. (90%)

Hot Start: <14 sec (50%), <18 sec (90%)

Warm Start: <41 sec (50%), <45 sec (90%)

Cold Start: <46 sec (50%), <50 sec (90%)

Note that this is not the same as the amount of time it takes after each power-up for the NTP servers to declare sync to GPS. With the default Stationary mode, the GPS survey has to first be completed once. This takes 34 minutes, after its tracking at least four satellites. In mobile mode, the very first time after shipment that its connected to GPS, the receiver needs to obtain the GPS to UTC offset from GPS, before it can sync. This can take up to 12.5 minutes after tracking one satellite. While in mobile mode, any subsequent reboot requires the receiver to be tracking at least four satellites and have a 3D fix before Sync is declared. This takes about 2 minutes or so after power-up.

NTP can't start to go into sync until GPS sync has occurred. Once Sync has occurred, NTP starts its alignment to the System Time (which is synced by GPS). In the newer versions of software for the Model 9300s, 9400s and SecureSync, this NTP sync time has been significantly reduced from around 14 minutes or so after GPS sync, down to about 3 minutes, after GPS Sync. NTP sync is when the Stratum level switches from Stratum 16 to Stratum 1.

Total time for NTP to be available for synchronization in a mobile environment is around 5-6 minutes or so (it is not a defined value and may vary a bit from one start-up to another).

Resolution-T GPS receiver RAM and Flash memory storage

Refer to: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Memory\SecureSync memory.pdf> (discusses receiver operation specific to SecureSync).

According to the Trimble, there used to be a combined total of 32MB of both RAM and Flash on the GPS receivers, via a single IC. This configuration was changed back around Feb 2008 to now being 32MB SRAM on one IC and 4MB flash on a second IC".

Positional accuracies of the Res-T receiver (DOP/PDOP/TDOP, herr, verr)

Note: For more info on DOP (Dilution of Position), refer to either: <http://www.developerfusion.com/article/4652/writing-your-own-gps-applications-part-2/2/> or <http://gauss.gge.unb.ca/papers.pdf/gpsworld.may99.pdf>.

The Resolution-T GPS receiver returns the DOP values differently depending on mode of operation.

In Stationary Mode the Survey operates and the Fix dimension is 3D-FIX for 2000 seconds. During this time the DOPs TDOP, PDOP, HDOP and VDOP are returned. At the end of the survey when the position is known and fixed, the TDOP is returned as 1.0 and other values as 0.

In Mobile mode the DOPs continuously change reflecting accuracy.

I am assuming your customer is in Mobile Mode, hence the DOP values.

I questioned Jim Early about this because I wanted to understand how DOPs and error can be related using the Resolution-T. The manual did NOT provide me a clear indication of how.

Jim Early provided the following relating to accuracy of the solution.

A Trimble table of 'error versus PDOP or TDOP' is not generally available.

PDOP of 12 corresponds to 250-300 meters of error

For every meter of position error there is 3.3 to 3.5 nsec of time error

The intrinsic accuracy of the Resolution-T is 2-5 meters. (Assuming with Selective Availability off)

Operation in 2D/3D Automatic modes is typically less than 200nsec of error.

In Stationary mode a survey of 60 seconds can result in less than 10 meters of error. 5-7 meters of error typical. (I think this assumes good sky view and good constellation geometry.)

Survey Duration of 600 seconds has been used successfully and was recommended to Trimble Customers.

2000 second surveys are the default ONLY because of fear that selective availability will be restored. The 600 second survey cannot overcome Selective Availability.

FAQs

Q. Our code that works with other GPS hardware stores uncertainty values that the user may want to examine to determine the quality of his position and time data. The figures we are getting from another vendor's equipment use one of the two "standard" ways of reporting GPS uncertainties and their system reports eph, epv, and ept figures. Unfortunately Spectracom uses the other standard which reports pdop, hdop, vdop, and tdop figures. When I

looked at the manuals and saw that the TSYNC_FixDataObj structure that your TSYNC_GR_getFixData returns herr and verr values, these names sounded like what I wanted for two of my displayed valuea. Unfortunately as the print out below of two returns from TSYNC_GR_getFixData indiactes both herr and ver are zero. Searching the web I did find some equations to convert between the two standards but unfortunately they require that fdom and tdom values and they are also left zero in your returned structure. Is there anything that I can do to get you board to start returning these values that are left zero? If not will these four zero values be returned in some future version of the firmware/driver? My last questions deals with the return structure's tdom value which seems too large if it is in seconds so are the units meters? If it is seconds then the number slightly too good. If it isn't meters then what are the units?

A. To begin, The Tsyncl-PCle timing boards use a Trimble Resolution-T GPS receiver. The manufacturer of the GPS receiver (Trimble) does not provide any tables of “positional error” versus the reported PDOP or TDOP values. However, in correspondence with Trimble, they have indicated that a PDOP value of 12 corresponds to 250-300 meters of positional error. They have also indicated the intrinsic accuracy of this GPS timing receiver is 2 to 5 meters (under ideal conditions of very low PDOP values and when Selective Availability is turned off in the GPS constellation, as it is currently).

Trimble does not define the errors for the PDOP values below 12, so we can only provide you with these two “outside boundary” error values for PDOP. We tried finding the means to convert all PDOP values to an estimated error value, in order to then covert again to the desired herr and verr values, but we weren't able to find any method to directly convert these values (it's like comparing apples to oranges).

Below is a general classification of the DOP values that may help:
Meaning of DOP Values

DOP Value	Rating	Description
1	Ideal	This is the highest possible confidence level to be used for applications demanding the highest possible precision at all times.
1-2	Excellent	At this confidence level, positional measurements are considered accurate enough to meet all but the most sensitive applications.
2-5	Good	Represents a level that marks the minimum appropriate for making business decisions. Positional measurements could be used to make reliable in-route navigation suggestions to the user.
5-10	Moderate	Positional measurements could be used for calculations, but the fix quality could still be improved. A more open view of the sky is recommended.
10-20	Fair	Represents a low confidence level. Positional measurements should be discarded or used only to indicate a very rough estimate of the current location.
>20	Poor	At this level, measurements are inaccurate by as much as 300 meters with a 6 meter accurate device (50 DOP × 6 meters) and should be discarded.

We did find one website that discusses DOP (Dilution of Precision) in great detail. The information provided at this site may help allow you to be able to make these conversions, if you are interested in pursuing these conversions. The website address is: <http://gauss.gge.unb.ca/papers.pdf/gpsworld.may99.pdf>.

****Mobile/Stationary/Single Satellite modes with a Resolution-T receiver**

- Choices for Receiver Mode in SecureSync are: “1 Satellite”, “Standard” and “Mobile”
- Choices for Receiver Mode in TSync-PCle are: “Single Satellite mode”, “Standard mode” (stationary), and “Continuous” (mobile) mode. Other modes exist but are seldom used.
- Choices for Dynamics codes are (TSync and SecureSync): “Land”, “Sea”, “Air” and “Stationary”.

A) Standard Mode

- Classic Interface browser: **System -> Set System Mode** page of the browser

Other notes

- “Stationary” dynamics code is automatically selected with the “Standard” mode selection, once the GPS survey has completed.
- The Dynamics code should be set to “Stationary” when in Standard (stationary) mode (the Factory default settings are “**Standard**” mode and “**Land**” dynamics code- until a GPS survey has been completed).
- Once the GPS survey has been completed, the Dynamics mode switches from “Land” to “Stationary”.
- In Standard mode, the GPS receiver requires four satellites at all times, even after GPS survey has been completed.

GPS Survey

- F) GPS Survey takes 2000 seconds (33.5 minutes) to complete, once the GPS receiver is tracking at least four satellites.
- G) GPS survey is not performed while the GPS receiver is in “mobile” (“Continuous”) mode.
- H) GPS survey only performed first time in new location, while in stationary mode. If the equipment is relocated, the survey is performed again, at the new location.
- I) Once a GPS survey has been completed and the SecureSync or TSynC-PCIe board is subsequently power cycled, the survey percent complete will remain at 0 % (Being 0% doesn't necessarily mean that the product is in mobile mode). Also, the dynamics code will switch from the default value of “Land” to “Stationary”

Note: Once the dynamics code is set to “**Stationary**”, it will remain this value, even after a power cycle.

B) Mobile Mode

- Mobile mode is selected with the “Continuous” mode selection (TSynC-PCIe) or “Mobile” mode selection (SecureSync).
- The Dynamics code choices available for “Continuous” (mobile) mode (both TSynC and SecureSync) are “Land”, “Sea” and “Air”.
- The GPS survey is not performed while in the Continuous” (mobile) mode.
- Trimble Res-T manual- statement about Mobile mode:

http://trl.trimble.com/dscgi/ds.py/Get/File-221342/ResolutionT_UG_2B_54655-05-ENG.pdf

See Page 38 for statement that PPS Output pulse will be degraded by a factor of 3 when unit is operated in a mobile application.

Time it takes to sync in mobile mode

The GPS receiver needs to be tracking at least 4 satellites and first be able to read the UT1 correction factor in the 12.5 minute looping GPS ephemeris data.

The GPS signal consists of 15 main frames that are 30 seconds long, each, resulting in a 12.5 minute message. It has to read the looping UT1 correction bit, before sync can be achieved.

FAQs

- Same old question: do you have the benchmark of the time accuracy for the mobile mode? How much less compared to the Stationary mode? I would like to have the clear number from the MFG for answering the project's related question.

From Trimble Res-T manual: http://trl.trimble.com/dscgi/ds.py/Get/File-221342/ResolutionT_UG_2B_54655-05-ENG.pdf (especially the second paragraph).

Timing receiver performance

The Resolution T GPS timing receiver is a complete 12-channel, parallel tracking, GPS receiver, designed to operate with the L1 frequency, Standard Position Service, Coarse Acquisition code. The receiver is designed in a single board format, specially adapted for timing applications where reliability, performance, and ease of integration are desired. The receiver features Trimble's improved signal processing code, a high-gain RF section for compatibility with standard active gain GPS antennas, and a CMOS level pulse-per-second (PPS) output for timing and synchronization applications.

Timing applications are assumed to be static. The special timing software used with the Resolution T receiver configures the unit into an automatic self survey mode at start up. The receiver will average position fixes for a specified time (one per second) and at the end of this period will save this reference location. At this time the receiver will go into an Overdetermined Clock mode and no longer solve for position but only for clock error and clock bias using all of the available satellites. This provides an accuracy of less than 15ns (1 Sigma) for the 1PPS output.

How to measure the difference between stationary and mobile modes:

Regarding the accuracy testing of stationary versus mobile modes, I spoke to a couple of our engineers about this. My initial thought was to use NTP running on a PC and to then use the NTP peers command to compare the SecureSync to another NTP server on the network. The engineers informed me that this test wasn't a good test. The accuracy differences between the two modes of the GPS receiver operation are too small for NTP to even notice. The accuracy difference between the two modes is just "noise" to NTP. You won't be able to detect any differences between the two modes, in respect to NTP.

In order to measure the differences for the two modes, the best test is to use a very accurate frequency counter (that is externally locked to another frequency reference to provide the most accuracy for the counter) and compare the 1PPS output from the back of SecureSync to a 1PPS from another very stable reference (such as another Rubidium-based frequency reference). Then, repeat the same test with the GPS receiver configured for the other mode (the first test performed while in stationary mode. Then, switch to mobile mode and compare the 1PPS output to the same 1PPS reference as the first test). The difference between the two measurements is the effect that the mode change has on the system 1PPS.

We suspect that you will see very little, if any, difference on the 1PPS by just switching to the mobile mode, while the SecureSync is stationary. The largest effect on this testing will be with the SecureSync actually being placed into motion, compared to the receiver being stationary, (even while stationary with it being configured for mobile mode). This will be the "worst-case scenario", resulting in the largest amount of difference.

The specification of the GPS receiver is that its 1PPS output will be degraded by a factor of 3 when the GPS receiver is operated in a mobile application. The accuracy spec in a stationary environment is +/- 15ns (1 Sigma) of UTC. So, in a mobile mode, the spec would become +/- 45ns (1 Sigma) of UTC. Since NTP accuracy is measured in milliseconds and not nanoseconds, you can see why the 1PPS accuracy degradation in mobile mode won't have any noticeable effect on NTP.

Email from Paul Myers

Mobile Mode versus Stationary mode

2 SecureSync's one in each mode.

Compare 1PPS from each using a counter.

- When Stationary both should be very accurate.
- When moving the mobile mode should be 3x worse per spec above

To compare mobile mode to a reference could they try disciplining a Rb and putting a SecureSync in holdover then using a RES-T SecureSync to compare the Rb 1PPS in holdover to 1PPS output of SecureSync in mobile mode while moving.

- Is the time required for the GPS survey in Stationary mode staying the same as the NetClock (35 minutes) for the SecureSync when position is moved?
- SecureSync will require the same survey time in stationary mode as NetClock.

C) Single Satellite mode

Important Note: Time accuracies CANNOT be guaranteed in Single Satellite mode. For accurate timing, we recommend using Standard mode- not Single Satellite mode.

Earlier version-Requires at least one QUALIFIED satellite and valid position information (either by completing a GPS survey or manually entering the correct position).

Note: Starting in SecureSync v4.5.0 (~5/1/11, and likely to also include TSync), Paul Myers is changing the operation of single sat mode to be true Res-T single sat mode. A Min of four sats will initially be required for a short period of time (doesn't have to do a survey, but has to get a 3D fix). Then, the min drops to just one sat.

With the changes incorporated in v4.5.0 (per the note above), a GPS survey/"Position Hold" does not apply to Single Satellite mode (only standard mode).

Each time the SecureSync powers-up in Single Sat mode, the GPS receiver needs at least four satellites to calculate position, or the position needs to be hand-set.

As the UTC offset is obtained and stored the first time the Ephemeris data is downloaded (no matter which GPS mode is selected) the SecureSync does not have to wait to download the ephemeris data to receive the UTC correction value each time it boots up. It just needs the 3D fix and then a short period of time to stabilize the PPS. Then it can declare sync.

Testing is showing SecureSync back in sync within just a couple of minutes of each power cycle:

Number of satellites used in fix while in Single Sat mode:

As shown in the screenshot below ("Number of tracked satellites" field), only one satellite is used for the fix, even if it's tracking more than one satellite.

GPS INPUT STATUS

Manufacturer/Model	Trimble Resolution T
1PPS Validity	OK
Time Validity	OK
Receiver Mode	1 Satellite
Dynamic Mode	Stationary
GPS Longitude	077° 35' 20.674" W
GPS Latitude	043° 04' 59.257" N
GPS Altitude	169.918 m
Survey Prog	Complete
Number of Tracked Satellites	1
Offset	0 nsec
Antenna Sense	OK

ID	2	4	5	10	12	13	25	29	26	0	0	0
SNR	44	42	44	43	42	39	41	39	39	0	0	0

Anti-jamming for both Trimble RES-T and RES-SMT-GG receivers

Email from Paul Myers 9 Dec 2013)

I spent some time testing the RES-T and GG using the GPS simulator trying to test noise conditions to see what I could learn.

Both appeared to work as Trimble explained they would and confirmed the answers I received from Trimble.

Trimble responded to my earlier questions that they recommend Anti-Jam feature to be turned on.

I can share their responses, but basically they can experience up to a 1 msec jump if they experience interference/jamming. Their fix makes it robust in their eyes by making their system require 2 satellites to sync, 3 satellites to recover at startup or after an extended outage of > 9 minutes and also by implementing a sort of holdover mode where the RES-T 1PPS is locked on the last DAC setting and frequency adjustments are NOT made and the 1PPS coasts until tracking is restored when reception improves.

This means that our current design could see a 1PPS jump and we will use it as valid input if the 'other' data provided to us looks valid. In MOST cases I believe we would see the RES-T stop tracking and we enter holdover because the RES-T does NOT do fixes and we do NOT sync and go into holdover when NO-FIXES are reported.

However, I know that this is not always the case. The 130 second GPS End-of-week outages we saw in many cases do NOT result in holdover. And in a very few of my test cases I saw 1 satellite and doing fixes so we did NOT enter holdover. IF a PPS jump occurred then we would feed that to the system.

However, our fix of allowing users to select the # of satellites would cause us to enter holdover if the number of satellites drops to 1 so no PPS jump would be affected.

To support my testing I made some firmware changes. And because it turned out not to be hard I ended up making a few 93xx changes to allow me to test Anti-Jam and improve Rb behavior.

Allowed user to select Number of satellites required to sync ranging from 1-6

Allowed user to enable/disable Anti-Jam feature (Only for Res-T version 1.20 and greater)

Change Rb code to save correction after 3.5 hours (12600 seconds) of continuous operation if loss of sync occurs, otherwise it still performs saving of correction every 24 hours.

Modified Rb code to match monitoring behavior of SecureSync – We found some minor numerical monitor value errors.

I built a 3.6.3 candidate and loaded on a 9383 Rb unit and ran it over the weekend. No issues.

This release could be re-built for an actual release. All that is needed is to update the release date, change the security settings to prohibit login, and rebuild AND make an update bundle and test. If Harris needs a release to placate them for 93xx we have one that allows for operation using the Anti-Jam feature and the shorter RB correction save operation. Which is more likely desired. The Anti-Jam in David Sohn's opinion might reduce sensitivity, Trimble did not respond to my concerns about this, just saying, Anti-Jam was recommended for more stable operation. They said "Using the anti-jamming mode ensures we are using our strictest method to use good SV data."

Modes of operation:

What I believe will happen based on my testing is described below.

Min # Sats	Anti-Jam	Sync Behavior	Assumed 1PPS behavior (Not observed)
>=1	OFF	Remains in Sync GPS End of Week issue	PPS could jump
>=1	ON	Remains in Sync GPS End of Week issue	PPS Coasts on RES-T TCXO if interference/jamming detected by RES-T
>=2	Off	Enters holdover for GPS end of week issue (1-sat) or if number of satellites =1	PPS Could jump if jamming/interference affects system before Number of satellites falls to 1
>=N	Off	Enters holdover for GPS end of week issue (1-sat) or if number of satellites < N	PPS Could jump if jamming/interference affects system before Number of satellites falls to below N-1
>=N	ON	Enters holdover for GPS end of week issue (1-sat) or if number of satellites < N	PPS Coasts on RES-T TCXO if interference/jamming detected by RES-T
>=2	ON	Enters holdover for GPS end of week issue (1-sat) or if number of satellites =1	PPS Could jump if jamming/interference affects system before Number of satellites falls to 1

The RES-SMT-GG seems to have ported the RES-T anti-jam behavior. It does have greater sensitivity and tolerates more abuse than the RES-T. However, jamming can impact it.

Our options for the RES-SMT-GG are:

- Do nothing – we can tolerate more noise, but no guidance on impact to 1PPS. (I assume the PPS does not jump like the RES-T...)
- Enable Anti-Jam – which requires 2 satellites minimum to sync and 3 to recover. Identical behavior to RES-T

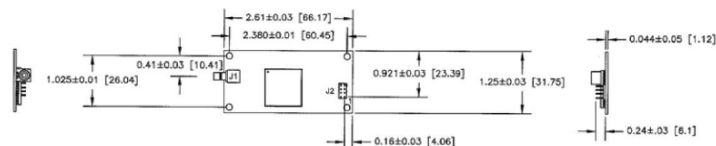
- Allow users again to select minimum number of satellites (TBD)
- Enable GPS+GLONASS – Enabling GLONASS allows both GPS and GLONASS to be used. If GPS signal levels or noise at the GPS carrier is introduced GLONASS continued without issue. Likewise if GLONASS signal levels were manipulated or distorted and (I didn't test, but assume) if GLONASS carriers were used as noise, GPS would not be impacted.
- We could consider using dual GPS/GLONASS operation assuming if one is jammed the other would still work.
- Testing with GPS interference or impacted signal levels demonstrated GLONASS only operation.

** Naelcom-RSMT receiver (Original Skylight phase 1 receiver)

- Trimble Res-SMT (not the RES-SMT-GG) GPS receiver sold by Naelcom
- **Our P/N:** MR30R-0GPS-0006
- Refer to: <I:\Engineering\Engineering Shared\Spectracom Parts ROHS\MPxxR-xxxx-xxxx\MP30R-xxxx-xxxx>
- Used in the original Skylight SecureSyncs (phase 1 with 4.7L software)

DC0116-R02

NLC-RSMT TECHNICAL DATA	
PERFORMANCE SPECIFICATIONS	
Sensitivity:	Tracking: -160 dBm Acquisition: -155 dBm (with A-GPS)
ENVIRONMENTAL SPECIFICATIONS	
Operating temp:	-40°C to +85°C
Vibration :	0.008 g ² /Hz..... 5Hz to 20Hz 0.05 g ² /Hz.....20Hz to 100Hz -3dB/octave..... 100Hz to 900Hz
Operating Humidity:	5% to 95% R.H. non-condensing, @ +60°C
ELECTRICAL CHARACTERISTICS	
Prime power:	+3.0VDC to 3.6VDC Power consumption: 100mA @3.3V
Ripple Noise:	Max 50 mV, peak-to-peak from 1 Hz to 1 MHz
INTERFACE CHARACTERISTICS	
Connections:	I/O: 8-pin (2x4) 2 mm Male Header RF: Right-angle SMB
Serial ports:	2 serial ports
PPS/Even second:	CMOS-compatible, TTL-level pulse, once per second
Supported Protocols:	TSIP, NMEA 0183 Bi-directional NMEA messages Messages selectable by NMEA commands Selection stored in flash memory
PHYSICAL CHARACTERISTICS	



**** Trimble Force 22E SAASM receivers (Model 9300s and SecureSyncs)**

- Link to Trimble receiver info: I:\Engineering\GPS RCVRs
- Link to unclassified SAASM documents: I:\Engineering\GPS RCVRs\SAASM-UnclassifiedDocs
- Link to controlled SAASM documents: [U:\Engineering](#)

Primary support for SAASM (Force 22/22E) GPS receivers:

Bruce Swearingen
System/Application Engineer
Military Technical Support
bruce_swearingen@trimble.com
408 481 7568

- **MFG:** Trimble
- Trimble P/N: 41205-U12E
- **Our P/N** MP30-0GPS-0003

Firmware upgrade for the Trimble Force 22E SAASM receivers

- Version 0612 update made available due to change to the signal.
- Link to the information about this firmware upgrade: [U:\Engineering\SAASM-FOUO\CustomerService\NetClock Trimble Force22E 0612 Upgrade](#)

Receiver mode

Per Paul Myers: Mobile (CONTINUOUS) mode is recommended.

****GB-GRAM (GBGRAM/GB Gram): SAASM GPS receiver**

Note: The GB-GRAM receiver is also called **MPE-S** receiver

- **Link to MFG data:** <I:\Engineering\GPS RCVRs\Rockwell>
- **Link to unclassified SAASM documents:** <I:\Engineering\GPS RCVRs\SAASM-UnclassifiedDocs>
- **Link to controlled SAASM documents:** <U:\Engineering>
- **Receiver Manufacturer:** Rockwell Collins
- GB-GRAM Stands for “Ground-Based GPS Receiver Application Module”.
- Designed as a low cost SAASM GPS receiver for ground-based (ARMY) applications.

MFG: Rockwell Collins

A) New half size receiver

- **Mfg P/N:** 987-9705-001
- **Our P/N:** MP30-0GPS-0007

B) Earlier full size receiver

- **Mfg P/N:** 987-9705-001
- **Our P/N:** MP30-0GPS-0004

GPS Receiver mode

Per Paul Myers: Mobile (CONTINUOUS) mode is recommended.

Motorola receivers

Motorola Oncore M12 GPS receiver

Antenna Sense circuit: 5 to 80 ma current limit for antenna +5vdc circuit.

Oncore GPS Receiver Accuracy and NAD output

GPS receiver sends time out as NAD 083 Format.

Position accuracy (From Synergy datasheet) on UT, GT and M12

100 m 2dRMS with SA as per DOD

Less than 25mSEP without SA.

SNR (Signal Strengths) for M12 receivers: 0 to 55

Link to GPS receivers: <I:\Engineering\GPS RCVRs>

Motorola VP/GT/UT receivers

GT receivers

- Refer to GPS receivers in the Model 8183 section of this document [GPS receivers](#)

UT receivers

- **UT Plus Part Number:** 064052
- **P/N annotated on the GPS receiver IC:** R5122U1115



UT receiver accuracy/Specs

(From: <I:\Engineering\Engineering Shared\Spectracom parts\064052>)

UT Plus Oncore™ GPS Receiver

Receiver Architecture	<ul style="list-style-type: none"> • 8 parallel channel • L1 1575.42 MHz • C/A code (1.023 MHz chip rate) • Code plus carrier tracking (carrier aided tracking)
Tracking Capability	<ul style="list-style-type: none"> • 8 simultaneous satellite vehicles
Dynamics	<ul style="list-style-type: none"> • Velocity: 1000 knots (515 m/s); > 1000 knots at altitudes < 60,000 ft. • Acceleration: 4 g • Jerk: 5 m/s³ • Vibration: 7.7G per Military Standard 810E
Acquisition Time (Time To First Fix, TTFF) (Tested at -30 to +85°C)	<ul style="list-style-type: none"> • < 15 s typical TTFF-hot (with current almanac, position, time and ephemeris) • < 45 s typical TTFF-warm (with current almanac, position and time) • < 90 s typical TTFF-cold • < 1.0 s internal reacquisition (typical)
Positioning Accuracy	<ul style="list-style-type: none"> • 100 m 2dRMS with SA as per DoD specification • Less than 25 m SEP without SA
Timing Accuracy (1 Pulse Per Second, 1 PPS)	<ul style="list-style-type: none"> • Time RAIM algorithm • 130 ns observed (1 sigma) with SA on • In position hold mode, < 50 ns observed (1 sigma) with SA on
Antenna	<ul style="list-style-type: none"> • Active micro strip patch antenna module • Powered by receiver module (5-80 mA @ 5 Vdc)
Datum	<ul style="list-style-type: none"> • WGS-84
Output Messages	<ul style="list-style-type: none"> • Latitude, longitude, height, velocity, heading, time (Motorola binary protocol) • Software selectable output rate (continuous or poll) • TTL interface
Power Requirements	<ul style="list-style-type: none"> • 5 ± 0.25 Vdc; 50 mVp-p ripple (max.)
"Keep-Alive" BATT Power	<ul style="list-style-type: none"> • External 2.5 V to 5.25 V; 15 µA (typ.) 60 µA (max.)
Power Consumption	<ul style="list-style-type: none"> • < 0.9 W @ 5 V with active antenna
Dimensions	<ul style="list-style-type: none"> • Receiver: 2.00 x 3.25 x 0.64 in. [50.8 x 82.6 x 16.3 mm]
Weight	<ul style="list-style-type: none"> • Receiver: 1.8 oz. (51 g)
Connectors	<ul style="list-style-type: none"> • Data/power: 10 pin (2x5) unshrouded header on 0.100 in. centers • RF: right angle OSX (subminiature snap-on)
Antenna to Receiver Interconnection	<ul style="list-style-type: none"> • Single coaxial cable • Antenna sense circuit
Operating Temperature	<ul style="list-style-type: none"> • Receiver module: -40°C to +85°C
Humidity	<ul style="list-style-type: none"> • 95% noncondensing +30°C to +60°C
Altitude	<ul style="list-style-type: none"> • 60,000 ft. (18 km) (max.) • > 60,000 ft. (18 km) for velocities < 1000 knots
Standard Features	<ul style="list-style-type: none"> • Time RAIM • Automatic site survey mode • Jamming protection
Optional Features	<ul style="list-style-type: none"> • Lithium battery • Straight OSX RF connector

SNR (Signal Strengths) for VP receivers: 0 to 255

SNR (Signal Strengths) for GT/UT receivers: 0 to 55

ONCORE TECHNICAL APPLICATION NOTE
Oncore Model Number and Feature Cross-Reference

Product	Part Number	Battery Option	Second Serial Port	Differential GPS (RTCM SC-104 & Mot binary)	1 Pulse Per Second (1PPS)	1PPS Accuracy (ns)	Low Noise Amplifier (supports passive antenna)	Raw Satellite Data	High Jamming Immunity	Low Profile Shields	Right Angle OSX Connector	Straight OSX Connector	Right Angle SMB Connector	Straight 10-pin Connector	Right Angle 10-pin Connector
SL Oncore 2.01 firmware	R6111G1111	*	*	*	< 500						*				*
	R6111G1141	*	*	*	< 500							*			*
	R6111G1171	*	*	*	< 500							*	*		
GT Plus Oncore 2.01 firmware	R3111G1111	*	*	*	< 500						*				*
	R3211G1111	*	*	*	< 500						*				*
	R3111G1141	*	*	*	< 500							*			
	R4112G1111	*	*	*	< 500	*						*			*
	R4212G1111	*	*	*	< 500	*						*			*
	R4112G1171	*	*	*	< 500	*						*	*		*
UT Plus Oncore 2.2 firmware	R5122U1112			*	< 50			*	*	*				*	
	R5222U1112	*		*	< 50			*	*	*				*	
	R5122U1152			*	< 50			*			*	*		*	
VP Oncore 10.0 firmware	B8121B1116		*								*			*	
	B8221B1116	*	*								*			*	
	B8121Z1116		*	*	< 50		*				*			*	
	B8221Z1116	*	*	*	< 50		*				*			*	
	B8121Z1156		*	*	< 50		*				*	*		*	

PRODUCTS

Diff programs (such as WinMerge or KDiff) to compare files

Instead of side-by-side, line-by-line comparing a customer's file to one of our files, use a third part "diff" program for Windows (such as either [WinMerge](http://winmerge.org/) or [KDiff](http://kdiff3.sourceforge.net/)) to compare their file to a default config file. It will show all of the config changes that have been made.

WinMerge: <http://winmerge.org/> (click "Download Now" to obtain this free program)

KDiff: <http://kdiff3.sourceforge.net/>

RoHS Directive (Restriction of Hazardous Substances)

➤ Refer to: www.rohsguide.com

What is RoHS?

RoHS stands for **Restriction of Hazardous Substances**. RoHS, also known as Directive 2002/95/EC, originated in the European Union and restricts the use of specific hazardous materials found in electrical and electronic products (known as EEE). All applicable products in the EU market after **July 1, 2006** must pass RoHS compliance.

What are the restricted materials mandated under RoHS?

The substances banned under RoHS are lead (Pb), mercury (Hg), cadmium (Cd), hexavalent chromium (CrVI), polybrominated biphenyls (PBB), polybrominated diphenyl ethers (PBDE), and four different phthalates (DEHP, BBP, DBP, DIBP).

RoHS 1, RoHS 2 vs RoHS 3

RoHS 1 required that any product in scope should not contain any of the 6 restricted substances and that the company (manufacturer, importer, or distributor) placing the product on the EU market should maintain records to show compliance. **RoHS 2** requires additional compliance recordkeeping from everyone in the supply chain. Additional compliance recordkeeping (which must be kept for 10 years) can include a conformity assessment, CE marking, maintenance of compliance throughout production, and self reporting of non-compliance.

RoHS 2 is also a CE-marking directive, with RoHS compliance now being required for CE marking of products. As such, all manufacturers of electrical/electronic products must comply with RoHS 2 before the CE mark can be applied on their products. *The original green RoHS label with the checkmark is no longer required or used as the CE mark now includes RoHS compliance.*

[RoHS 2 vs RoHS 3 \(EU 2015/863\)](https://www.rohsguide.com/rohs3.htm)

➤ Refer to: <https://www.rohsguide.com/rohs3.htm>

Guide to RoHS 3 Compliance: Regulations, Exemptions, Certification, Initiatives. RoHS 3 (EU 2015/863) RoHS 3 (EU Directive 2015/863) adds Category 11 (catch-all) products and adds four new restricted substances - all phthalates.

www.rohsguide.com

RoHS 3 (EU Directive 2015/863) adds **Category 11** (catch-all) products and adds four new restricted substances - all phthalates. The four phthalates are mainly used as insulation plasticizers, and are on the REACH list of SVHC (Substances of Very High Concern). The expanded list for RoHS 3 is thus as follows:

- Cadmium (0.01 %)
- Lead (0.1 %)
- Mercury (0.1 %)
- Hexavalent chromium (0.1 %)
- Polybrominated biphenyls (PBB) (0.1 %)
- Polybrominated diphenyl ethers (PBDE) (0.1 %)
- Bis(2-ethylhexyl) phthalate (DEHP) (0.1 %)**

Butyl benzyl phthalate (BBP) (0.1 %)

Dibutyl phthalate (DBP) (0.1 %)

Diisobutyl phthalate (DIBP) (0.1 %)

Category 11 products include all other electronic and electrical equipment not covered under the other categories. Included are 2-wheeled vehicles, electronic nicotine delivery systems (ENDS) such as e-cigarettes, cannabis vaporizers and vape pens. Also included are electrical cables that are less than 250V working voltage.

Export Control (CCATS numbers HTS, ECCN numbers) for all products

A) CCATS Numbers **CCATS** (*Commodity Classification Automated Tracking System*)

- CCATS is an official classification determination by the US Department of Commerce
- Refer to: <I:\Trade Compliance\CCATS Commerce Classifications>

Per Mary Slack (29 Jan 18) If a customer requests a **CCATS** (*Commodity Classification Automated Tracking System – an official classification determination by the US Department of Commerce*) for one of our products, you may go to this folder location to get one – if we have it: <I:\Trade Compliance\CCATS Commerce Classifications>. Go ahead and bookmark the page.

Also found in that folder are two letters regarding our self-classification of SecureSync (one for Hong Kong specifically), and one regarding our self-classification of GSG-55.

If a customer requests a CCATS for a product but you don't see it in that folder, please let me know. Either I neglected to put it in the folder, or more likely, we self-classified. If a self-classification letter for a specific product is required, as opposed to you telling them we self-classified, then let me know the product and I'll write one up.

B) HTS and ECCN Numbers

- For HTS and ECCN Numbers for all our products, refer to the latest version of the “**US_Export_Controls_Matrix**”, at either of the following
 - <I:\Trade Compliance\Export Control Matrix>
 - <I:\Customer Service\Export Control-HTS and ECCN numbers>

Note: Other available locations for HTS/ECCN: t

- This info is also listed in “ITEMS” in Arena (search for the desired product and its listed)
- Other available in the SAP Registered Products table

Email from Mary Slack (27 Feb 17) I've attached the latest and greatest [Export Controls Matrix](#) for Spectracom. You can find this file in two other locations:

- 1- US Export Compliance Library in Salesforce: [SalesForce Export Compliance Library](#)
- 2- Compliance Documents in SharePoint: [SharePoint Trade Compliance Documents](#)

Please note that this ***new*** version of the matrix reflects the classification category changes announced earlier in the month for our timing products. You may share this document or the information in it if you include this disclaimer:

This commodity classification information is available for informational purposes only, and not intended to constitute legal advice or to be used as a substitute for specific legal advice. It may not reflect the most current legal developments, and Orolia (Spectracom) does not represent, warrant or guarantee that it is complete, accurate or up-to-date. This information is subject to change without notice.

Bug/issue in Intel's Atom C2000 processor ("Clock Signal Component Issue")

- Refer to Salesforce case 24389
- Reported by Cisco, as this chip is adversely affecting some of their switches
- Refer to the following sites for more info on this specific issue: (Cisco's advisory letter to their customers) <http://www.cisco.com/c/en/us/support/web/clock-signal.html#~overview> and (A good summary of the Cisco announcement and of the specific issue itself) <http://www.guru3d.com/news-story/intel-atom-c2000-chips-are-bricking-products.html>.
- This component is not used in any Spectracom devices (such as SecureSyncs and Legacy VelaSyncs - which are spec'd to use in Intel Xeon processor).

Product Registration/register your product

- **Website address to register a Spectracom product:**
<http://register.spectracomcorp.com/?ProductFamily=SecureSync&SN=ENG-1208>

Premium Support Packages (PSP and GPSP)

- **Link to info/data sheet on our website:** <https://www.rolia.com/products-services/support-plans#anchor-2354>

Actual PSP/GPSP contracts are in Salesforce

Contact info

Entitlement Descriptions for Spectracom Service Contract Number: 057961

24/7 emergency technical customer support

We understand that many operations are continuous so support on a 24/7 basis is important to ensure fast resolution to mission-critical problems anytime. If you are not able to reach a technical support representative immediately, then we return your call in less than 1 hour.

Telephone number	Country, city reference	Std time UTC offset	Add an hour for summer time
+1 585 455 7411	United States, New York	UTC-5	Second Sunday of March to first Sunday of November
+33 (0)9 88 28 40 70	France, Paris & United Kingdom, London	UTC; UTC+1	Last Sunday of March to last Sunday of October

When you call the 24/7 emergency technical customer support number, please have your service contract number if possible. If it is not available, then we will verify the entitlement by company name, contact name or email address, or serial number.

Annual Cost/pricing for PSP

- PSP is NOW charged at **20%** of the price of the appliance, GPSP is **30%**. (no longer 15% at time of purchase or 18% thereafter, as it used to be)

Email from Scott Z (4 March 2019) (I had mentioned I thought it as 15%/18%) One correction -This is considered the "floor" meaning we do NOT want to price below this unless previously discussed and approved by me. Need some compelling reasons as to why. However, you can always quote a higher percentage based on specific needs of the customer as long as we can deliver.

I will make sure the verbiage and % gets updated in our Price Book to avoid confusion.

Restrictions based on age of equipment

Per Denise Cond (March 2021) We only offer PSP on the unit for 7 years. After that time we tell them they should look in to get a new unit

Nice description from Jeremy on what constitutes Emergency Tech Support

Mission Critical Error: causes the Product to cease operating or operating in any material respect or causes a significant function of the Product to be impaired although it still operates; or (ii) is likely to cause the operation of the Product to delete, impair, damage or corrupt any System or "Customer" data. A Mission Critical Error will also include any Error in the Product that poses, or causes the operation of the Product to pose, imminent harm to any System or "Customer" data, or (iii) may have a material adverse impact on "Customer's" business. This does not include general practices such as Product setup and configuration, firmware updates, or general questions about the Products operation or functionality. For Mission Critical Errors outside of Spectracom's normal support hours, Errors must be reported by phone at 585-xxx-xxxx. The general support line and email are not acceptable methods of notification for Mission Critical Errors outside of normal business hours.

"In country" terms (for PSP loaners)

From Salesforce

"In country terms means locations with a service center that is prepared to overnight ship loaners to the customer's location."

Email from Keith to Tony DiFlorio (10 Feb 16): So, I believe this means that Spectracom US, Spectracom France and with limitations, EZU rentals in Asia, will cover the costs to overnight a temporary loaner to an address in the country that the "Service Center" is located in (Dave, Morgan and I ship the loaner to a US address on our shipping account). We can still ship a temporary loaner to another country, but the customer is responsible for all shipping/customs fees to and from that location. Note- as they also get expedited repairs for a quick turn- a loaner shipped overseas may not be worth all of the addition shipping costs - they would be much better off having a spare available at that location,

The temporary loaner covers the time needed for transit, repair and re-install of the original equipment. customer is responsible for return shipping of the loaner back to us.

As will all repairs (whether or not they have PSP), the customer is responsible for shipping equipment to Spectracom. While the equipment is here, all PSP customers get expedited repair service. We return warranty repairs our cost to the desired address. Customers are responsible for the return shipping of non-warranty repairs.

SpectraTime / SpectraTime oscillators

****Warranty period on repairs and new units**

Q. What is the warranty period for the oscillators part?

A. **Email from Lisa Perdue (11/1/12)** We always give 90 days on repair parts, and the new unit is 3 years.

****SpectraTime contact for RMA Status**

- Send RMA requests/ RMA Status and requests for root cause to Nino.

Nino De Falcis

VP of Sales and Marketing

(512) 394-8463 (Houston, TX)

Email: nino@spectratime.com

Point of contact for SpectraTime (in Les Ulis)

Florise Breiner florise@spectratime.com

Email from Eric Girard (Oct 2020) I will forward this to Florise who also work for Spectratime

Obtaining RMA Numbers for SpectraTime oscillator repair requests

- For info on SpectraTime RMAs, refer to “**SpectraTime RMA Procedure.docx**” located in: <I:\Customer Service\Spectratime RMAs>
- Link to form on our Spectracom website (for customers to request an RMA)
<http://spectracom.com/support/spectratime-return-request>
- Per Nino- RMA must be processed thru our RMA form at <http://www.spectratime.com/support/returns/> and submitted at RMA@spectratime.com.

Email from Dave Lorah to a customer (20 Nov 2015) To apply for a Spectratime RMA number we must ask you to please complete this request from our website:

<http://spectracom.com/support/spectratime-return-request>

This will ensure the RMA process is not delayed. I will then assist you with the return to Spectracom and forward the device to SpectraTime.

Spectracom Cage Code and NSN Numbers (National Stock Numbers)

per one of NAVY customers (8 Oct 2019) "The CAGE (Commercial And Government Entity) code is a number assigned by the Defense's Logistics Agency (DLA)"

Cage Code Number for Spectracom

- Refer to <https://www.logisticsinformationservice.dla.mil/bincs/details.aspx>

(Search for "Orolia")

The screenshot shows the DLA LIS website with the following details:

- DEFENSE LOGISTICS AGENCY** Logistics Information Service
- Navigation: Home | Products | Services | Programs | Cataloging | Log Tools | Supplier | Training | Library
- BINCS** Company Details
- BINCS Information**
 - DUNS Number: 067920074
 - JCP Cert. Number: 0046901
 - CAGE Code: 59797
 - Links: [Do a System for Award Management - SAM \(formerly CCR\) inquiry](#), [Do a JCP Inquiry](#)
- CAGE Information**
 - Company Name: SPECTRACOM CORPORATION
 - CAGE Status: Active Record
 - SAM Expiration Date: 06/26/2015
 - Parent CAGE:
 - Address: 1565 JEFFERSON RD STE 460
 - P.O. Box:
 - City: ROCHESTER
 - Zip: 14623-3190
 - CAO-ADP: 53306A-HQ0337
 - State: NY
 - County:
 - Voice Phone Number: 5853215806
 - Fax Phone Number: 5853215219
 - Date CAGE Code Established: 12/06/1980
 - CAGE Last Updated: 6/26/2014
 - Point of Contact: TONY DIFLORIO
 - Company Web Site: [HTTP://WWW.SPECTRACOMCORP.COM/](http://www.spectracomcorp.com/)

- A) Cage Code number for "Orolia, USA" (Rochester) is 59797
- B) Cage Code number for "Orolia" (France) is FARL2
- C) Cage Code number for "Orolia Limited" (Portsmouth) is U0BZ2
- D) Cage Code number for "Orolia" (France) is FARL2
- E) Cage Code number for "Orolia LTD" (UK) is U0913
- F) Cage Code number for "Orolia SAS" (UK) is FAU27

Lists of all Spectracom NSN numbers

- Go to http://www.dlis.dla.mil/webflis/pub/pub_search.aspx and enter just the “CAGE Code” value for one of the following:
 - **59797 for Spectracom Rochester items**
 - U0913 for Spectracom UK items
 - FARL2 for Spectracom France items
 - FAU27 for Spectracom Guidel items
 - U0BZ2 for Spectracom Portsmouth items

Examples:

SecureSync 012		
1165-0012-0600	SERVER,AUTOMATIC DATA PROCESSING	7035015900470
1191-1001-0600	CIRCUIT CARD ASSEMBLY	5998015975669
1200-011	GENERATOR,DIGITAL CLOCK PULSE	6625016030257
1200-013	FREQUENCY REFERENCE AND ELECTRON	6625015944656
1200-06	CIRCUIT CARD ASSEMBLY	5998015968519
1204-01	CIRCUIT CARD ASSEMBLY	5998016165496
1204-02	CIRCUIT CARD ASSEMBLY	5998016165498
1204-05	CIRCUIT CARD ASSEMBLY	5998015968515
1204-08	CIRCUIT CARD ASSEMBLY	5998016165499
1204-10	CIRCUIT CARD ASSEMBLY	5998016165497
1204-18	CIRCUIT CARD ASSEMBLY	5998016165501
8181-0001-B000	RECEIVER SUBASSEMBLY,RADAR	5840014990546
818183A	RECEIVER SUBASSEMBLY,RADAR	5840014990546
8183A	RECEIVER SUBASSEMBLY,RADAR	5840014990546
8225 0001 0600	ANTENNA	5985015798484
8225-0001-B000	PARTS KIT,ELECTRONIC EQUIPMENT	5895014990506
8225FAA	PARTS KIT,ELECTRONIC EQUIPMENT	5895014990506
8226-0001-B000	ABSORBER,OVERVOLTAGE	5920014990549
8226-0002-0600	ARRESTER,ELECTRICAL SURGE	5920015909191
9383 NETCLOCK	GENERATOR,DIGITAL CLOCK PULSE	5895015941499
9383 OPT-08-09	CLOCK,MASTER REGULATING	6645015957428
9383-05	CLOCK,MASTER REGULATING	6645016011707
9383-OPT11	CLOCK,MASTER REGULATING	6645015741961
9383-OPT11	CLOCK,MASTER REGULATING	6645015741969
CA010N0N3100	CABLE ASSEMBLY,RADIO FREQUENCY	5995015922520
CA01-0N0N-3100	CABLE ASSEMBLY,RADIO FREQUENCY	5995014990571
CA07050	CABLE ASSEMBLY,RADIO FREQUENCY	5995014990550
CAL7050	CABLE ASSEMBLY,RADIO FREQUENCY	5995015969953
CAL7100	CABLE ASSEMBLY,RADIO FREQUENCY	5995014990571
CNT-91R/AF	COUNTER,ELECTRONIC,DIGITAL READO	6625016106855
GPS TIME SERVER	CLOCK,MASTER REGULATING	6645015273561

LS-518A/SIC MOD	INTERCOMMUNICATION STATION SUBAS	5830013764710
MODEL 9383	COMPUTER SUBASSEMBLY	5895015798026
MP00023	PAPER,CHART,LITHOGRAPHIC	9310011344140
MP33R-0000-0002	CONVERTER,FREQUENCY,ELECTRONIC	5895015742109
MP33R-0000-0003	CONVERTER,FREQUENCY,STATIC	5895015742108
NETCLOCK 9383-05	CLOCK,MASTER REGULATING	6645016011707
S00001	SWITCH,PUSH	5930011226420
S00002	SWITCH,PUSH	5930011226421
T10001	TRANSFORMER,POWER	5950011226549
TPRO-CPCI	CIRCUIT CARD ASSEMBLY	5998015888759
TTS200	CLOCK,MASTER REGULATING	6645015273561
TV400W	GENERATOR,DIGITAL CLOCK PULSE	6625015732513
VGO-VME	CCA VIDEO GRAPHICS,	5999015544249

Conflict Minerals position report/Smelter list

- Refer to the example response email/Orolia report: [I:\Customer Service\Conflict minerals report](#)
- See Mary Slack to obtain our latest report.
- Refer customers directly to Mark if they have any questions/additional requirements.


Example report below:

Orolia USA_Spectracom_CFSL_CMRT 4.10_asOf_31DEC2015-final [Protected View] - Excel

File Home Insert Page Layout Formulas Data Review View Tell me what you want to do

PROTECTED VIEW Be careful—email attachments can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing

R41C2



Conflict Minerals Reporting Template (CMRT)

Selections:
 Select language: **English**
 Select country: **USA**
 Select company type: **Manufacturer**
 Select product type: **Electronics**
 Select product category: **Consumer Electronics**
 Select product subcategory: **Smartphones**
 Select product model: **iPhone 12**
 Select product description: **iPhone 12, 128GB, 5.8 inch**

Declaration

The purpose of this document is to collect sourcing information on tin, tantalum, tungsten and gold used in products

Mandatory fields are noted with an asterisk (*)

Company Information

Company Name (*): Orolia USA, Inc. (dba Spectracom)
Declaration Scope or Class (*): A. Company
Description of Scope: Company wide
Company Unique ID: 87820074
Company Unique ID Authority: DUNS
Address: 1665 Jefferson Road, Suite 460, Rochester, NY 14623-3190 US
Contact Name (*): Mary Slack
Email - Contact (*): mslack@spectracom.com
Phone - Contact (*): +1-585-321-5800
Authorizer (*): Derek Darling
Title - Authorizer: Operations Manager
Email - Authorizer (*): ddarling@spectracom.com
Phone - Authorizer (*): 585-321-5800
Effective Date (*): 31-Dec-2015

Answer the following questions 1 - 7 based on the declaration scope indicated above

1) Is the 3TG intentionally added to your product? (*)

Answer	Comments
Tantalum (*) Yes	We are not intentionally adding 3TG to our products. However, we may use 3TG in our products. Source is unknown. Inconsistent supply chain.
Tin (*) Yes	
Gold (*) Yes	
Tungsten (*) No	

2) Is the 3TG necessary to the production of your company's products and contained in the finished product that your company manufactures or contracts to manufacture? (*)

Answer	Comments
Tantalum (*) Yes	We are not intentionally adding 3TG to our products. However, we may use 3TG in our products. Source is unknown. Inconsistent supply chain.
Tin (*) Yes	
Gold (*) Yes	
Tungsten (*) No	

3) Do any of the smelters in your supply chain source the 3TG from the covered countries? (SEC term, see definitions tab) (*)

Answer	Comments
Tantalum (*) Unknown	We are not intentionally adding 3TG to our products. However, we may use 3TG in our products. Source is unknown. Inconsistent supply chain.
Tin (*) Unknown	
Gold (*) Unknown	
Tungsten (*)	

Taking remote control of a customer's PC (gotomeeting/teamviewer)

Choices

- A) Webex (Spectracom doesn't currently don't have an account for us to use this service-).
- B) gotomeeting
- C) Arkadin (we have an account)
- D) join.me (
- E) teamviewer (<http://www.teamviewer.com/en/index.aspx>)

Gotomeeting

- Customer and Tech Support needs to download “**desktop**” (not “lite”) to make us a presenter (allows us to take control of mouse and keyboard)
- open gotomeeting
- Send invite to email address (add message in Outlook)
- download “desktop” version Gotomeeting
- customer selects “Share keyboard + mouse” (under “Screen” tab). If selection not there, likely not using the desktop version of gotomeeting
- make them the presenteer
- don’t forget to type “exit” to logout of the timeserver.

Linux BASH terms commonly used with Linux-based products

➤ Refer to sites such as: <http://ss64.com/bash/>

- **cat**: Type the contents of a file
- **cd /**
- **echo " ":** displays text
- **find**: finds files or directories
- **getent**: Displays entries from databases in */etc/nsswitch.conf*.
Supported databases: ahosts ahostsv4 ahostsv6 aliases ethers group gshadow hosts initgroups netgroup networks passwd protocols rpc services shadow

Note: to filter, enter the username at the end of the string

Example:

```
spfactory@Spectracom /etc $ getent shadow spadmin
spadmin:$1$a0P9NVVT$8VOU8EP7awhQs63mq9vRT.:16176:0:99999:7:::
```

- **grep**: Search file(s) for lines that match a given pattern

grep -v reverses the sense of the match. It's a "not" so it will do the opposite (look for anything not the grepped value)

Refer to sites such as: <http://en.wikipedia.org/wiki/Grep>

Examples: grep "sys" kern.log

```
spfactory@Spectracom /home/spectracom/log $ grep "sys" kern.log
Mar 20 18:11:05 Spectracom kernel: rtc_cmos rtc_cmos: setting sys
18:10:14 UTC (1426875014)
Mar 20 18:11:05 Spectracom kernel: EXT3-fs (hda1): mounted file
mode
Mar 20 18:11:05 Spectracom kernel: VFS: Mounted root (ext3 file
```

cat kern.log | grep signal

```
spfactory@Spectracom /home/spectracom/log $ cat sys.log | grep signal
Feb 17 18:56:41 Spectracom exiting on signal 15
Feb 17 19:12:18 Spectracom exiting on signal 15
Feb 18 23:06:20 Spectracom exiting on signal 15
Feb 18 23:10:10 Spectracom exiting on signal 15
```

- **less** or **more**: text files to scroll
- **ls**: list the contents of a folder.
- **ls -al** list the contents of a folder and includes permissions, file sizes, etc
- **rm -f xxxxxx** (delete a file. Where xxxxxx is the file name to remove)
- **tail**

tail -f file name: Tail prints the last line from given input. (it updates automatically if a new entry is asserted)

Example: tail -f log/user.log

tail -n file name: Tail -n prints the last N number of lines from given input. By default, it prints last 10 lines of each given file.

Example: **tail -n1** (once per second)

file text editors (vi, nano, etc)

A) nano Text editor

➤ refer to sites such as: <https://www.computerhope.com/issues/ch000773.htm>

type nano in front of the file name

B) vi: (vi editor) Text Editor

- refer to sites such as: <https://www.cs.colostate.edu/helpdocs/vi.html> and <https://kb.iu.edu/d/afdc>

Notes:

- <ESC> denotes the **Esc** key, and <CR> denotes the **Enter** key.
- The expression <cmd> means that you should enter a command. <f> means that you should enter a filename, and <x> means that you should enter a character or number.
- The symbol ^ (caret) means that you should hold down the **Ctrl** key while pressing the indicated letter.

Vi editor command keys:

ZZ	Exit, saving changes	t<x>	Up to <x> forward
Q	Enter ex mode	T<x>	Back up to <x>
<ESC>	End of insert	<x>	Go to column <x>
:<cmd>	Execute ex command	w,W	Forward one word
!<cmd>	Shell command	b,B	Back one word
^g	Show filename/size	e,E	End of word
^f	Forward one screen	^h	Erase last character
^b	Back one screen	^w	Erase last word
^d	Forward half screen	^?	Interrupt
^u	Backward half screen	~	Toggle character case
<x>G	Go to line <x>	a	Append after
/<x>	Search forward for <x>	i,I	Insert before
?<x>	Search backward for <x>	A	Append at end of line
n	Repeat last search	o	Open line below
N	Reverse last search	O	Open line above
]]	Next section/function	r	Replace character
[[Previous section/function	R	Replace characters
%	Find matching () { or }	d	Delete
^l	Redraw screen	dd	Delete line
^r	Refresh screen	c	Change
z<CR>	Current line at top	y	Yank lines to buffer
z-	Current line at bottom	C	Change rest of line
^e	Scroll down one line	D	Delete rest of line
^y	Scroll up one line	s	Substitute character
``	Previous context	S	Substitute lines
H	Home window line	J	Join lines
L	Last window line	x	Delete after
M	Middle window line	X	Delete before
+	Next line	Y	Yank current line
h j k l	Cursor movement: left/down/up/right	p	Put back lines
0	Beginning of line	P	Put before
\$	End of line	<<	Shift line left
f<x>	Find <x> forward	>>	Shift line right
F<x>	Find <x> backward	u	Undo last change
		U	Restore current line

Ex mode commands:

q	Quit	set <x>	Enable option
q!	Quit, discard changes	set no<v>	Disable option
r <f>	Read in file <f>	set all	Show all options
sh	Invoke shell		
vi	Vi mode		
wq	Write and quit		
w <f>	Write file <f>		
w! <f>	Overwrite file <f>		

How To's

To search for partial or whole words/phrases press "/" (ctrl c to go back to the search)

To insert text, paste and then press esc

Inserting or Adding Text

The following commands allow you to insert and add text. Each of these commands puts the vi editor into insert mode; thus, the <Esc> key must be pressed to terminate the entry of text and to put the vi editor back into command mode.

*	i	insert text before cursor, until <Esc> hit
	I	insert text at beginning of current line, until <Esc> hit
*	a	append text after cursor, until <Esc> hit
	A	append text to end of current line, until <Esc> hit
*	o	open and put text in a new line below current line, until <Esc> hit
*	O	open and put text in a new line above current line, until <Esc> hit

To exit the file

- To exit AND SAVE file changes: press esc, then shift & “:” Then type: **q**
(or type “**quit**” (quit by itself) can also “shift c” and then type **quit**)
- To exit and NOT SAVE file changes: press esc then shift & “:” Then type: **q!** (lower-case q and the “!” symbol)
(or type “**quit!**” (quit followed by an exclamation mark))

- **watch**: refresh one or more displayed items such as tables

Note: CTRL C to exit

A) Watch only one item:

watch -n 0.1 CS_GetTime 0 0 (where 0.1 is the refresh rate in seconds)

```
spadmin@Spectracom ~ $ watch -n 0.1 CS_GetTime 0 0
spadmin@Spectracom ~ $
```



```
spadmin@Spectracom:~
Every 0.1s: CS_GetTime 0 0 Tue Mar 25 16:10:49 2014

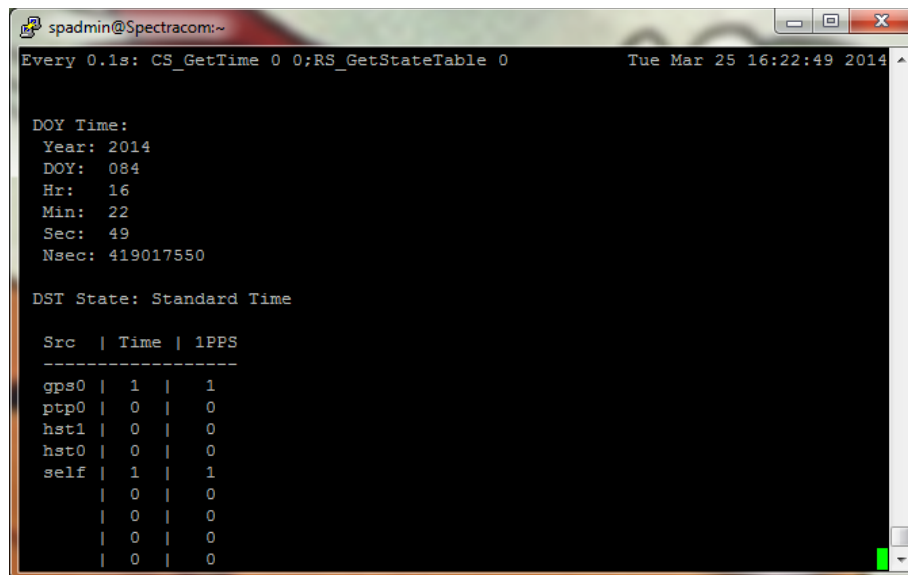
DOY Time:
Year: 2014
DOY: 084
Hr: 16
Min: 10
Sec: 49
Nsec: 119427170

DST State: Standard Time
```

B) Watch two items at the same time:

watch -n 0.1 'CS_GetTime 0 0;RS_GetStateTable 0 2' (where 0.1 is the refresh rate in seconds)

```
spadmin@Spectracom ~ $ watch -n 0.1 'CS_GetTime 0 0;RS_GetStateTable 0'
spadmin@Spectracom ~ $
```



```
spadmin@Spectracom:~
Every 0.1s: CS_GetTime 0 0;RS_GetStateTable 0 Tue Mar 25 16:22:49 2014

DOY Time:
Year: 2014
DOY: 084
Hr: 16
Min: 22
Sec: 49
Nsec: 419017550

DST State: Standard Time

Src | Time | 1PPS
-----
gps0 | 1 | 1
ptp0 | 0 | 0
hst1 | 0 | 0
hst0 | 0 | 0
self | 1 | 1
    | 0 | 0
    | 0 | 0
    | 0 | 0
    | 0 | 0
```

- **whereis**: Search the user's \$path, man pages and source files for a program
- **which**: Search the user's \$path for a program file
- **whoami**: which account you are logged as

Time of Day conversion (seconds since midnight)

TOD (Seconds) 0 to 86400:

01:00= 3600

02:00 = 7200

03:00 = 10800

04:00 = 14400

05:00 = 18000

06:00 = 21600

07:00 = 25200

08:00 = 28800

12:00 = 43200

17:00 = 61200

19:00 = 68400

22:00 = 79200

SHA-256/MD5 file checksums for software update files (for all products)

1. <https://github.com/jessek/hashdeep/releases>

email from Dave Sohn (1 Aug 2019) I found a set of command line tools that can generate these hashes: <https://github.com/jessek/hashdeep/releases>

v 5.8.4

MD5: cff47c5d5dd75c58c9bd1ed180c02f29

SHA1: ec44f522e7fd1f48a4a6b93af2ed81d5cc94a54f

SHA-256: f9c555a088a9ada99584be673b5166e6848e35e203db2e13c3da46da7fbca4fb

v5.8.5

MD5: ccadbb4309b97a77d3adfca335c7546d

SHA1: 69ba0eb415c0751a0cd3ece26c0b5aa38567ab02

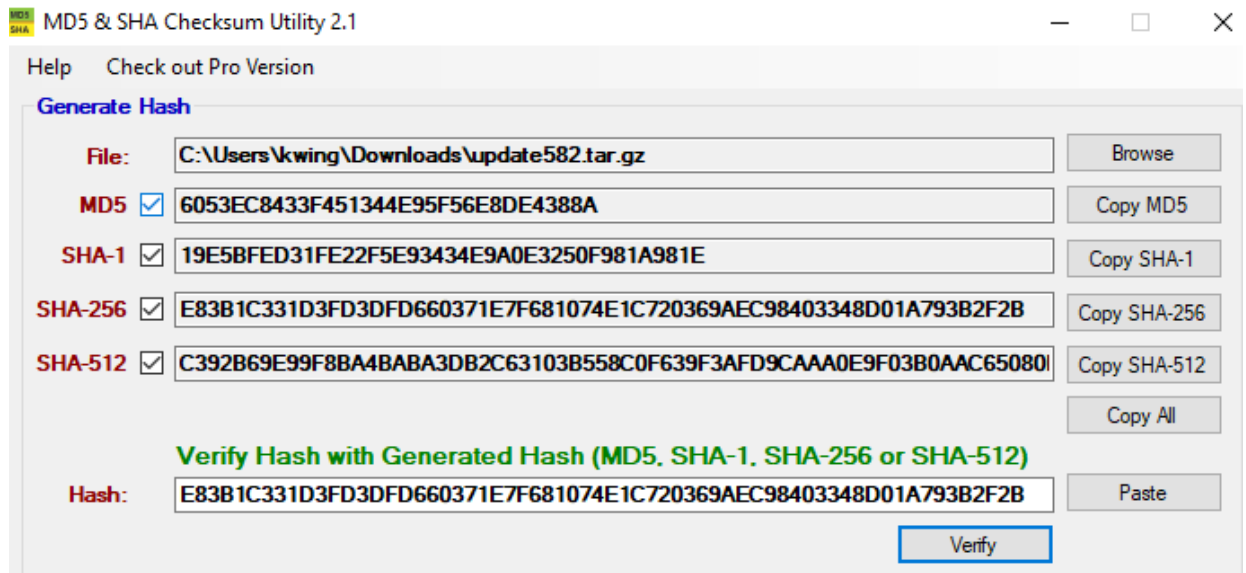
SHA-256: 75892205ae019500f18e8da275a5a2d056da3a25d4e13011f071689ebd469d78

2. for SHA-256/SHA-1 or MD5 checksum, download a program such as “MD5 & SHA Checksum Utility” (<https://raylin.wordpress.com/downloads/md5-sha-1-checksum-utility/>) to verify an upgrade file. In the upper right, it's in the Software dropdown

The directions to generate a hash are on the same page (below the download button) and excerpted below:

Instruction to Generate hash

1. Tick on the hashes that you want to generate
2. Drag and drop a file into the program or use the Browse button to select a File
3. Selected hashes will be generated
4. Click on Copy All button if you want to copy all the selected hashes to clipboard (Useful for sharing hash with people)



Note: after generating the hashes, verify the **MD5** hash in the generator matches the MD5 checksum for the update file posted on our website. This confirms the validity of the other generated checksums (if the MD5 hash doesn't match the one on our site, there was a problem somewhere with the generation of the hashes (wrong file

was used to generate it, the file used to generate the hashes may be corrupt, etc)

Instruction to Verify hash

1. Download a software that provides MD5, SHA-1 & SHA-256 hash
2. Copy one of the hashes to clipboard (Ctrl + C)
3. Drag and drop the downloaded file into the program or use the Browse button to select the downloaded file
4. Selected hashes will be generated
5. Click on the Paste button
6. Click on the Verify button and the result will be displayed in a message box

You can try generate hash for this software and verify with one of the the checksum below.

Checksums for MD5 & SHA Checksum Utility 2.1 (Free)

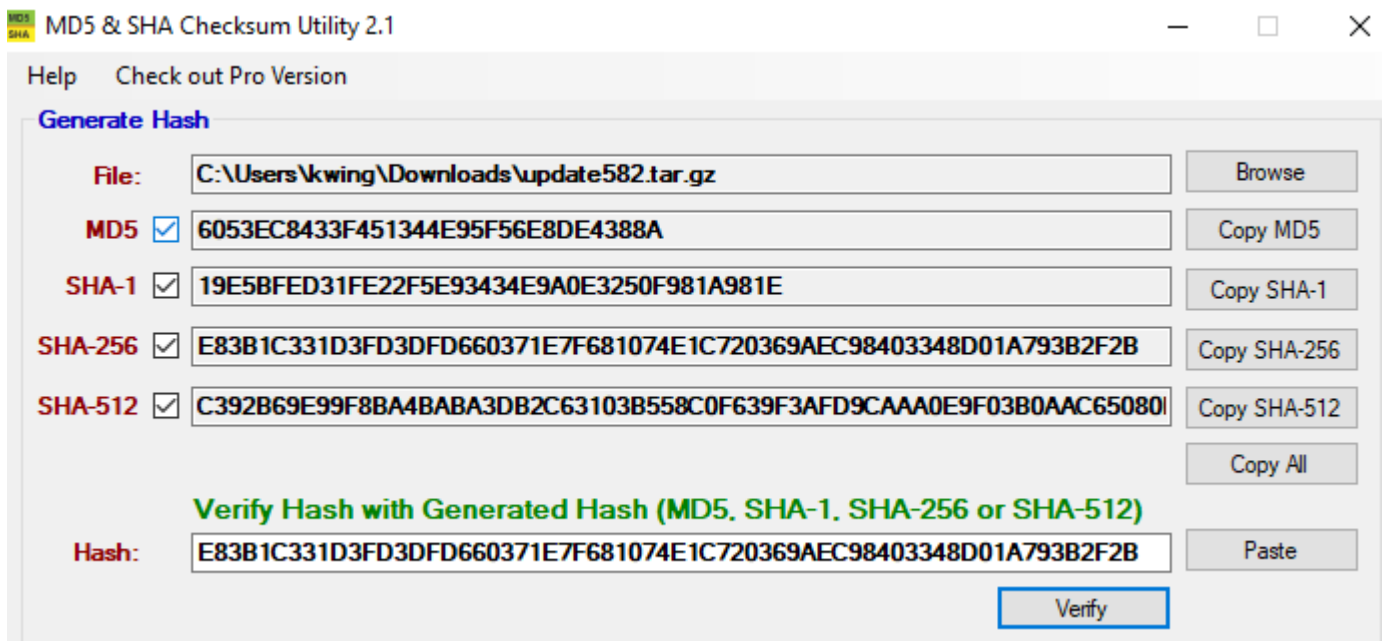
MD5 Checksum: 2D423B85E6684956B817E6C7E36BE3DC

SHA-1 Checksum: 4B70B5213249014C3785460720B81B5F9BEABEC3

SHA-256 Checksum: D3D6F3597AEBA37312F61E59BA465E57B19140CC9A4517C7F9C49461F1D0A4BB

SHA-512 Checksum (double-click below in order to select and copy full checksum):

53914AFA0E66C50BBD12D9FFB7833FD5094FA10735D8700BFF9CD87C2A7EB478D6715B3



- For just MD5, use a program such as MD5 checker (<http://www.georgejopling.co.uk>) to verify an upgrade file. In the upper right, it's in the **Software** dropdown.
- We supply the MD5 hash on our website.
- The .md5 file in the New Released drive (such as update485.tar.gz.md5) is a text file indicating the correct md5 checksum for the update file.
- To verify a file, either get the MD5 hash from our website or open the corresponding MD5 file for that particular update file as a Notepad or WordPad document. This will provide the correct MD5 hash.
- "Copy" this value.

- Run MD5 checker against the update file. **File -> Select File.**
- It will compare the checksum to the one that was copied and then report if it was a valid check.

This Tool now reporting an error message after selecting a file to hash, and no longer able to generate hashes for higher than sha-1 (sha-1 and MD5 hashes can still be generated just fine)

“System.InvalidOperationException: This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms. at System.Security.Cryptography.MD5CryptoServiceProvider..ctor() at MD5_SHA_Checksum_Utility.frmMD5_SHA_Checksum_Utility”

- Refer to sites such as: <https://stackoverflow.com/questions/14509354/this-implementation-is-not-part-of-the-windows-platform-fips-validated-cryptogra>
- Appears our IT team has since hardened security on our PCs to include changes for FIPS compliancy. This tool is no longer meeting the FIPS requirements, and the only way to get the tool to perform sha-256 or higher hashes is to override group policy settings???
-

MTBF/MTTR (for all products)

MTBF (Mean Time Between Failure)

Wikipedia- MTBF is the predicted elapsed time between inherent failures of a system during operation.^[1] MTBF can be calculated as the [arithmetic mean](#) (average) time between [failures](#) of a system. The MTBF is typically part of a model that assumes the failed system is immediately repaired ([MTTR](#)), as a part of a [renewal process](#). This is in contrast to the mean time to failure (MTTF), which measures average time to [failures](#) with the modeling assumption that the failed system is not repaired (infinite repair rate).

MTTR (Mean Time To Repair)

Wikipedia - MTTR is an abbreviation that has several different expansions, with greatly differing meanings. It is wise to spell out exactly what is meant by the use of this abbreviation, rather than assuming the reader will know which is being assumed. The M can stand for any of *minimum*, *mean* or *maximum*, and the R can stand for any of *recovery*, *repair*, *respond*, or *restore*. The most common, *mean*, is also subject to interpretation, as there are many different ways in which a mean can be calculated.

- [Mean time to repair](#)
- [Mean time to recovery/Mean time to restore](#)
- [Mean time to respond](#)
- [Mean time to replace](#)

For estimated MTBF calculations Scott Holmes has performed, refer to the (SecureSync Reliability Summary" (Product Reliability.xlsx spreadsheet)

https://oroliagroup-portal1.sharepoint.com/_layouts/15/osssearchresults.aspx?u=https%3A%2F%2Foroliagroup%2Dportal1%2Esharepoint%2Ecom&k=product%20reliability#k=product%20reliability

To calculate the "Actual" MTBF (based on repair data) use the **MTBF** database located in: [\Company Wide\access\TESTLOG](#)

A) Legacy VelaSync (Model 1225)

Email from Justin Velez to Andrew (9 Dec 16)

Here is the Legacy VelaSync's quality performance data:

Fielded MTBF = 132,588 hours

2016 First Pass Yield = 97%

B) GSG (GPS Simulators)

Per Lisa Perdue (12 Feb 2013), refer to GSG manuals for MTBF calculations.

C) BUS-LEVEL TIMING BOARDS

1. TSync series timing boards (TSync-PCIe, TSync-PMC, TSync-cPCI, TSync-VPX, etc)

Email from Scott Holmes (8 June 16) to Tony Diflorio: We haven't calculated MTBF for any of the board products to date.

We changed tactics on this over the past 6 months and now we send out to a reliability service (SoHaR) that calculates MTBF for a base product in a product line. Once that's done, SoHaR delivers a report and the program files to us. We purchased and installed the same software SoHaR uses so we can recalculate for future options or similar products in the product line.

It's about a 2 to 3 week lead time from SoHaR for a MIL-217 MTBF report. Cost to have a board product calculated is about \$1,200.

Note: Per Scott Homes (29 Oct 15): he hasn't ever officially calculated MTBF for the TSync family timing boards. The MTBF numbers that have been provided thus far (such as the calculation below) were an estimate of what the number would likely be if it was calculated based on the SecureSync's MTBF calculations.

The MTBF for the TSync-PCIe is 167,161 Hrs per MIL-HDBK-217F. Environment is Ground Benign @ 25C.

Email from Dave Sohn (responding to an email about Tsync-PMC MTBF 10/30/15 KW) We don't have an MTBF specifically calculated for the PMC, however, the MTBF of our TSync-PCIe board, as calculated per MIL-STD-217F, is 104,680 hours for a mission profile of ground benign at 25°C. The PMC board is substantially similar to this PCIe board. The top 8 components that contribute to 97.3% of the failure rate are identical in both boards.

3. TSync-VPX boards

Email from Dave Sohn (25 Nov 15) We don't have an MTBF specifically calculated for the VPX, however, the MTBF of our TSync-VPX board, as calculated per MIL-HDBK-217F, is 104,680 hours for a mission profile of ground benign at 25°C. The VPX board is substantially similar to this PCIe board. The top 8 components that contribute to 97.3% of the failure rate are identical in both boards.

4. (TPRO-PCI-66U / TSAT-PCI-66U) and (TPRO-PCI-U-2 / TSAT-PCI-U-2)

- Both Models are the same, only difference is the firmware – MTBF is the same for both the PCI-66U and PCI-U-2

Per Scott Holmes' calculations: **195,888 Hrs per MIL-HDBK-217F. Environment is Ground Benign @ 25C.**

Per Jim Allocco, round-up to be 200,000 hours

5. MTBF for TPRO/TSAT-PMC/cPCI boards

The MTBF for the Spectracom model PMC-100 IRIG Reader/Generator boards in an AIR Cargo environment (AIC) = 110,807 hours.

The MTBF for the Spectracom model PMC-100 IRIG Reader/Generator board in a Ground Benign environment (GB) = 797,807 Hours.

6. MTBF for TPRO/TSAT-VME

(Email from Dave Lorah, 3/10/11) Using the Visual and repair data the MTBF is calculated at 605,000 hours (69 years).

Response from Jim Allocco: Email response from Jim Allocco: use "**80,000 hrs**"

D) 2400 SecureSync MTBF

- See Alaysia Gilbert with the Quality team. She has the MTBF data (Telcordia and Mil-HDBK)

(9 Dec 2022. From Alaysia Gilbert)

Telcordia and Mil-HDBK are the different methods used to calculate MTBF

Depending on the configuration:

Telcordia SR-332		MIL-HDBK-217F	
min MTBF	max MTBF	min MTBF	max MTBF
hrs	hrs	hrs	hrs
265307	320196	268307	320196

For this analysis, an ambient temperature of 25°C was investigated. An average temperature rise of 15°C was conservatively assumed, and a device operating temperature of 40°C was used for each component in the analysis.

E) 1200 SecureSync MTBF

- Refer to folder: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\MTBF>
- (10 Nov 17 KW) See Scott Holmes for MTBF reports, if a report for the desired Model is not in the folder referenced above. I understand Scott H has now started working with an outside vendor (Advanced Logistics Developments) to have them generate a more formal MTBF report. The folder above should contain the report for at least one Model, as an example of these newer reports.

SecureSync Option Cards

Per Ron Dries (15 May 2020) "For option card boards we say ~100,000 hours"

Email Keith sent The MTBF for SecureSync Option cards is ~100,000 hours (we do not calculate individual MTBF for each Model Option Card available for SecureSyncs)

Base SecureSync variants

D.1) Model 1200-213

- in folder at link above

D.2) Model 1200-201

Email from Dave Sohn, February 2020 "Don't use that older MTBF document from Scott H any more. We're basing it on a newer reliability study on the 1200-213 we contracted, then looking at deltas based on the old document.

We should say for **1200-201** that it is **>130,000 hours.**"

(Earlier info = use the info above for MTBF)

~~Email from Scott Holmes (19 Sept 17) Below is information on what we have for calculated MTBF that should be helpful.~~

~~We are using new reliability prediction software and hiring a service to do much of this work for us. Last year I asked them to calculate reliability prediction for the 1200-213 and they found the MTBF for this configuration to be 130,589 Hrs in a Ground Benign, 25°C environment. You can safely use this number for both the 003 and 013. The values would rise a little with no DG and OCXO but not enough to make a significant difference.~~

~~The better numbers are a result of more component improvements since the MIL-217 calculation method was last updated in 1995.~~

~~Partial email from Scott Hildebrandt to Josh (5 Oct 17) I don't know if you received an answer back on your inquiry, but here is the information you are looking for~~

Product	MTBF
SecureSync model 1200-001	130,000 hours
SecureSync model 1200-013	130,000 hours
SecureSync model 1200-023	130,000 hours

UPDATE (Note per Dave Sohn, February 2020) Don't use that older MTBF document from Scott H any more. We're basing it on a newer reliability study on the 1200-213 we contracted, then looking at deltas based on the old document.

— **Link to SecureSync MTBF in SharePoint ("", under "Test Report")**

➤ — Calculated per: "**MIL-HDBK-217F: Reliability Prediction of Electronic Equipment**"

➤ — **Link to SecureSync MTBF in sharepoint** (scroll down to "**Test Reports**" and select "**SecureSync MTBF**"— which is P/N "1200-1000-217Fr9)

— <https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/products/SecureSync/default.aspx>

Or search the entire site for "**1200-1000-217Fr9**"

"https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/products/SecureSync/_layouts/15/osssearchresults.aspx?u=http%3A%2F%2Foroliagroup%2Dportal1%2Esharepoint%2Ecom%2FSpectracom%2FEngineering%2Fproducts%2FSecureSync&k=1200%2D1000%2D217Fr9"

— **Component level MTBF breakdown (SecureSync Generic MTBF" under "Test Report")**

<https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/products/SecureSync/default.aspx>

Front panel keypad/LCD display

➤ — Per Scott Holmes, the MTBF data for SecureSync does not include the front panel keypad/LCD as they are not essential to operation of the equipment.

Individual SecureSync components: <https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/products/SecureSync/Shared%20Documents/SecureSync%20Generic%20MTBF.pdf>

Email from Russ Cope (2/5/10)

The poor number for the FPGA is per the MIL-HDBK-217 requested data to make the calculation.
The MIL-HDBK-217 MTBF for the complete units in Ground, Benign, 25°C conditions starts out at:
SecureSync Model 10 with: AC, Res-T, OCXO = 46,377 hrs

This number excludes non-critical components such as the front panel (displays and keypad), fan and option cards.
Major components in the unit that have the biggest impact on these numbers are as follows:

GPS Resolution T receiver = 471,183 (Mil 217 number)

Advantech ETX Module = 759,542 (Bellcore number)

OCXO = 594,262 (Unknown method)

AC Power Supply = 545,375 hrs

SecureSync MTTR (email sent to Florise on 1/6/11)

As for the MTTR (Mean Time to Repair) data for SecureSync, this value really depends on whether or not the customer has a spare SecureSync available at the site that they can swap in. If they have a spare appliance available (it never hurts to have a spare), the MTTR is about 45 minutes, or so. This includes moving all of the cables over to the spare, power-up, a new GPS survey being performed inside SecureSync and NTP synching to the System Time. Upon completion of the NTP being synced, the network has an NTP server available again.

If the customer does not have a spare SecureSync available at the site, the MTTR is then much larger, to include time for shipment of the equipment to the repair facility, the time needed to test and repair the equipment, time to ship back the appliance and the time to reinstall/resync the equipment to GPS, once they receive it back from the repair process. This time will inherently vary based on such factors as how long it takes to ship the unit in both directions (is it being returned to the US for repair or will it be returning to you for Eric to repair, customs delays, etc) form, and how long it takes to repair it when it arrives (for the US facility, our repair turnaround time is typically one to two weeks upon us receiving the equipment to the time that we are shipping it back to the customer). The recovery time once they receive back the equipment is about 45 minutes from the start of it being re-installed until its ready to synchronize a network.

Another available factor that we offer to help significantly reduce the MTTR is to offer the Premium Support Package. When a customer purchases Premium Support Package and the equipment fails, a free loaner SecureSync can be shipped out our next business day (For our US customers, we ship the loaner out for next day delivery). Having a loaner sent to the site will thus lower the MTTR to just a few days, depending on how fast they receive the loaner SecureSync. Once they receive the loaner, it takes about 45 minutes for the loaner to be ready to sync the network. Once they receive the repaired SecureSync back from repair, it takes about 45 minutes again to swap their SecureSync back in and then they can return the loaner.

In summary, I would say the typical MTTR if they do not have a spare SecureSync so that they can swap in for "immediate" recovery (and don't purchase the optional Premium Support Package to receive a loaner unit) is going to be about 3 to 4 weeks.

Model 9400 series (9483 and 9489) MTBF

Email from Scott Holmes (5 May 2014) We are using the SecureSync MTBF numbers for the 9400 series products. So just select the **SecureSync** configuration that matches closest to the 9400 series configuration and use that MTBF number.

- Link to SecureSync MTBF (scroll down to test reports and select "**SecureSync MTBF**")

<https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/products/SecureSync/default.aspx>

1. Model 9489

- Per Scott Holmes, the MTBF data for SecureSync does not include the front panel keypad/LCD as they are not essential to operation of the equipment.
- The Model 9489 is the same as a **SecureSync 1200-003** (minus the front panel) - AC power only, TCXO oscillator, Commercial GPS receiver.

2. Model 9483

- Per Scott Holmes, the MTBF data for SecureSync does not include the front panel keypad/LCD as they are not essential to operation of the equipment.
- Link to SecureSync MTBF (scroll down to test reports and select "SecureSync MTBF")
<https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/products/SecureSync/default.aspx>
- **Per Scott Holmes (5 May 2014)** The TCXO and OCXO have the same reliability so the numbers are the same for both. So, the comparable **SecureSync with OCXO is 1200-013**

Internal Email Keith sent (8 Jan 2019) Hi Trevor (Justin and Dave S), Good afternoon.

Per Scott Holmes, a while back, NetClock 9483/9489 MTBF is not "individually" calculated, since the NetClock 9400s are essentially the same as a "similar config" SecureSync.

SecureSync MTBF isn't calculated using the LCD/keypad, because these two items aren't considered essential for operation. So, the MTBF of a Model 9489 (no LCD/keypad and with a TCXO osc and commercial GNSS receiver) is essentially the same as a SecureSync with TCXO oscillator and commercial GNSS receiver (**1200-003**). There is no need to differentiate MTBF between SecureSyncs and 9400 NetClocks, because they are "the same product" (other than for Marketing purposes/feature sets).

Per Scott Holmes (Sept 2017) the MTBF for a 1200-003 is 130,589 hours in a Ground Benign, 25°C environment

"We are using new reliability prediction software and hiring a service to do much of this work for us. Last year I asked them to calculate reliability prediction for the 1200-213 and they found the MTBF for this configuration to be 130,589 Hrs in a Ground Benign, 25°C environment. You can safely use this number for both the 003 and 013. The values would rise a little with no DC and OCXO but not enough to make a significant difference"

Hi Dave Sohn,

Can you just confirm the MTBF value above in green is OK for Trevor to provide to his customer?

Update (8 Jan 2019) Dave S responded the value above (130,589 hours) is fine to provide to customers.

F) Model 9300 series data

The MIL-HDBK-217 MTBF for the complete units starts out at:

9383 w/OCXO = 30,285 hrs
 9383 w/TCXO = 31,911 hrs
 9383 w/Rb = 25,937 hrs

The complete front panel display board has an MTBF of 49,730 hrs. When this is removed the above numbers change to:

9383 w/OCXO = 77,454 hrs
 9383 w/TCXO = 89,062 hrs
 9383 w/Rb = 54,210 hrs

The worst components on the display board itself are the graphic displays at 50,022 hrs. The remaining components are in the 8 and 9 figure area.

The other major components on the board come out as follows:

GPS Resolution T receiver = 471,183 (Mil 217 number)

Advantech ETX Module = 669,059 (Bellcore number)

OCXO = 594,262 (Unknown method)

Rb = 138,532 (SpectraTime actual number)

Model 9389 MTBF

Note that the MTBF is based on the specific configuration of the Model 9389, including whether or not Option 02 (Front panel time display and one extra Remote and Serial port) is installed, and which oscillator is installed.

These numbers are based on MIL-HDBK-217 specifications.

MTBF for the Model 9389 with the front panel LCD Display Option (Option 2) installed:

Model 9389 with the OCXO oscillator (Option 05) installed = 30,285 hrs

Model 9389 with the TCXO oscillator installed = 31,911 hrs

Model 9389 with the Rubidium oscillator (Option 04) installed = 25,937 hrs

MTBF for the Model 9389 without the front panel LCD Display Option (Option 2) installed:

Model 9389 with the OCXO oscillator (Option 05) installed = 77,454 hrs

Model 9389 with the TCXO oscillator installed = 89,062 hrs

Model 9389 with the Rubidium oscillator (Option 04) installed = 54,210 hrs

MTBF for the Model 9388:

9388- If I remove the Res T Receiver from the 9383 w/TCXO and no front panel display, the reliability according to MIL-217 changes from 89,062 to 109,821 hours MTBF.

G) MTBF for the Model 8230 GPS antenna (replacement for the Model 8225):

- Refer to: [EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8230\MTBF](#)
- Can also refer to Arena
<https://files.bom.com/download/IYVIGpXhLdIgLlIqxKTikYBVNwE1BMlc/prbdckemrkaghoprdfiucgglitablxps/MTBF%20-%20Declaration%20-%20Orolia%20-%20Spectracom.pdf>

Email from Dave Lorah (10 Feb 2014, based on direction from John Fischer- John's email to Dave further below)
Hello Samantha,
I have some information for you regarding your request for MTBF on the Spectracom model 8230 GPS Antenna. These antennas have a very long calculated MTBF, way over **one million** hours. They have few semiconductors and are very reliable.

I have attached the MTBF calculations documents from the manufacturer Telcordia.

Email from John Fischer to Dave Lorah (10 Feb 2014) No, we should tell our customers this:

40 deg C, calculates to over 1 million hours. It only has a few active semiconductors in it, so it is quite reliable. The MTBF for this antenna, when calculated per Telecordia standards at

We should share the data calculations with them too.

Partial email from Scott Hildebrandt to Josh (5 Oct 17) I don't know if you received an answer back on your inquiry, but here is the information you are looking for

Product	MTBF
GNSS antenna model 8230	3,953,286 hours

H) MTBF for the Model 8227 inline GPS amplifiers

- Refer also to [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8227\MTBF](#)

Partial email from Scott Hildebrandt to Josh (5 Oct 17) I don't know if you received an answer back on your inquiry, but here is the information you are looking for

Product	MTBF
Preamplifier model 8227	250,000 hours

I) MTBF for the Model 8226 surge suppressors

- Refer also to [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\8230, 8225, 8225S, 8226, 8227 and grounding kit\8227\MTBF](#)

Partial email from Scott Hildebrandt to Josh (5 Oct 17) I don't know if you received an answer back on your inquiry, but here is the information you are looking for

Product	MTBF
Surge protector model 8226	2,530,000 hours

J) MTBF for the 8225:

- MTBF for the T-1000 (newer 8225) antenna from Cliff at Synergy (Forwarded 9/14/09 from Tom Richardson):

T-1000 MTBF

Date	Amount(a)	Days of usage(b)	Days used per month(c=a*b)
2009 Jan.	405	240	97200
Feb.	201	210	42210
Mar.	401	180	72180
Apr.	200	150	30000
May	302	120	36240
Jun.	4	90	360
Jul.	230	60	13800
Aug.	201	30	6030
Subtotal	1944	1080	298020

Year	RMA unit
2009	13

MTBF 91,698 hrs (=903780*0.7*12/13)
50% usage rate and used 8 hrs per day

K) MTBF for Model 8143 (distribution amp)

Email from Jim Allocco (6/8/11) Let's cap it at **100,000** hours. Our actual data might be a little hard to believe.

L) Epsilon Clock Equipment MTBF:

1. SAS-17E/SAS-36E

(Email from Sylvain on 11/2/10) The MTBF of the SAS 36E: 200,000 h (Per Laurent, it's the same for the SAS-36E, also).

3. SAS-17e-IR-AL

(Email from Laurent on 8/4/10): The MTBF of the SAS17E-IR-AL is estimated at 200 000 hours.

Email from Emmanuel (3/4/11) SAS MTBF: 200000 hours (MIL217F, 25°C, fixed grounded); Measured reliability from fielded units suggest a better MTBF.

Number of fielded units: more than 800 units in operation, including in broadcast applications where reliability is key.

Factory repair time: depends on support organization:

4. EC20S

(Email from Sylvain) I can give you the values for MTBF (calculated support: MIL HDBK 217 / 25°C, fixed, grounded criteria) 95000h

5. SASE

Email from Sylvain

I can give you the values for MTBF (calculated support: MIL HDBK 217 / 25°C, fixed, grounded criteria) :

EC20S: 95000h

SAS 17-E: 200 000h

6. EC22S

Email from Sylvain 6/14/11 *EC22S - Nowadays, we communicate with the 115 000h value but for already few years. I am going to check with the R&D team to check if the value can be updated with experience and feedback.*

Sigma/Standard Deviation (such as “one sigma”, “two sigma”, etc)

“One sigma” (1 sigma) for the 1PPS specs:

- Based on the “three-sigma rule”
- Refer to sites such as

http://en.wikipedia.org/wiki/Standard_deviation

http://en.wikipedia.org/wiki/68%E2%80%9393.95%E2%80%9399.7_rule

<http://math.stackexchange.com/questions/320370/how-to-calculate-standard-deviation-and-use-three-sigma-rule-for-couple-variable>

In [statistics](#), the **standard deviation (SD)** (represented by the Greek letter sigma, σ) is a measure that is used to quantify the amount of variation or [dispersion](#) of a set of data values.^[1] A standard deviation close to 0 indicates that the data points tend to be very close to the [mean](#) (also called the expected value) of the set, while a high standard deviation indicates that the data points are spread out over a wider range of values.

In [statistics](#), the so-called **68–95–99.7 rule** is a shorthand used to remember the percentage of values that lie within a band around the [mean](#) in a [normal distribution](#) with a width of one, two and three [standard deviations](#), respectively; more accurately, 68.27%, 95.45% and 99.73% of the values lie within one, two and three standard deviations of the mean, In the [empirical sciences](#) the so-called **three-sigma rule of thumb** expresses a conventional heuristic that "nearly all" values are taken to lie within three standard deviations of the mean, i.e. that it is empirically useful to treat 99.7% probability as "near certainty"

Sigma	Certainty	expected frequency outside of range
1 sigma	66.7%	1 in 3
2 sigma	95%	1 in 22
3 sigma	99%	1 in 370

IP rating/Ingress Protection rating (for all products)

- Refer to sites such as: <http://www.dsmt.com/resources/ip-rating-chart/>
- IP rating is an international protection classification for equipment. It specifies how safe the product is and how well it holds out solids and liquids. Example is: IP66

- **IP** at the beginning stands for “Ingress Protection”
- The **first number** after “IP” specifies **protection for persons and equipment** (such as holes in the product that allows a wire or dust to penetrate).

Level	Object size protected against	Effective against
0	Not protected	No protection against contact and ingress of objects
1	>50mm	Any large surface of the body, such as the back of the hand, but no protection against deliberate contact with a body part.
2	>12.5mm	Fingers or similar objects.
3	>2.5mm	Tools, thick wires, etc.
4	>1mm	Most wires, screws, etc.
5	Dust Protected	Ingress of dust is not entirely prevented, but it must not enter in sufficient quantity to interfere with the satisfactory operation of the equipment; complete protection against contact.
6	Dust Tight	No ingress of dust: complete protection against contact.

- The **second number** after “IP” indicates protection against **liquids**

Level	Object size protected against	Effective against
0	Not protected	–
1	Dripping water	Dripping water (vertically falling drops) shall have no harmful effect.
2	Dripping water when tilted up to 15°	Vertically dripping water shall have no harmful effect when the enclosure is tilted at an angle up to 15° from its normal position.
3	Spraying water	Water falling as a spray at any angle up to 60° from the vertical shall have no harmful effect.
4	Splashing water	Water splashing against the enclosure from any direction shall have no harmful effect.
5	Water jets	Water projected by a nozzle (6.3mm) against enclosure from any direction shall have no harmful effects.
6	Powerful water jets	Water projected in powerful jets (12.5mm nozzle) against the enclosure from any direction shall have no harmful effects.
7	Immersion up to 1m	Ingress of water in harmful quantity shall not be possible when the enclosure is immersed in water under defined conditions of pressure and time (up to 1 m of submersion).
8	Immersion beyond 1m	The equipment is suitable for continuous immersion in water under conditions which shall be specified by the manufacturer. Normally, this will mean that the equipment is hermetically sealed. However, with certain types of equipment, it can mean that water can enter but only in such a manner that it produces no harmful effects.

Sample breakdown for IP values of IP55 to IP69

		direction.
IP55	Protected from limited dust ingress.	Protected from low pressure water jets from any direction.
IP56	Protected from limited dust ingress.	Protected from high pressure water jets from any direction.
IP57	Protected from limited dust ingress.	Protected from immersion between 15 centimeters and 1 meter in depth.
IP58	Protected from limited dust ingress.	Protected from long term immersion up to a specified pressure.
IP60	Protected from total dust ingress.	Not protected from liquids.
IP61	Protected from total dust ingress.	Protected from condensation.
IP62	Protected from total dust ingress.	Protected from water spray less than 15 degrees from vertical.
IP63	Protected from total dust ingress.	Protected from water spray less than 60 degrees from vertical.
IP64	Protected from total dust ingress.	Protected from water spray from any direction.
IP65	Protected from total dust ingress.	Protected from low pressure water jets from any direction.
IP66	Protected from total dust ingress.	Protected from high pressure water jets from any direction.
IP67	Protected from total dust ingress.	Protected from immersion between 15 centimeters and 1 meter in depth.
IP68	Protected from total dust ingress.	Protected from long term immersion up to a specified pressure.
IP69K	Protected from total dust ingress.	Protected from steam-jet cleaning.

Refer to <http://www.duncansonline.ca/IP66.htm> for more information on IP66

- IP Rating for the newer “**NexTec FPLNFNFBP05**” Model 8226 is **IP68**
- IP rating for **SecureSync** is **IP30** (protected against objects larger than 2.5mm but no protection against liquids).
- IP rating of the **Model 9383/9389/9388** NTP time servers is **IP30**.
- IP rating for the **Synergy Timing 1000 (Model 8225)** antennas is **IP66**.
- IP rating for the **Model 8227 GPS preamp**: See info directly below.

(11/17/10) Tom Richardson checked with the vendor about this. The preamp meets the specs of **IP 66** but is not officially certified as IP 66.

Email sent to customer about this: “We received information back from the vendor of the Model 8227 GPS preamplifier. The manufacturer stated that the GPS preamplifier meets the specifications of IP 66 but is not officially certified as IP 66.

We always recommend the Model 8227 be installed indoors and after the location of the Model 8226 surge suppressor. However, if they are concerned by not having the IP 66 specification, they can wrap the entire preamplifier with our weather-proofing kit. This would be always be required if they were to install it outdoors.”

Power packs (for all products)

Note: Search Salesforce ("Products") for the applicable Part Number to see if we still offer a power pack

Note: Only the part numbers in green text are still available for purchase from Spectraco,

Model	Power supply	Output specs	Associated ancillary kit to sign out	Also known as	Was P/N	Cost (Have customer confirm with Admin)
SecureSync/9400s (for redundant "DC" input)	PS06R-2Z1M-DT01	(24vdc)	N/A	N/A	N/A	In salesforce at: https://orolia.my.salesforce.com/01tC00000039TX8?srPos=0&srKp=01t
SASe second DC input for redundant input power) (called "Special Item Timing – USA")	PS06R-2Z1M-DT03			N/A	N/A	In salesforce at: https://orolia.my.salesforce.com/01t1A000004Tz1l?srPos=0&srKp=01t
9383/9389/9388	PS06-0E0J-DT04	(12vdc)	1165-0000-0701	N/A	N/A	No longer available. See additional info further below “(PS06-0E0J-DT04)”
9383/9389 with Opt 4: Rb osc	PS06-0E1M-DT03	(24vdc)	1165-0000-0702	N/A	N/A	No longer available. See additional info further below “(PS06-0E0J-DT03)”
9383 with SP360	PS06-0E1M-DT03	(24vdc)	1165-0000-0704	N/A	N/A	No longer available. See additional info further below “(PS06-0E0J-DT03)”
9183/9189/9188/9283/9289/9288	PS06-0E0J-DTA0	(12vdc)	1122-0000-0701	T00060 PW118	PS06-0E1M-DT00 PS06-0E0J-DT01 (PW118/PW172) PS06-0E0J-DT03 PS06-0E0J-DTA0	Still available as of 18 March 2018 In salesforce at: https://orolia.my.salesforce.com/01t80000001ZbRU?srPos=0&srKp=01t
9183/9283/9289 with Opt 04:Rb	PS06-0E1M-DT00	(24vdc)	1142-0002-0701	T00061	PS06-0E1M-DT00	Still available as of 18 March 2018 In salesforce at: https://orolia.my.salesforce.com/01t80000001XYCj?srPos=0&srKp=01t
TTS200/TTS220	PS06-0E0J-DTA0	(12vdc)	1142-0001-0701	T00060	PS06-0E0J-DT01 (PW118/PW172) and PS06-0E0J-DT03	No longer available
TTS240Rb	1142-0002-0701	(24vdc)	1142-0002-0701	T00061	PS06-0E1M-DT00	Still available as of 18 March 2018 In salesforce at: https://orolia.my.sale

						sforce.com/01t80000001XYCj?srPos=0&srKp=01t
9175 (TV210W TV210V TV210U)	PS03-0T0J-WM01	Regulated 12v, 0.8A	1001-0000-0701	T00059		No longer available. See additional info further below "(PS03-0T0J-WM01)"
TV400W/TV400U/TV400V (no DIP switches on the rear panel)	PS06-0E0J-DTA0	12v, 1.5A	1122-0000-0701	T00060 PW118	PS06-0E0J-DT01 (PW118/PW172) PS06-0E0J-DT03	No longer available. See additional info further below (PS06-0E0J-DTA0
TV312	PS03-0T0J-WM01	Regulated 12v, 0.8A	1001-0000-0701	T00059	N/A	No longer available
TV400 (Model 8177 with DIP switches on the back panel)	T00058 (newer version of T00058 is US only, 100-240 VAC Universal Input, 12vdc output)	(12vdc unregulated output)	N/A	T00058	N/A	No longer available
8145, 8177 (TV400- not TV400W), 8183, 8183ES, 8185, 8188, 8189	T00058 (US only, 12vdc)	(12vdc unregulated output)	N/A	T00058	N/A	No longer available
PS00142 (International power supply for TV400- not TV400W), 8183, 8183ES, 8185, 8188, 8189	PS00142	(12vdc regulated output)	N/A	N/A	N/A	No longer available
TV230 (Model 8175)	PS03-0T0J-WM01? Was T00054. This power supply is discontinued/no longer available for purchase.		N/A	T00059	N/A	No longer available
8179T TimeTap	T00026				N/A	No longer available
8178T TimeTap	T00025				N/A	No longer available
DA-36 (Fiber distribution)	50-60-0195 (Refer to ECO-0787)					No longer available

8140VT (Opt 40) T00058 for 8145, 8183, 8183ES, 8185, 8188, 8189, etc

Model	Power Supply	Associated ancillary kit	Also Known as	Was P/N
8140VT (Opt 40) 8145, 8183, 8183ES, 8185, 8188, 8189	T00058 (US only, 12vdc) or PS00142 (Intl, 12vdc)	N/A	N/A	N/A

SecureSync (PS06R-2Z1M-DT01 for Second “DC” input for redundant AC input power)

Model	Power Supply	Associated ancillary kit	Also Known as	Was P/N
SecureSync	PS06R-2Z1M-DT01 (100 to 240VAC) (Released on ECN 2735)	N/A	N/A	N/A

SASe (PS06R-2Z1M-DT03 for second DC input for redundant input power) (called “Special Item Timing – USA”)

Model	Power Supply	Associated ancillary kit	Also Known as	Was P/N
SAS-17E and SAS-36E	PS06R-2Z1M-DT03 (released on ECN 2829)	N/A	N/A	N/A

EC1S-DC (Power supply 236293 = AC to DC converter for DC input)

Model	Power Supply	Output specs	Associated ancillary kit	Also Known as	Was P/N
EC1S	236293	(Note: 24vdc output – not compatible with all EC1S units)	N/A	N/A	N/A

PathAlignR External battery charger (15V 1A)

Model	Power Supply	Associated ancillary kit	Also Known as	Was P/N
PathAlign-R	PS08R-2Z0U-WM01	N/A	N/A	PEN6-1300-1005

Note: ECN 2968 changed PEN6-1300-1005 to PS08R-2Z0U-WM01 (July 2012)

Notes about various Power Packs

A) T00058 and PS00142 (12vdc) no longer available

- for Models such as the 8177 (TV400s), 8183s, 8189s,

Refer to:

- PS00142 (“international 50/60 Hz, 12vdc power supply)

Ault P/N: PW118RA1202F02 (this was a custom-made Power supply)

(“PS00142 Part Spec Record”) <I:\Engineering\Engineering Shared\Spectracom parts\PS00xxx>

Spectracom Part Specification Record						
REFERENCE DATA						
Spectracom Part Number: PS00142						
Description: INTERNATIONAL POWER SUPPLY PS, DT, SW, 100-250VAC, 12VDC, 1.5A						
Min Purchase Quantity: 1						
Manufacturer	Part #	Preference				
Ault	PW118RA1202F02	1				
PRICING HISTORY						
Date	PO	Vendor	Qty.	Part Number	Price	Lead Time
VENDOR INFORMATION						
Rep/Distributor	Salesperson	Phone	Email			
ADDITIONAL INFORMATION						
Custom power supply min. order applies.						
Input voltage	100-250 VAC					
Line Frequency	47 - 63 Hz					
Current	0.5A max at 90 VAC					
Output voltage	12 VDC					
Output current	1.5A					
Ripple	1% max					
Overcurrent/ short circuit protected						
Safety approvals	UL 60950-1					
CE Compliant						
Operating temperature	0 to 40 C					
Input connector	IEC320 w/ ground C14					
Output connector	Switchcraft 760 plug or equivalent					

- **T00058 (US-only 60 Hz, 12vdc power supply)**
 ("T00058 Part Spec Record") <I:\Engineering\Engineering Shared\Spectracom parts\Txxxxx>

Spectracom Part Specification Record						
REFERENCE DATA						
Spectracom Part Number: T00058						
Description: Wall Adapter, 12 VDC, 1A						
Min Purchase Quantity: 1						
Manufacturer	Part #	Preference				
Ault	P48121000A050G	1				
Stancor	STA-4812A	1				
PRICING HISTORY						
Date	PO	Vendor	Qty.	Part Number	Price	Lead Time
VENDOR INFORMATION						
Rep/Distributor	Salesperson	Phone	Email			
ADDITIONAL INFORMATION						
2.1 mm inside diam.						
5.5 mm outside diam.						
Positive shell/negative center						
For 8145, 8177, 8183, 8183ES, 8185, 8188, 8189, 8140VT-OPT40 (US only) 120 VAC - 12VDC, 60Hz, 1A, US only.						

DC output voltage

- **T00058** is 60 Hz input/12vdc **unregulated** power pack
- **PS00142** is 50/60 Hz input/12vdc **regulated** power supply

Output polarity

- Positive shell, negative center (this is commonly the opposite polarity of other power packs)

T00058 and PS00142 power packs are no longer available for purchase

- 8177s should be replaced by TV400W display clocks

Email from Sadie (9 Feb 16) This power supply has been deactivated in SFDC and is showing as "no longer available". I will no longer be quoting it. **Please** advise customers of that if they request it. The 8177 was last shipped in 2003.

Note: The Declaration of Conformity for the PS06R-2Z1M-DT01 power pack is included in the SecureSync's Declaration of Conformity Certificate.

Per Dave Sohn (15 Jun 15): it includes EN 60950-1:2006/A11:2009 for safety. We don't test to EN61000-6-1:2007 or EN 61000-6-3:2007, instead testing against EN 55022:2006/A1:2007 for Class A emissions, and EN55024:1998/A2:2003 for immunity.

C) PS06-0E0J-DT04 (12vdc) and PS06-0E1M-DT03 (24vdc) for 9383s

- Both these power packs are longer available from Spectracom

- 1. **PS06-0E0J-DT04 (12vdc supply for 9383/9389 with TCXO or OCXO oscillator)**
 - Not for use with a Rb oscillator installed
 - 12vdc out, 1.5A
 - Terminal block connector on end of power pack
 - The P/N for the raw power supply we purchase is **PS06-0E0J-DT04** (In Arena: https://app.bom.com/items/detail-spec?item_id=1202845985&version_id=10244006968&orb_msg_single_search_p=1https://app.bom.com/items/detail-bom?item_id=1202836866&version_id=10298327828)
 - Link to part spec record for **PS06-0E1M-DT01**: <I:\Engineering\Engineering Shared\Spectracom parts\PS06-0E0J-XXXX>)
 - The modified power supply P/N is **PS06-0E0J-DT04**
 - Link to drawing () to modify the raw power supply:

To verify the output of the 12vdc power pack

- To measure the 12 VDC. please use a DC voltmeter on the top of the terminal block



Replacement 12 vdc Power pack to replace a faulty one in the field

- These power supplies/power packs are no longer available from Spectracom.
- Can purchase locally a replacement 12vdc power pack and cut the ends off.
 - New one won't likely have a terminal block connector on the end. Can re-use the terminal block connector from the original power pack.

Part numbers for replacement/comparable power packs

- None listed in Arena (just need one with output of 12vdc, at least 1.5A)

2. PS06-01M-DT03 (24 vdc power supply for 9383/9389 with Rb oscillator)

Note: No longer available from Spectracom

- 24VDC out, 3.75A
- Terminal block connector on end of power pack
- The P/N for the raw power supply we purchased was **PS06-0E1M-DT01** (In Arena: https://app.bom.com/items/detail-bom?item_id=1202836866&version_id=10298327828)
 - Link to part spec record for PS06-0E1M-DT01: <I:\Engineering\Engineering Shared\Spectracom parts\PS06-0E1M-DT00>
- The modified power supply P/N is **PS06-0E1M-DT03**
- **Link to drawing (0300-1000-0012) to modify the raw power supply:** <I:\Engineering\Engineering Shared\Spectracom parts\PS06-0E1M-T00\PS06-0E1M-DT03rc>

To verify the output of the 24vdc power pack

- To measure the 24 VDC, please use a DC voltmeter

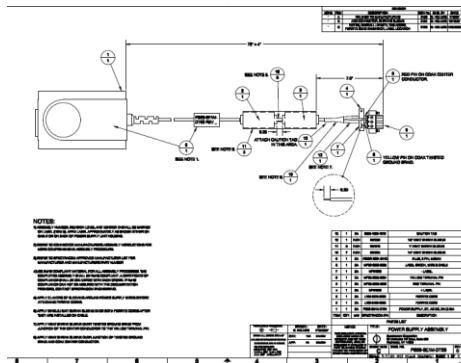


Replacement 24 vdc Power pack to replace a faulty one in the field

- These power supplies are no longer available from Spectracom.
- Can purchase locally a replacement 12vdc (or 24vdc for Rb osc) power pack and cut the ends off.
 - New one won't likely have a terminal block connector on the end. Can re-use the terminal block connector from the original power pack.

Part numbers for replacement/comparable power packs

- **(Mouser Electronics P/N 418-TRG70A24-V)**
<http://www.mouser.com/ProductDetail/Cincon/TRG70A240-11E03-Level-V/?qs=XuJNf8XTLBQJhEQdOLVUUw%3D%3D>
 - **XPPOWER P/N:** AEB70US24 http://www.newark.com/xp-power/aeb70us24/ac-dc-converter-external-plug/dp/77M9132?CMP=KNC-GUSA-GEN-KWL&mckv=|pcrid|190495088376|&gclid=EAlaIQobChMIh5PTsaSY1QIVUT2BCh1xCQI1EAAYAiAAEgLda_D_BwE
 - **Cincon P/N:** TRH70A240-21E02 (links to the Mouser 418-TRG70A24-V, the first item in this list)
<https://www.mouser.com/ProductDetail/Cincon/TRG70A240-11E03-Level-V/?qs=XuJNf8XTLBQJhEQdOLVUUw%3D%3D>
- **Link to drawing (0300-1000-0012) to modify the raw power supply:** <I:\Engineering\Engineering Shared\Spectracom parts\PS06-0E1M-DT00\PS06-0E1M-DT03rc>



D) PS06-0E0J-DTA0 / PS06-0E0J-DT01 (PW118/PW172 series) Power pack information (for TV400Ws for instance)

Note: Neither of these power packs are no longer available from Spectracom

Note: ECN 2264 replaced the PS06-0E0J-DT01 (PW118) and PS06-0E0J-DT03 with PS06-0E0J-DTA0.

Available directly from Digi-Key (Still available as of at least March, 2018): <http://www.digikey.com/>

- **Direct link:** <https://www.digikey.com/products/en?keywords=PW172KB1203F01>

PN: PW172 series (used to be PW118 series)

Full Ault P/N: PW172KB1203F01

<http://www.aultinc.com/products/smps/default.asp>

Link to power supply vendor data sheets: <I:\Engineering\Engineering Shared\Spectracom parts>

Link to the spec sheet ("PS06-0E0J-DTA0 Part Spec Record"): <I:\Engineering\Engineering Shared\Spectracom parts\PS06-0E0J-XXXX>

Input: 100-250VAC 50-60 Hz (Single-phase input only)

Output: 12vdc at 1.50 Amps

Note for replacement: This part was replaced in the 928x on ECN 1064 to the PS06-0E0J-DT03. The DT01 had a specialized right-angle connector so we had to buy large quantities whereas the DT03 is a straight-in connector enabling us to buy smaller quantities. Both are cross-compatible).

E) PS03-0T0J-WM01 (T00059- used to be T00054) for TV210W/TV312/TV230

Note: No longer available from Spectracom

Description: PS,SW,100-240VAC,2.5mm,RT ANG,12VDC,0.8A (female)

- Note the power pack needs to provide a regulated 12vdc output to the wall clock.. Using an unregulated output can potentially damage the display clock
- **Connector:** Power pack Must have female DC output connector with 2.5 mm center pin
- **Polarity** positive-center and negative-shell.

Refer to:

Part Spec Record (PS03-0T0J-WM01) <I:\Engineering\Engineering Shared\Spectracom parts\PS03-0T0J-WM01>
Excerpt below

Low Profile Part, with right angle DC output connector.

- Ault PW10 Mechanical dimensions 2.68"(68mm)L x 1.73"(44mm)W x 1.18"(30mm) H
- Ault PW117 Mechanical 3.35"(85mm)L x 1.81"(46mm)W x 1.30"(33mm)H
- Elpac WP1212 Mechanical 2.95"(75mm)L x 1.95"(49.5mm)W x 0.98"(25mm)H

Possible second source is Elpac WP1212-RA760. Need to obtain and test, or obtain copy of Elpac FCC test report. Vendors of Elpac are Digi-Key, Allied Electronics, Mouser, Newark, MPAQ, Power Plus, Electro-sonic.

Also identified Mean Well with a candidate part, the SW12U12, but needs a new part number for the right angle DC output connector **with 2.5 mm center pin instead of the standard SW12U12-P1I, which has straight DC output connector with 2.1 mm center pin.**

Email from Keith (29 May 18) Attached is a copy of the TV210W display clock user manual. Refer to Section 2.3 (pages 2.3 and Figure 2-4 which shows the polarity requirements) for information on the 12vdc power pack required for the TV210W.

Note the power pack needs to provide a regulated 12vdc output to the wall clock. Using an unregulated output can potentially damage the display clock. The minimum rating should be at least 0.8 amps.

The power connector is a Female connector with a 2.5mm center pin. Or the original connector can be re-used by splicing it onto the end of a new power pack. The polarity is positive-center and negative-shell.

Power pack connectors/info

- The Model 9183, 9283 and 9383 power packs use an AC line cord with an IEC 60320 (also known as IEC 320) /C14 connector. Refer to http://en.wikipedia.org/wiki/IEC_connector#C13_and_C14_connectors
- W01000 AC line cord included with the power packs
- Cord is 6 feet long
- It has a C13 plug on the end that plugs into the converter box with the other end of the line cord being a standard US three prong connector (NEMA 5-15 plug).
- Type of material for the "case" of the power pack: The case is polycarbonate.

Time Scales (UTC/GPS/TAI) for all products

- **Link to a great time scale converter on the Internet:** <http://tycho.usno.navy.mil/simpletime.html> (not the computer's time)

Chemicals (for all products)

F) Polychlorinated biphenyl (PCB)

- a synthetic organic chemical compound of **chlorine** attached to **biphenyl**, which is a molecule composed of **two benzene rings**

Q. Would you be able to provide any documentation to support that none of Spectracom's equipment has polychlorinated biphenyl (PCB) usage?

A Question was forwarded from Engineering to Justin to investigate.

REST API interface/Postman (alternate to using the standard web browser or CLI)

Note: For info on python script, refer to the next main section further below “Python program used to create or run scripts..”

- The REST API is available for Apache web browser products, such as SecureSync/9400s, 2400 SecureSyncs, 1232 VelaSyncs, VersaSyncs and VersaPNTs
- REST API /Postman collection on our website: <https://www.orolia.com/document/securesync-netclock-9400-rest-api-collection-and-documentation/>
- Here is a link to what we have for the REST API documentation in SecureSync: <https://files.spectracom.com/client-downloads/5820>
- Rons's Blog: <https://spectracom.com/resources/blog/ron-dries/2018/rest-api-powerful-interface-remote-control-pnt-devices>
- Refer also to documents (such as API guide) in: <\\rocfnp02\drive\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\REST API and Python scripts>
- allows for status and configuration data to be sent and retrieved without having to use the Web UI.
- uses the JSON data format when performing HTTP GET and POST operations

Refer to more particular REST API info for each product (such as SecureSyncs) in the applicable Tech Support document for that Product (search it for “REST API”)

Representational state transfer (REST) is an architectural style consisting of a coordinated set of architectural constraints applied to components, connectors, and data elements, within a distributed [hypermedia](#) system. REST ignores the details of component implementation and protocol syntax in order to focus on the roles of components, the constraints upon their interaction with other components, and their interpretation of significant data elements.^{[1][2]}

Blog by Ron Dries (“The REST API: A Powerful Interface for Remote Control of PNT Devices”)

- <https://spectracom.com/resources/blog/ron-dries/2018/rest-api-powerful-interface-remote-control-pnt-devices>

Monitoring and managing PNT devices that can be spread across the globe can be challenging. It is also necessary to ensure the devices are configured and running properly. In certain applications, there could also be the need to schedule a task or automate some functionality of a PNT device.

The built-in web GUI (Graphical User Interface) in Orolia products, such as the SecureSync and VersaSync, is designed to quickly and easily show status and provide configuration settings for users to manage their devices. It does, however, require the user to manually log in to the device and navigate to the desired web pages. This is not always practical and can be time consuming if multiple devices need to be monitored and managed at the same time.

But, by utilizing the built-in **REST (Representational State Transfer)** API, any functionality that can be done manually through the web GUI can also be scripted, allowing for machine-to-machine communication and control. The REST API utilizes JSON (JavaScript Object Notation) formatted data for sending commands and receiving status information from the devices.

One example of a task that can be simplified and automated using the REST API is downloading log and configuration bundles. The log and configuration bundles are important files to retrieve from a PNT device for troubleshooting issues or to determine how a PNT device has been running over time. Configuration bundles are also necessary to control the configuration of a PNT device, as well as to quickly configure multiple devices with the same configuration.

The REST API can simplify this task by automatically creating a script to go out to specified Orolia PNT devices and then saving the log and configuration bundles to a PC. This removes the need to manually log in to each device and download both files. Also, this process can be scheduled to download the configuration bundle periodically, which can be useful for controlling the configuration. Monitoring applications, like Nagios, can utilize python scripts using the REST API to create custom queries to pull the exact information from the device that they are interested in monitoring. After this status information is retrieved, a quick health report of the device can be shown in the tool. The REST API makes integration into existing monitoring tools easier.

The REST API is a powerful interface that can allow for more advanced remote control of PNT devices, and it can be utilized in a variety of different applications.

REST API/Postman documentation

Here is a link to what we have for the REST API documentation in SecureSync. <https://www.oriala.com/document/securesync-netclock-9400-rest-api-collection-and-documentation/>

Note this function requires software versions 5.4.5 and above be installed.

In summary: the REST API allows anything available via the browser to be scripted, using programs such as python.

The graphical Web User Interface ("Web UI") used with Spectracom's SecureSync and NetClock time servers has a built-in REST API which allows for status and configuration data to be sent and retrieved from the device without having to use the Web UI. This is useful for machine-to-machine communication, as well as for developing mobile apps. The REST API uses the JSON data format when performing HTTP GET and POST operations.

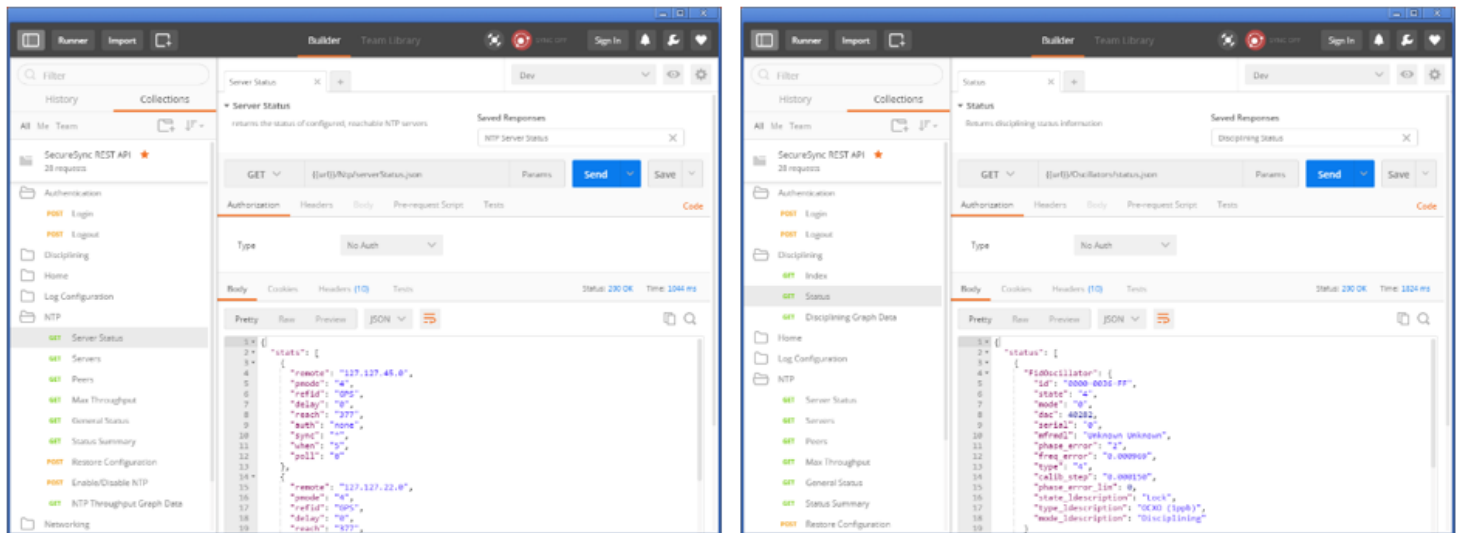
To perform these HTTP operations, it is necessary to know the data format required to retrieve and send data to SecureSync. Spectracom's Postman™ 1 collection is a compilation of frequently used operations which may serve as examples of how to pull and send data through the SecureSync API.

Representational state transfer (REST) is an architectural style consisting of a coordinated set of architectural constraints applied to components, connectors, and data elements, within a distributed [hypermedia](#) system. REST ignores the details of component implementation and protocol syntax in order to focus on the roles of components, the constraints upon their interaction with other components, and their interpretation of significant data elements.^{[1][2]}

OROLIA PROPRIETARY – COMPETITION SENSITIVE

REST API

Documented/Delivered as Postman Collection



Nagios®

General

[Home](#)
[Documentation](#)

Current Status

[Tactical Overview](#)
[Map \(Legacy\)](#)
[Hosts](#)
[Services](#)
[Host Groups](#)

Summary

Grid

[Service Groups](#)

Summary

Grid

[Problems](#)

Services

(Unhandled)

Hosts (Unhandled)

Network Outages

Quick Search:

Reports

[Availability](#)
[Trends \(Legacy\)](#)
[Alerts](#)

History

Summary

Histogram (Legacy)

[Notifications](#)
[Event Log](#)

System

[Comments](#)
[Downtime](#)
[Process Info](#)
[Performance Info](#)

Current Network Status

Last Updated: Tue Jan 26 09:50:52 EST 2016

Updated every 90 seconds

Nagios® Core™ 4.1.1 - www.nagios.org

Logged in as nagiosadmin

View History For This Host

View Notifications For This Host

View Service Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0

All Problems

All Types

0	1
---	---

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
8	1	0	0	0

All Problems

All Types

1	9
---	---

Service Status Details For Host 'eng-0016'

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
eng-0016	CPU	OK	01-26-2016 09:44:55	49d 17h 4m 31s	1/3	1 CPU, load 70.0% < 85% : OK
	DISK	OK	01-26-2016 09:44:35	49d 17h 5m 2s	1/3	/: 42%used(401MB/946MB) (<70%) : OK
	ETH	OK	01-26-2016 09:48:11	4d 0h 32m 30s	1/3	eth0:UP (0.7KBps/0.6KBps):1 UP: OK
	GNSS	WARNING	01-26-2016 09:41:55	4d 0h 45m 7s	3/3	GNSS Warning, Antenna Open - 15 satellites tracked
	HTTPS	OK	01-26-2016 09:45:55	49d 17h 13m 11s	1/4	HTTP/1.1 200 OK
	MEM	OK	01-26-2016 09:46:06	49d 17h 3m 40s	1/3	Ram : 33%, Swap : 0% : OK
	NTP	OK	01-26-2016 09:46:55	49d 17h 13m 30s	1/4	NTP OK: Offset 1.6459001 secs
	PING	OK	01-26-2016 09:49:55	49d 17h 11m 11s	1/4	PING OK - Packet loss = 0%, RTA = 0.25 ms
	SSH	OK	01-26-2016 09:49:45	49d 17h 13m 13s	1/4	SSH OK - OpenSSH_6.9p1-hpn14v5 (protocol 2.0)

Results 1 - 9 of 9 Matching Services

General info about REST API

The graphical Web User Interface ("Web UI") used with Spectracom's SecureSyncs (Model 1200 and 2400s) 9400 series NetClock time servers, 1232 Velasyncs, as well as VersaSyncs/VersaPNTs has a built-in REST API which allows for status and configuration data to be sent and retrieved from the device without having to use the Web UI. This is useful for machine-to-machine communication, as well as for developing mobile apps. The REST API uses the JSON data format when performing HTTP GET and POST operations.

To perform these HTTP operations, it is necessary to know the data format required to retrieve and send data to these various products. Spectracom's **Postman**™1 collection is a compilation of frequently used operations which may serve as examples of how to pull and send data through the SecureSync API.

Note: refer to **"Postman details"** further below

Scripts/Scripting using REST API

Customers often want to run scripts to retrieve data from SecureSyncs and other products. This isn't possible with the web browser itself. However (per Ron D) the REST API allows anything available via the browser to be scripted, using programs such as python.

Basic/summary Info about python

Note: refer also to the main **Python** section in this same document, just below this section about REST API.

<https://www.jetbrains.com/help/pycharm/step-1-creating-and-running-your-first-python-project.html>
available for Windows or Linux as a free install

Online tutorial: <https://docs.python.org/3.6/tutorial/appetite.html>

running a Python Script:

G) Copy the script file to the PC (such as in **c:/temp** for instance)

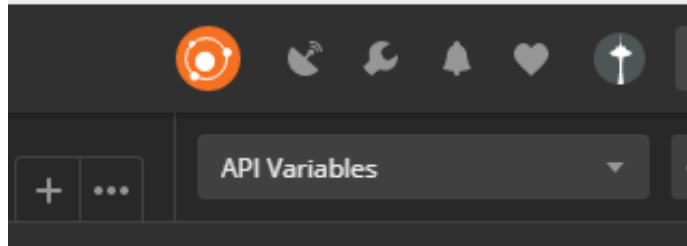
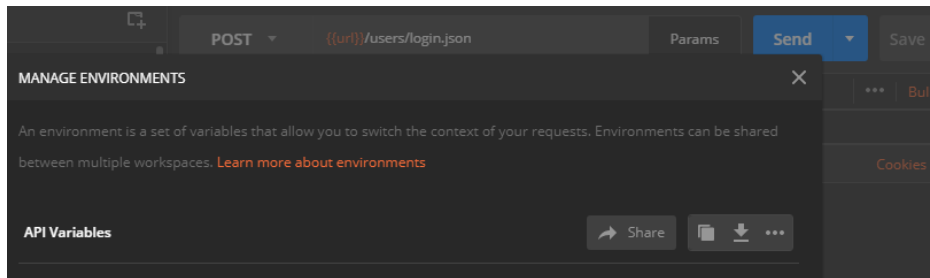
H) Open Windows command prompt window (**start -> run** and type **cmd**)

“To run the script, issue at the Windows command prompt the following command on a PC that has python installed (<https://www.python.org/downloads/release/python-352/>).

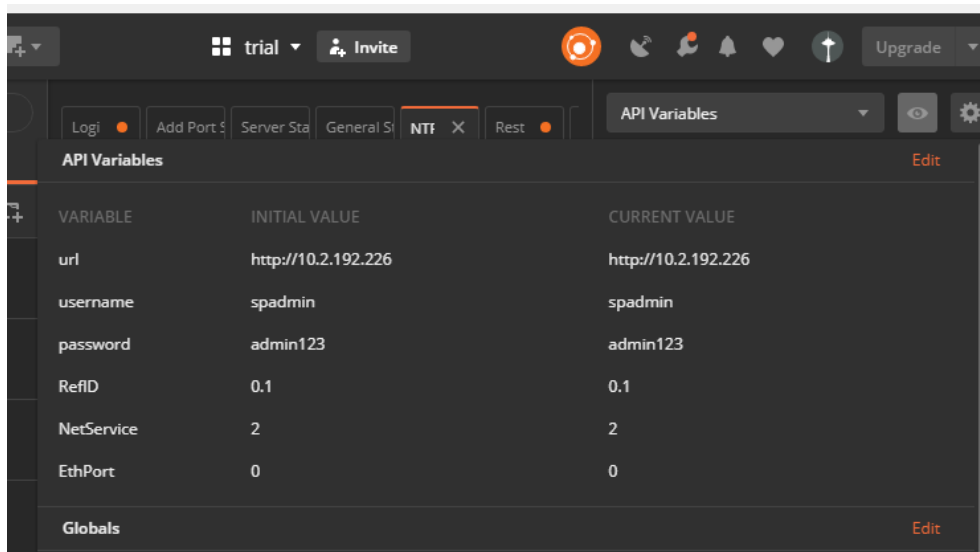
```
py query_ntp_stats_csv.py -H <SecureSync IP address> -u <username> -p <password>  
py query_ntp_stats_csv.py -H 10.2.192.226 -u spadmin -p admin123
```


Postman details

- Refer to “**Spectracom REST API Developer Guide**” (included in zip file and at: <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\REST API and Python scripts>)
- A) login to the Management => Network page of Apache device (such as the SecureSync) via its normal browser. Make sure “HTTP” service is enabled (it appears HTTP must be enabled for it to be compatible with postman)
- B) Open Postman installed on desktop of PC
- C) “Import the DEV environment”: Click the gear icon in upper-right corner, click import and select the file “API Variables.postman environment.json” file.
- D) API Variables” will be displayed in the middle and top-right side of the page (as shown below).



- E) In the Environment drop-down menu (next to the EYE button), select “Dev” to load the environment imported above.
- F) Click the EYE button (“Environment Quick look”) next to the gear icon, to see which environment variables have been loaded with this environment file: One variable is called url, another one is spadmin, etc.



- G) Click “Edit” (top-right) to change any/all the values (such as the URL/login credentials of the desired device). Then click “Update”.

API Variables		
VARIABLE	INITIAL VALUE	CURRENT VALUE
url	http://10.2.192.226	http://10.2.192.226
username	spadmin	spadmin
password	admin123	admin123
RefID	0.1	0.1
NetService	2	2
EthPort	0	0

H) To use a development variable, apply two curly brackets in the body code:



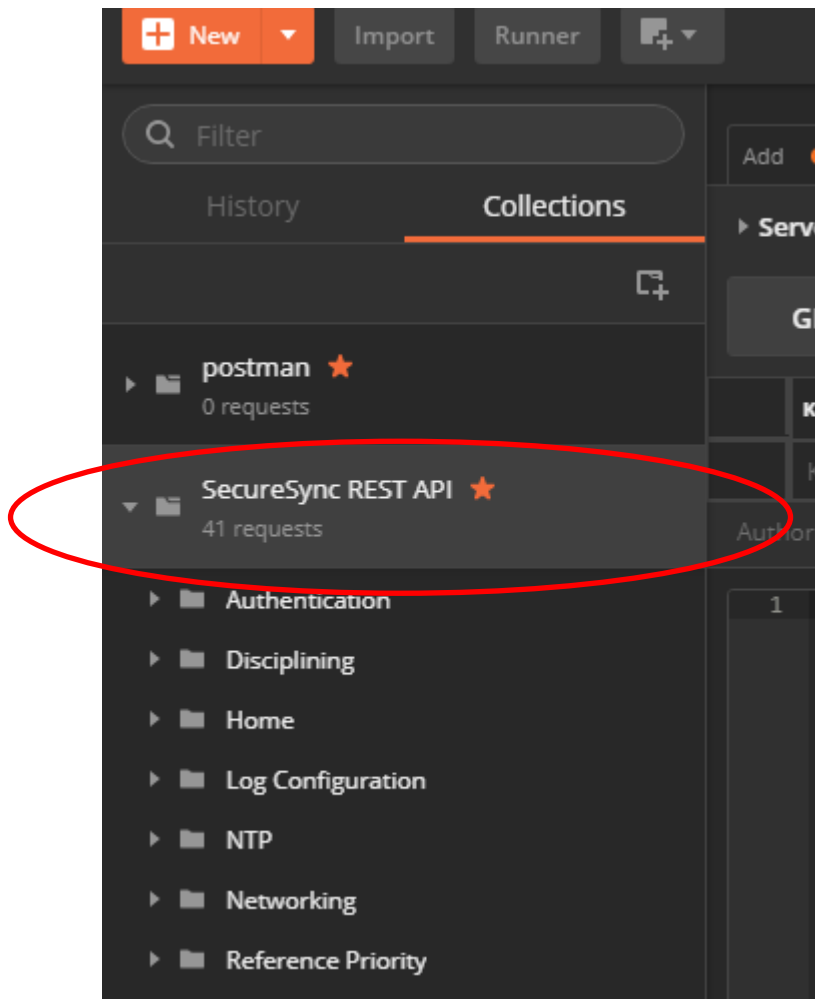
To test, click the blue **Send** button (top-right corner of the page). The coding window will display the requested code:

```

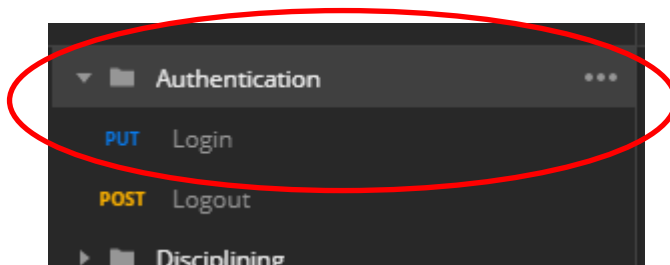
1: {
2:   "args": {},
3:   "data": "Quis possere augue vel cursus pharetra. In luctus a ex nec pretium. Praesent neque quam, tincidunt nec leo eget, rutrum vehicula magna.\\n\\nMorcenas consequat elementum elit, id semper sem tristique et. Integer pulvinar euismod quis consectetur interdum volutpat.",
4:   "files": {},
5:   "form": {},
6:   "headers": {
7:     "Host": "echo.getpostman.com",
8:     "Content-Length": "256",
9:     "Accept": "*/",
10:    "accept-encoding": "gzip, deflate, br",
11:    "accept-language": "en-US,en;q=0.8,de;q=0.6",
12:    "Cache-Control": "no-cache",
13:    "Content-Type": "text/plain",
14:    "Origin": "chrome-extension://fhbjghifrljldgggchcdhcnlddmmq",
15:    "Postman-Token": "7c1d1466-3d4e-6d58-63d2-403711314046",
16:    "User-Agent": "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.87 Safari/537.36",
17:    "x-forwarded-port": "344",
18:    "x-forwarded-proto": "https"
19:  },
20:   "json": null,
21:   "url": "https://echo.getpostman.com/post"
22: }
  
```

I) Login to the time server

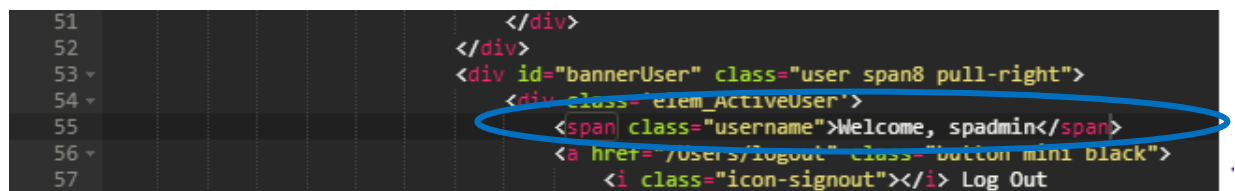
- On the **left-side** of the page, expand “**SecureSync REST API**”,



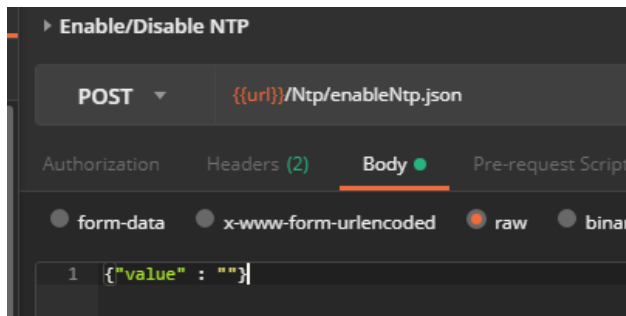
J) Expand and perform Authentication -> "Login" to the desired SecureSync. Press Send.



in the "Body -> Pretty" tab, scroll down about 53 lines and verify it indicates (in white text) "**Welcome, spadmin**". This confirms you are logged into the time server. No need to login again for each task desired to be performed



- K) For “Get” commands (cannot edit Get commands),
- L) Select the “**Body**” tab in the second main window down
- M) For “Post” commands (which allows edits of the values)
- N) Select the “**Body**” tab and select “**JSON**” in the drop-down (in the “**Pretty**” tab)
- O) Then select “**raw**” on the upper window to edit values (in yellow text).



Logout of the time server when done

- On the **left-side** of the page expand “**SecureSync REST API**”, expand and perform **Authentication** -> “**Logout**”. press the send button to the desired SecureSync
 - scroll down about 53 lines and verify it indicates (in white text) “

Specific examples where REST API can be used

- refer to: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\REST API and Python scripts\Python scripts](#)

A) 10 MHZ and 1PPS outputs

- Refer to Salesforce case 25034

Q We have a customer (BAE in Los Angeles) that wants to turn on and off the 10 MHz and 1PPS outputs using the CLI. It appears we have the command for 1PPS **ppscrtl**, but I didn’t see one for 10 MHz – is there one

A Email from Dave S (12 Apr 17) These configurations can also be adjusted via the REST API that we are continuing to document. Any 1PPS or 10MHz in the system could be controlled in this way.

B) Download GPS status info

- “Here is a simple python script (without error checking) to login and extract the GPS information and put it in a csv file.”

Apparent Issues associated with REST API

SecureSyncs/NetClock 9400s

1. 500 web UI error

- Fixed in Version 5.7.0 [JIRA ticket SSS-262] – “500 web UI error with REST API”

About Postman

Postman is an HTTP client that serves as a development app to prototype and test APIs. As of December 2016, the Postman app is available for Google Chrome™, or as native apps for Microsoft Windows™, Mac OS X or later, and Linux: <https://www.getpostman.com/apps>.

Postman can be used to send the requests to a SecureSync or NetClock unit, and it will return the JSON response from the device. The JSON response is formatted in a clean and legible format that is useful for understanding each of the API calls. This allows to quickly test API calls without having to develop test software, and the format of the data returned can be easily analyzed for inclusion into scripts or applications that can consume the data.

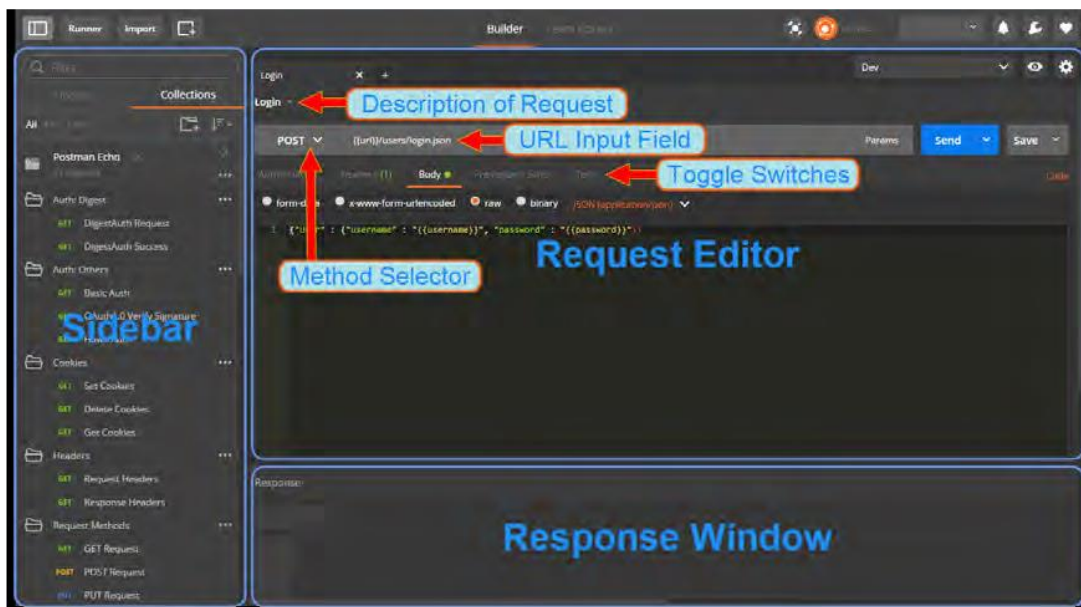
Downloading and Installing the Postman™ Chrome™ App

1. Install the Google Chrome web browser.
2. Navigate to <https://www.getpostman.com/apps>, and select "Download Postman for Chrome".
3. Click ADD TO CHROME.
4. Once the Chrome App Launcher has opened, click the Postman app icon to open Postman.
5. Create an account by signing up. This will ensure your requests, collections, environments, and history data are saved for future reference.
6. The app will open.

Familiarizing Yourself with Postman

The following is a brief overview of the Postman UI. More comprehensive assistance can be found under <https://www.getpostman.com/docs>.

The Sidebar lists the requests stored in the loaded Collections (see "Spectracom REST API Developer Guide" on the previous page), and – under the History tab – a list of recently submitted requests.



The Sidebar lists the requests stored in the loaded Collections (see "Spectracom REST API Developer Guide" on the previous page), and – under the History tab – a list of recently submitted requests.

Postman functionality highlights:

Create requests by conveniently specifying Method, URL parameters, Header and Body.
Submit API calls quickly to test scripts; generate code snippets that can be copied and pasted.

Specify authorization to be used.

Display responses in different formats e.g., "pretty", "raw", or as rendered HTML pages.

Organize and store requests in Collections.

Store request parameters that will be used repeatedly (e.g., keys and values used as login credentials) in development project-specific Environments.

Access history of sent requests.

Capture documentation for requests in a description field.

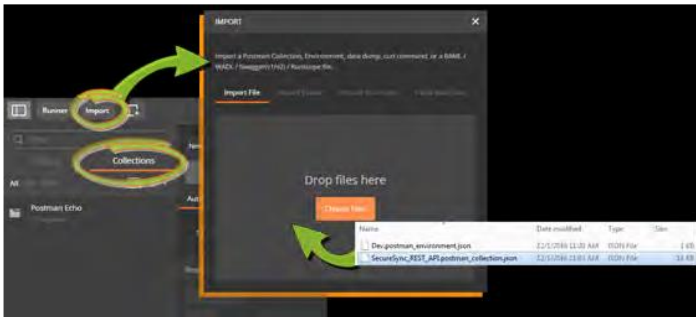
Importing the Spectracom Collection

Spectracom's Postman™ collection provides examples of how to pull and send data through the API.

To import this collection:

1. Unzip the Spectracom REST API kit to a local directory of your choice.
2. Unzip the kit files to a local directory of your choice.
3. Open the Postman app, using the credentials of your previously created account.
4. Import the SecureSync REST API Collection:
 - a. With the Google Chrome app, click the Import button at the top left corner of the screen. For the standalone app, click the Collection menu option on the top of the screen, then select Import.

➤ Navigate to Collections > Import: Choose File.



- c. From the zip folder created in step 2, select the file `SecureSync_REST_API.postman_collection.json`, and open it. Under the Collections tab in the Sidebar on the left, SecureSync REST API will be displayed. Click on it to display the Collection's folders which reflects the menu structure of the SecureSync Web UI e.g., Networking, Log Configuration, NTP, etc. Each folder contains requests.

Click on any request to display it in the Request Editor.

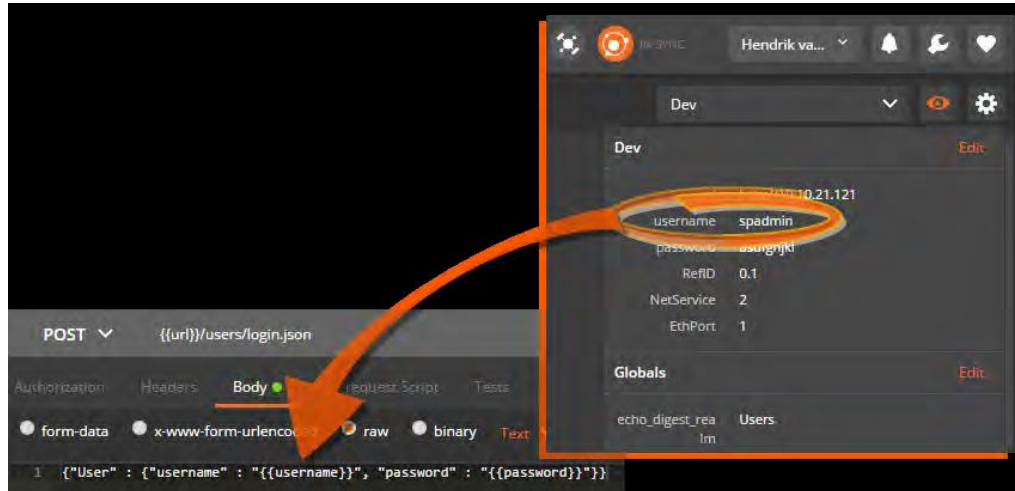
Importing the DEV Environment

The Development Environment includes a selection of variables/parameters that are frequently used when interacting with a SecureSync unit via the API.

To import the Development Environment:

1. In Postman, click the GEAR button on the right, and select Manage Environments.
2. Click Import, navigate to the folder in which you unzipped the Spectracom API Developer Kit files, and select the file `Dev.postman_environment.json`.

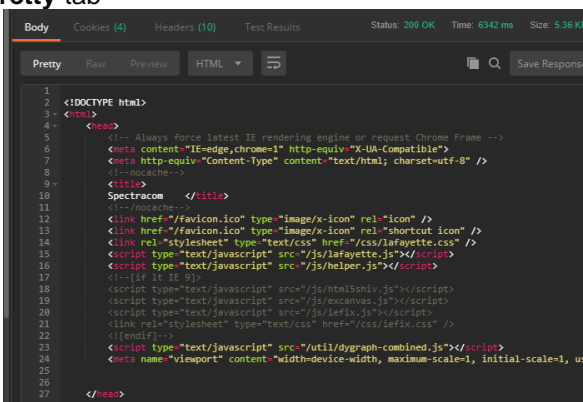
3. In the Environment drop-down menu (next to the EYE button), select Dev to load the environment imported above.
4. Click the EYE button to see which environment variables have been loaded with this envr file: One variable is called url, another one is spadmin, etc. To use a development variable, apply two curly brackets in the body code:



To test, click the blue Send button. The coding window will display the requested code:



Pretty tab

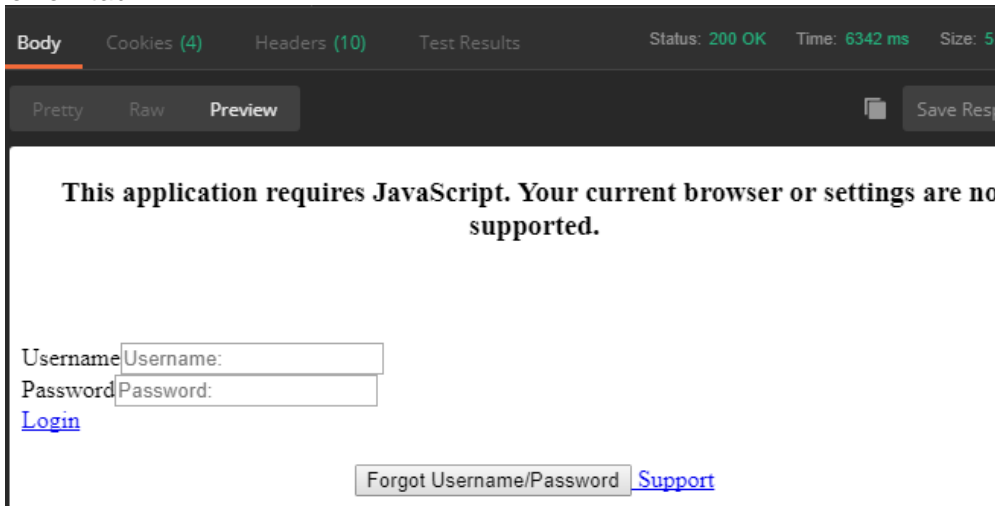


Raw tab

```
Body Cookies (4) Headers (10) Test Results Status: 200 OK Time: 6342 ms Size: 5.36 KB
Pretty Raw Previous Save Response

<!DOCTYPE html>
<html>
<head>
<!-- Always force latest IE rendering engine or request Chrome Frame -->
<meta content="IE=edge,chrome=1" http-equiv="X-UA-Compatible">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<!--nocache-->
<title>
Spectracore
</title>
<!--/nocache-->
<link href="/favicon.ico" type="image/x-icon" rel="icon" />
<link href="/favicon.ico" type="image/x-icon" rel="shortcut icon" />
<link rel="stylesheet" type="text/css" href="/css/lafayette.css" />
<script type="text/javascript" src="/js/lafayette.js"></script>
<script type="text/javascript" src="/js/helper.js"></script>
<!-- If it is a -->
<script type="text/javascript" src="/js/htabohiv.js"></script>
<script type="text/javascript" src="/js/scanas.js"></script>
<script type="text/javascript" src="/js/iefix.js"></script>
<link rel="stylesheet" type="text/css" href="/css/iefix.css" />
</script>
<script type="text/javascript" src="/util/dygraph.combined.js"></script>
<meta name="viewport" content="width=device-width, maximum-scale=1, initial-scale=1, user-scalable=0">
</head>
<body>
<div class="container-fluid page-container">
<!--nocache-->
<script type="text/javascript">(function(){document).ready(function(){});</script>
<!--/nocache-->
<noscript>center<h3>This application requires JavaScript. Your current browser or settings are not supported.</h3></center></noscript>
</body>
</html>
```

Preview tab

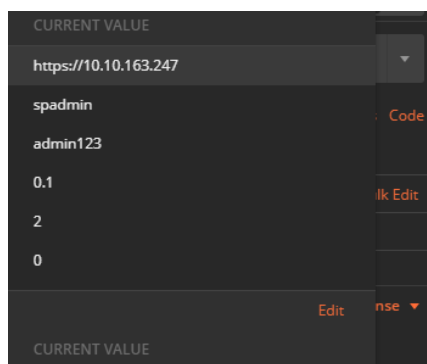


- **GET:** Whenever a user accesses a page, the View component issues a GET request to the Controller, since the user ultimately wants to retrieve (or: GET) the data that is displayed on the loaded page
- **SET/POST:** If, however, a user wants to add or configure a setting, the View component will issue a SET (or: POST) request to the Controller. In both cases, the Controller will receive the request, decide which operation to apply (CRUD), and then forwards the processed request to the Model, which will execute the request

REST API login to a device:

- Can login using either HTTP or HTTPS

When logging in with HTTP, make sure the HTTP service is enabled in the device



Python program used to create or run scripts/script files

- Refer also to (in SecureSync folder): [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\REST API and Python scripts\Python scripts](#)
- **Websites/tutorial with info on using Python to create scripts:** <https://docs.python.org/3.6/tutorial/logging-in-with-serial-interpret.html>
- Python scripts can be used in conjunction with the REST API interface in products such as SecureSyncs/9400s to script anything that can be performed in the unit's standard web browser.
- Free download for linux or Windows

A) Python on Linux

The Python interpreter is usually installed as /usr/local/bin/python3.6 on those machines where it is available; putting /usr/local/bin in your Unix shell's search path makes it possible to start it by typing the command: **python3.6** to the shell. [1] Since the choice of the directory where the interpreter lives is an installation option, other places are possible; check with your local Python guru or system administrator. (E.g., /usr/local/python is a popular alternative location.)

B) Python on Windows

- Refer to sites such as: https://www.infoworld.com/article/3505957/python-and-windows-get-cozier.html?utm_source=Adestra&utm_medium=email&utm_content=Title%3A%20Python%20and%20Windows%20get%20cozier&utm_campaign=IDG%20Insider&utm_term=Editorial%20-%20IDG%20Insider&utm_date=20191220152133
- Download Python: (<https://www.python.org/downloads/release/python-352/>).

On Windows machines, the Python installation is usually placed in **C:\Python36**, though you can change this when you're running the installer. To add this directory to your path, you can type the following command into the command prompt in a DOS box:

Shortcut to Python.exe [C:\Users\kwing\AppData\Local\Programs\Python\Python36-32\python.exe](#)

Online Tutorial: <https://docs.python.org/3.6/tutorial/interpreter.html>

Example scripts for SecureSync/9400s

- Refer to: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\REST API and Python scripts\Python scripts](#)

A) getting raw qual log

```
import json
import requests
import csv

# variables
SecureSync = "http://10.2.100.177" # SecureSync to query
User = "spadmin" # username
Pass = "admin123" # password
File = "gpsStatusLog.csv" # data filename
```



```

class SecureSyncInst:

    def get_gps_status_log(self):
        global Session

r = Session.get(SecureSync + "/logs/gpsStatusLog.json")

    with open(File, 'wb+') as f:
        dict_writer = csv.DictWriter(f, fieldnames=['id', 'feature_id', 'sys_timestamp',
'sats_tracked', 'avg_tracked_snr', 'max_tracked_snr', 'min_tracked_snr'])
        dict_writer.writeheader()
        dict_writer.writerows(r.json())

    def login(self, user, password):
        global Session

Session = requests.Session()

        # Login to SecureSync
        payload = {'User': {'username' : user, 'password': password } }
        r = Session.post(SecureSync + "/Users/login/index.json", json=payload,
verify=False)

    def logout(self):
        global Session

        # logout of SecureSync
        r = Session.post(SecureSync + "/Users/logout", verify=False)

if __name__ == '__main__':

    engine = SecureSyncInst()

    engine.login(User, Pass)

    engine.get_gps_status_log()

    engine.logout()

```

B) Example of getting NTP throughput data (viewed with codewriter)

Per your earlier request for the SecureSyncs to be able to automatically export NTP data, one of our engineers has created an example Python script for you, which uses the SecureSync REST API to retrieve the NTP stats from the SecureSync.

This script logs in to a SecureSync and requests the NTP stats. The stats are printed to the command terminal, and they are also saved to a file in the directory the script is run from (called "ntp_stats.csv"). This allows the stats data to be opened directly in Excel.

To run the script, issue at the Windows command prompt the following command on a PC that has python installed (<https://www.python.org/downloads/release/python-352/>).

`python query_ntp_stats_csv.py -H <SecureSync IP address> -u <username> -p <password>`

for our SecureSync, this becomes: `python query_ntp_stats_csv.py -H 10.2.100.176 -u admin -p admin123`

```
#!/usr/bin/env python

import requests
import sys
import parser
import argparse
from threading import Timer

VERSION_STRING = "0.0.1a"

ENDPOINT = "/Logs/getGraphStatus/LogNtpStat.csv"
args = {}

def main():
    global args

    requests.packages.urllib3.disable_warnings()

    parser = argparse.ArgumentParser(description='Process cli arguments.')

    parser.add_argument("-H", "--hostname", dest='hostname', action='store',
                        default="10.10.201.1", type=str, help="hostname of target server")
    parser.add_argument("-t", "--timeout", dest='timeout', action='store', type=int,
                        help="timeout for the operations in seconds")
    parser.add_argument("-V", "--version", action='version', version=VERSION_STRING,
                        help="show the plugin version and exit")
    parser.add_argument("-u", "--username", dest="username", action="store",
                        default="spadmin", type=str, help="SecureSync username")
    parser.add_argument("-p", "--password", dest="password", action="store",
                        default="admin123", type=str, help="SecureSync password")

    args = parser.parse_args()

    if args.timeout:
        t = Timer(int(args.timeout), timeout_exit)
        t.start()

    browser = requests.Session()

    results = call_json_endpoint(browser, ENDPOINT)

    if results:
        print(results.text)
        create_csv(results)
    else:
        print("Request failure")

def timeout_exit():
    print_results("Timeout", exit_status=3)

def create_csv(results):
    f = open('ntp_stats.csv', 'w')
    f.write(results.text)
    f.close()
```



```

def login_post(browser):
    browser.post("https://" + args.hostname + "/Users/login.json", json={"User" :
{"username" : args.username, "password" : args.password}}, verify=False)

def call_json_endpoint(browser, endpoint, attempts = 5):
    """
    Calls a JSON endpoint on the server
    Attempts a default of 5 times, on the 5th attempt it
    returns a empty json.
    """

    results = browser.get("https://" + args.hostname + endpoint, verify=False)

    if(results.url == ("https://" + args.hostname + "/users/login")):
        if(attempts == 0):
            return {}
            login_post(browser)

        return call_json_endpoint(browser, endpoint, attempts -1)
    else:
        return results

if __name__ == '__main__':
    main()

```


COMPLIANCY (for all products)

**UL and CE Testing / Declarations of Conformity statements (for all products)

A) UL - EMI/EMC testing

STD IEC 62236-4 re I/O port Surge test (surge test of the RF input to a GNSS receiver)

- Refer to Salesforce case 24513
- Testing needs to be performed with a Model 8226 or equivalent GPS surge suppressor attached to the RF input connector of the unit under test (UUT).
- Connecting a surge generator directly to the RF input is highly likely to damage the GNSS receiver.

	Environmental phenomena	Test specification	Basic standard	Test set-up	Remarks	Pe
2.1	Radio-frequency common mode	0.15 MHz to 80 MHz 10 V (p.m.s.) 80 % AM, 1 kHz	Unmodulated carrier	IEC 61000-4-6 IEC 61000-4-6	See Notes 1, 2 and 5 The test level specified is the c.m.s. value of the unmodulated carrier	
2.2	Fast transients	±2 kV 500 ns 5 kHz	Peak 3/1/1 Repetition frequency	IEC 61000-4-4 IEC 61000-4-4	See Note 1 Capacitive clamp used	
2.3	Surges	±2 / 50 / 5 ±2 kV ±1 kV	Open circuit test: voltage, line to earth Open circuit test: voltage, line to line	IEC 61000-4-5 IEC 61000-4-5	See Notes 1, 3 and 4	

NOTE 1: This test applies to I/O port connected to cable inside 5 m boundary or connected to cable longer than 30 m within 10 m boundary.
I/O ports connected to cable other than those should comply with the requirements of IEC 61000-4-2 except that Note 2 of Table 2 of IEC 61000-4-2 is not applicable.

NOTE 2: Applicable only to ports interfacing with cables whose total length according to the manufacturer's specification may exceed 5 m.

NOTE 3: This test is intended to replicate the phenomenon known as direct coupling; hence an output impedance of 42 Ω (per 15 and 2.0 generator) and a 40 V or less are recommended.

NOTE 4: For telecommunication ports and other ports intended for connection to highly balanced pairs, a line to line test is not required.

NOTE 5: The test level can also be defined as the equivalent current into a 150 Ω load.

Question from Customer: The question to the GPS clock vendor is per note 4 of the standard (highlighted above), if the GPS antenna coax RF connection can be considered as “telecommunication port or its input is highly balanced pairs”, then this surge test on the RF input port of the clock is not required.

Reply from Keith to customer (based on direct input from Tom Richardson, 22 Feb 17) Thanks for your email pertaining to EMI/EMC testing of the SecureSync. I have some info for you which should help with your testing.

In summary, it is imperative that a GPS surge suppressor (such as the Spectracom Model 8226 surge suppressor) first be connected directly to the SecureSync's RF input connector (via a minimum of about a 10 foot length of coax cable), and for this surge suppressor to be connected to ground. The EMI/EMC testing should then be performed on the “antenna” side of the Model 8226 (not on the SecureSyncs connector directly). Inducing a surge to the RF input connector of the SecureSync with no surge protector connected between the surge generator and the SecureSync is almost certain to result in non-warranty damage to the SecureSync's GPS receiver and possibly to other components inside the SecureSync.

The SecureSync's GPS/RF input connector is not considered a telecom port. The surge suppressor mentioned above which is highly recommended to be installed on all SecureSyncs having a connection to an antenna is intended to help protect the SecureSync from surges on the antenna cabling. Note that the “42 ohms” referenced in the spec is the output impedance of the Surge generator (not the SecureSync) in use for the conducted testing.

Please contact the Spectracom Sales team if you need to obtain a Model 8226 surge suppressor before performing the desired testing.

B) Declarations of Conformity

- EMI testing and EMC testing –refer to the applicable CE Declaration of Conformity for the particular product

All products

- Link to UL Certificates (expand “Certificate”)

<https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/products/SecureSync/default.aspx>

GSG GPS simulators

<https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/products/gsg/default.aspx>

SecureSyncs (expand “Certificate”)

<https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/products/SecureSync/default.aspx>

TSync-PCle (under “certificate”)

<https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/products/TSync/default.aspx>

Q. could you please tell me if this item complies to any safety specifications such as UL 60950

A. Email from Dave S: There is a CE safety certification for the TSync, but not UL. (also in [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\Timing boards\TSYNC-PCle\Agency-CE approval](#))

NetClocks (9400s and 9300s are in two different sections on this page)

<https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/products/NetClock/default.aspx>

TPRO/TSAT boards

<https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/products/tprotsat/default.aspx>

MIL-STD-461 (ELECTROMAGNETIC INTERFERENCE CHARACTERISTICS)

- Refer to <https://en.wikipedia.org/wiki/MIL-STD-461>

MIL-STD-461^[1] is a [United States Military Standard](#) that describes how to test equipment for [electromagnetic compatibility](#).

Various revisions of MIL-STD-461 have been released. Many military contracts require compliance to MIL-STD-461E. The latest revision (as of 2015) is known as "MIL-STD-461G".^[2]

While MIL-STD-461 compliance is technically not required outside the US military, many civilian organizations also use this document.^[3]

Electromagnetic compatibility test labs typically set up their [anechoic chamber](#) to comply with MIL-STD-461. Test labs attempt to comply with this standard for two reasons

A) For SecureSync

- Refer also to (MIL-STD-461) in: [..\SecureSync CustAssist.pdf](#)

Q It is not mentioned in the Datasheet that SecureSync is compliant with MIL-STD-461. However, in every EMC Test reports available in Arena, it mentioned by Chomerics Test Services that:

Chomerics test facility operates under the current revision of Chomerics Quality Assurance (QA) Manual Document Number QA002.

The QA Manual has been constructed to reflect a quality program in accordance with the requirements of the National Institute of Standards and Technology (NIST), ISO 9002, ISO 17025, ISO Guide 25, NIST Handbook 150, EN 45001, MIL-I-45208A, MIL-STD-461D, 462D and Chomerics Quality Assurance Program (QAP).

The QA Manual outlines and describes the procedures for establishing and maintaining the quality of analysis, research, inspection, and testing within Chomerics Test Service (CTS).

This test report does not represent an endorsement by the U.S. Government.

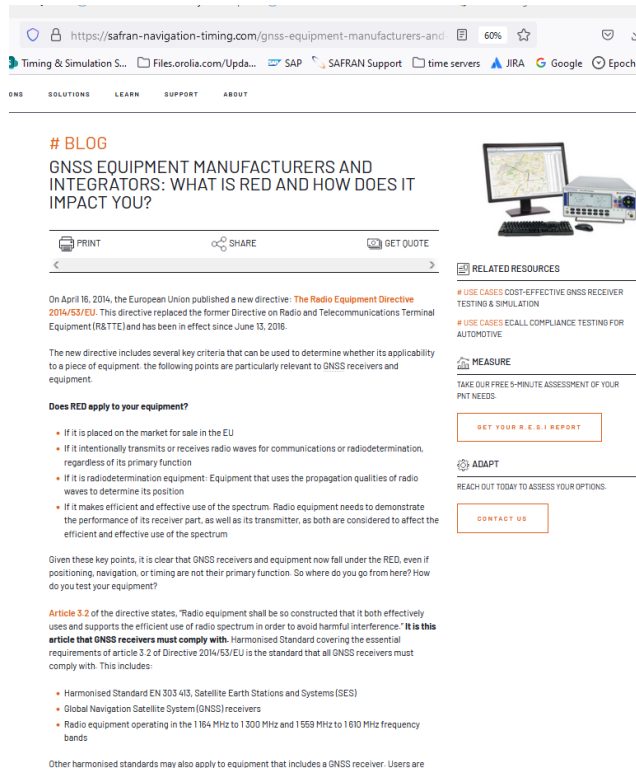
The results and/or conclusions within this test report refer and/or apply only to the unit(s) tested as defined by this report.

Measurements performed for this test are traceable to the National Institute of Standards and Technology (NIST) based on the fact that all test equipment used for the measurements were previously calibrated using standards traceable to NIST.

A reply from Dave Sohn (27 May 2019) SecureSync is not compliant with MIL-STD-461. The test house, Chomerics, is capable of testing to that standard, which is why they list that in their documentation.

Article 3.2 of the EU Radio Equipment Directive (RED) / ETSI EN 303 417: Wireless power transmission systems (WPT)

- Refer to Salesforce Case 300857
- Refer to sites such as
 - Blog on our website: <https://safran-navigation-timing.com/gnss-equipment-manufacturers-and-integrators-what-is-red-and-how-does-it-impact-you/> (excerpt below)



- https://www.etsi.org/deliver/etsi_en/303400_303499/303417/01.01.01_30/en_303417v010101v.pdf (excerpts below)

1 Scope

The present document specifies technical characteristics and methods of measurements for wireless power transmission (WPT) systems, using technologies other than radio frequency beam, in the 19 - 21 kHz, 59 - 61 kHz, 79 - 90 kHz, 100 - 300 kHz, 6 765 - 6 795 kHz ranges.

The present document covers wireless power transmission systems which are regarded as radio equipment since including inherent radio communication functionality or radiodetermination via the WPT interface or port at the specific WPT frequency ranges.

Such systems usually consist of:

- 1) A power transmitter, with additional communication capability to control the charge function, in conjunction with the receiving part. The power transmitter could also be named as base station.
- 2) A power receiver, which supplies the received energy to a mobile device and performs a control/supervision function for the mobile device status and charge operation. Both parts in combination are able to transmit and receive data in addition to the power transmission mode e.g. to control the mobile device status and to optimize the power transmission mode.

These radio equipment types are capable of operating in the permitted frequency bands below 30 MHz as specified in Table 1.

The present document covers fixed systems, mobile and portable systems.

Table 1: WPT systems within the permitted frequency bands below 30 MHz

WPT frequency range Frequency Bands Applications

Transmit and Receive 1 19 kHz to 21 kHz WPT systems

Transmit and Receive 2 59 kHz to 61 kHz WPT systems

Transmit and Receive 3 79 kHz to 90 kHz WPT systems

Transmit and Receive

100 kHz to 119 kHz WPT systems

Transmit and Receive 119 kHz to 140 kHz WPT systems

Transmit and Receive 140 kHz to 148,5 kHz WPT systems

Transmit and Receive 148,5 kHz to 300 kHz WPT systems

Transmit and Receive 5 6 765 kHz to 6 795 kHz WPT systems

NOTE 1: The frequency ranges listed in Table 1 are also used for generic inductive short range devices, according to ETSI EN 300 330 [1].

NOTE 2: The limits and the frequency ranges of the present document are EU wide harmonised according to EC Decision 2013/752/EU [i.2] and ERC/REC 70-03 [i.1].

NOTE 3: In addition, it should be noted that other frequency bands may be available in a country within the frequency range below 30 MHz

4.2.1 Background information

In this clause all general considerations for the testing of wireless power transmission (WPT) systems using technologies other than radio frequency beam in the 19 - 21 kHz, 59 - 61 kHz, 79 - 90 kHz, 100 - 300 kHz, 6 765 - 6 795 kHz ranges are given. The tests cover all different operational modes, as described in clause 4.2.3.

4.2.2 Wanted performance criteria

A WPT system always consists of a base station and a mobile device which are in proximity to each other. The performance of a WPT system is dependent on the related operational mode, see clause 4.2.3.

For the purpose of the receiver performance tests, the WPT system shall produce an appropriate output under normal conditions as indicated below:

- use as intended without degradation of performance; or
- a degradation of the performance is indicated by the WPT system as described in the manual.

The manufacturer shall declare the performance criteria used to determine the performance of the receiving parts inside the WPT system (related to the mode)

ISO 8601 (ISO-8601) compliancy (internationally accepted way to represent dates and times)

- Refer to sites such as https://en.wikipedia.org/wiki/ISO_8601 and <http://www.iso.org/iso/home/standards/iso8601.htm>
- ISO 8601 describes an internationally accepted way to represent dates and times using numbers.
- ISO 8601 tackles this uncertainty (of using various methods to indicate date/time) by setting out an internationally agreed way to represent dates: **YYYY-MM-DD**

When dates are represented with numbers they can be interpreted in different ways. For example, 01/05/12 could mean January 5, 2012, or May 1, 2012. On an individual level this uncertainty can be very frustrating, in a business context it can be very expensive. Organizing meetings and deliveries, writing contracts and buying airplane tickets can be very difficult when the date is unclear.

ISO 8601 tackles this uncertainty by setting out an internationally agreed way to represent dates: **YYYY-MM-DD**

For example, September 27, 2012 is represented as 2012-09-27.

A) SecureSyncs/9400s

- **Web browser date/time display:** does use this particular formatting
- **Front panel date/time display:** does not use this particular formatting
- **ASCII output:** Formats 0, 1, 2 and 3 do not use this particular formatting
- **NTP/PTP:** does not use this particular formatting
- **Sylog logs:** (per Dave S, The syslog timestamps that are in our logs are not ISO 8601 compliant)

To begin, the SecureSync can display and output time/date info in several places/ways, such as on its front panel, in its web browser, in the units logs, via NTP and also via various optional Option Cards that can be installed to receive and/or output date/time using various methods (PTP, ASCII, IRIG, Havequick, etc).

The SecureSync's web browser reported date format IS compliant with ISO 8601. But the vast majority of outputs available from the SecureSync are not ISO 8601 compliant. So I would recommend indicating in the survey you received that the SecureSync isn't ISO 8601 compliant (note that many of these limitations are due to the protocols that SecureSync supports and not a limitation of the SecureSync itself).

****DISA/STIG (Security Technical Implementation Guide) for all products**

Email from Bill Glase (3/5/12)

Leisa, if it helps you can send them a copy of our CIP-7 Security Report (on our internal network [here](#)) as an example of the security assessments we do. It is not a STIG compliance statement though.

<https://login.microsoftonline.com/ppsecure/post.srf?wa=wsignin1%2E0&rpsnv=2&ct=1333973817&rver=6%2E1%2E6206%2E0&wp=MBI&wreply=https%3A%2F%2Fwww1877%2Esharepoint%2Ecom%2F%5Flayouts%2Flanding%2Easpx%3FSource%3Dhttps%253A%252F%252Forliagroupemeamicrosoftonlinecom%252D1%252Esharepoint%252Eemea%252Emicrosoftonline%252Ecom%252F%255Fforms%252Fdefault%252Easpx&lc=1033&id=500046&cbcxt=mai&wldp=1&gues t=1&bk=1333973817>

Email from Paul Myers (3/5/12)

NOTE: We support NTP which is good.

NTP security has NOT been an issue so far, but I doubt we meet any STIG if it describes security.

Our NTP Supports security which includes Symmetric Keys and a single configuration of the AUTOKEY 'IFF protocol'. Our AUTOKEY implementation is the most basic and supports IFF Group and Client Keys. We only support RSA keys and MD5 hash.

This is NOT likely the preferred method and we don't use a FIPS OpenSSL if that is require

Email from Paul Myers (3/5/12) I don't believe we support the Military Key Distribution schemes. Otherwise, Mark Goodlein would have pointed this out in his research of the STIGS.

I can report what we currently support. NOT compliance to specific STIGs as Mark Goodlein did this research.

In regards to SSH:

- We do not support any "Certificates" for SSH.
- SSH uses Public Keys.
- We allow the user to Load Public keys via the Web UI.
- The current public keys can be added to by adding text at the end of the list or by replacing entirely what is there.
- The user can create a single or list of public keys into the web browser.
- The number of public keys typically corresponds to 1 key per user. I was able to load a several key file.
- Public key length depends on the number of bits in the key and key type. A key file is typically 1-2Kbytes in my experience, but STIG compliant keys could be longer????
- Our code does not limit the length of the key file. SSH does not limit the number of public keys that I am aware of.
- A bug seems to exist in the Web UI which can cause the Web UI to fail to return after loading a LARGE key file of several kilobytes. The key file is loaded, but the connection is lost. I tried to load a 10Kbyte keyfile and the file was loaded, but I had to reconnect to the web ui. This will be investigated.

In regards to HTTPS:

- Certificates are used for HTTPS sessions. We only support the following.
- Loading x509 PEM certificates from the Web UI – Default for APACHE web server
- We support the user loading Public Keys via FTP by specific filename and then selecting then enabling that certificate for use using the WebUI
- This could be improved on with a better web UI but so far no one has complained or even used it I believe.
- We convert the following certificates from these types identified by file name to the x509 PEM used by Apache
- FTP a file named cert.pem which means x509 PEM
- FTP a file named cert.der which means x509 DER
- FTP a file named certpem.p7c which means PKCS7 PEM
- FTP a file named certder.p7c which means PKCS7 DER

CIP/Cyber Security/Potential Vulnerabilities/Anti-virus software

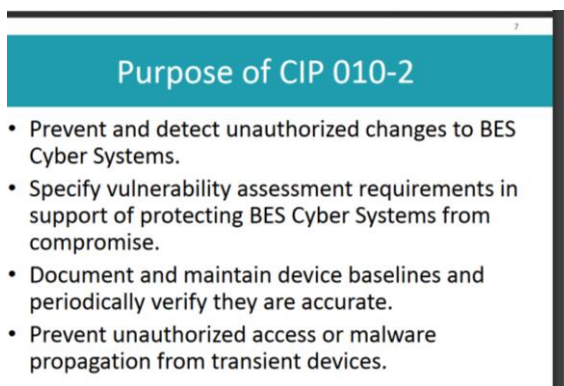
CIP (Critical Infrastructure Protection) for NERC (North American Electric Reliability Corporation)

- Refer to <http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>
- List of various Standards for the **Power industry/Power grid**

A) CIP-010 (CIP-10) (“Cyber Security- Configuration Change Management and Vulnerability Assessments”)

- Refer to http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-010-2&title=Cyber%20Security%20-%20Configuration%20Change%20Management%20and%20Vulnerability%20Assessments&jurisdiction=null

From: <https://www.wecc.biz/Administrative/07%20-%20CIP-010-2%20-%20Christensen.pdf>



Q (per SF case 126907) Do you have a list of commands at the CLI level to pull a configuration baseline to satisfy CIP-010 compliance?

A Per Ron Dries (19 Feb 18) Taking a look at CIP-010 it does not appear to state explicitly what the configuration baseline has to be. Also this appears to be mainly a way to track device configuration and changes made to it.

<https://www.cimcor.com/blog/achieving-nerc-cip-10-compliance-with-file-integrity-monitoring>

Potentially having the customer save a configuration bundle from the SecureSync might be enough, using the saveconf command.

B) CIP-007 (CIP-7) (“Cyber Security - System Security Management”)

- Refer to http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-007-6&title=Cyber%20Security%20-%20System%20Security%20Management&jurisdiction=null
- Refer to “**SecureSync-CIP007-Security-Compliance-Report.pdf**” at the following link: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Security- Vulnerabilities](#)

From Dave Sohn to Matt Loomis (13 Mar 2013) We had put together a NERC CIP-007 document for SecureSync some time ago. This might help the customer.

In general, we take in security vulnerability reports from our own scanning, from customers, and from vulnerability databases. Generally, these are handled within our quarterly releases. We try to provide workarounds in the mean-time, however, if necessary, we can do an out of band release to resolve.

Note: Refer to the link above for the document Dave is referring to.

****Information Assurance (IA) / Common Criteria (CC) / EAL levels**

- Sounds similar to FIPS, but FIPS is a government security standard while IA appears to be an International standard.

EAL (Evaluation Assurance Level)

Per Google

An Evaluation Assurance Level (EAL) is a category ranking assigned to an IT product or system after a [Common Criteria security evaluation](#). The level indicates to what extent the product or system was tested.

from https://en.wikipedia.org/wiki/Evaluation_Assurance_Level

The **Evaluation Assurance Level** (EAL1 through EAL7) of an IT product or system is a numerical grade assigned following the completion of a [Common Criteria](#) security evaluation, an [international standard](#) in effect since 1999. The increasing assurance levels reflect added assurance requirements that must be met to achieve Common Criteria certification. The intent of the higher levels is to provide higher confidence that the system's principal security features are reliably implemented. The EAL level does not measure the security of the system itself, it simply states at what level the system was tested.

To achieve a particular EAL, the computer system must meet specific *assurance requirements*. Most of these requirements involve design documentation, design analysis, functional testing, or penetration testing. The higher EALs involve more detailed documentation, analysis, and testing than the lower ones. Achieving a higher EAL certification generally costs more money and takes more time than achieving a lower one. The EAL number assigned to a certified system indicates that the system completed all requirements for that level.

*Note the EAL levels in the following table are described in more detail at the link further above):

EAL Level	Description
EAL 1	Functionally tested
EAL 2	Structurally tested
EAL 3	Methodically tested and checked
EAL 4	Methodically designed, tested and reviewed
EAL 5	Semi-formally designed and tested
EAL 6	Semi-formally verified design and tested
EAL 7	Formally verified design and tested

Information assurance (IA)

from Wikipedia:

Information assurance (IA) is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. While focused dominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form. Information assurance as a field has grown from the practice of [information security](#) which in turn grew out of practices and procedures of [computer security](#).

From Wikipedia:

The **Common Criteria for Information Technology Security Evaluation** (abbreviated as **Common Criteria** or **CC**) is an [international standard](#) (ISO/IEC 15408) for [computer security](#) certification. It is currently in version 3.1.^[1] Common Criteria is a framework in which computer system users can *specify* their security *functional* and *assurance* requirements, vendors can then *implement* and/or make claims about the security attributes of their products, and testing laboratories can *evaluate* the products to determine if they actually meet the claims. In other words, **Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security**

product has been conducted in a rigorous and standard manner.

Update/more email reply from Dave Sohn regarding the email below that Tony had sent back in 2012 (I had asked him if this earlier email still applies today, 12 Oct, 16): Yes. We have not done any analysis or certification against Common Criteria standards (EALs).

Email from Tony Diflorio to a customer (8/3/12)

We do not have a formal IA certification, but have evaluated the SecureSync against industry standards such as CIP-7, and HIPAA.

We regularly scan the product for security vulnerabilities using a commercial assessment tool.

The CC Eval does not typically apply to a product that is providing "Time" over a network. So, the answer is "not evaluated". Please let us know if you need further information.

Scada Systems

Refer to sites such as: <http://www.cimatic.com/blog/bid/190307/What-is-SCADA-Anyway>

SCADA is the system responsible for monitoring a technical process and, in some cases, controlling and optimizing those processes. Through these systems, human operators monitor and control input and output values related to safe and efficient operations from one central location, regularly acquiring data that allows supervision of industrial controls in real (or near real) time.

Terms

- **SCADA Stands for:** Supervisory Control and Data Acquisition (SCADA)
- **HMI:** Human Machine Interfaces

Points / Data Points To the application developer the network represents itself as a set of elementary data elements, called data points (or simply points). These data points are the logical representation of the underlying physical process, which control network nodes drive or measure. Each node can be associated with one or more data points. In the logical view each data point represents a single datum of the application. It can correspond to an aspect of the real world (such as a certain room temperature or the state of a switch) or be of more abstract nature (e.g., a temperature set point). The data points are connected through a directed graph, distinguishing output points and input points. The application is defined by this graph and a set of processing rules describing the interactions caused by the change of a point value. The logical links which this graph defines can be entirely different from the physical connections between the nodes.

Telcordia GR-63-CORE (NEBS Earthquake/seismic-related enclosures)

- Refer to “Telcordia GR-63-CORE” in the Custserviceassist doc <I:\Customer Service\1- Cust Assist documents\CustomerServiceAssistance.pdf>

Y2k38 (year 2038 rollover) (“Unix Millennium Bug”)

From Wikipedia (https://en.wikipedia.org/wiki/Year_2038_problem)

The **Year 2038 problem** is an issue for computing and data storage situations in which time values are stored or calculated as a [signed 32-bit integer](#), and this number is interpreted as the number of seconds since 00:00:00 [UTC](#) on 1 January 1970 ("the [epoch](#)").^[1] Such implementations cannot encode times after 03:14:07 UTC on 19 January 2038, a problem similar to but not entirely analogous to the "[Y2K problem](#)" (also known as the "Millennium Bug"), in which 2-digit values representing the number of years since 1900 could not encode the year 2000 or later. Most [32-bit Unix-like](#) systems store and manipulate time in this "[Unix time](#)" format, so the year 2038 problem is sometimes referred to as the "**Unix Millennium Bug**" by association.

Associated Spectracom products

A) SecureSyncs/VersaSyncs

- Refer to the ‘ResT_Yeatest.xlsx’ spreadsheet referenced below: [I:\Customer Service\GPS\Y2k38 \(year 2038\)](I:\Customer Service\GPS\Y2k38 (year 2038))

Email from Paul Myers (25 Apr 16) The 2038 Problem is that times are stored as a signed 32-bit integer and if the number of seconds since 1 Jan 1970 00:00:00 UTC rolls over as an EPOCH 03:14:07 UTC on 19 January 2038.

Our KTS Timing system is 32 bit and counts time in seconds. Our code supports a based year of 1970. However, we accept input years up to 2099, and perform calculations using 64-bit arithmetic.

The Gentoo and other Linux distributions should be addressing these issues; however we need to pay attention that our filesystem even addresses this because dates in the file system can be stored in 32-bit format.

I think we need to test the 2038 rollover for KTS impact.

However, the issue we will face is that the RES-T receivers will have issues before then based on testing I had Mary Catherine perform, in 2025 and later depending on the RES-T firmware year.

B) NetClock 9300 and 9200 series

- Refer to the “ResT_Yeatest.xlsx” spreadsheet: [I:\Customer Service\GPS\Y2k38 \(year 2038\)](I:\Customer Service\GPS\Y2k38 (year 2038))

C) 1232 Velasync

D) VersaSync/VersaPNT

E) Legacy VelaSync

Voluntary Product Accessibility Template (VPAT) Section 508 form / Form 508 of The Rehabilitation Act (for people with disabilities: Blind, hearing impaired. etc)

- The form is called “**Voluntary Product Accessibility Template (VPAT)**”.
- Refer to Salesforce Cases such as **208201**

Q What is Section 508 compliance?

A In 1998 the US Congress amended the Rehabilitation Act to require Federal agencies to make their electronic and information technology accessible to people with disabilities. **Section 508** was enacted to eliminate barriers in information technology, to make available new opportunities for people with disabilities, and to encourage development of technologies that will help achieve these goals.

We claim exception from this form:

Email from Sadie Nedo (11 Sept 2019) We do not have a VPAT. We take the following exception to Section 508:

Exception in 1194.3 (f) applies to our products:

(f) Products located in spaces frequented only by service personnel for maintenance, repair, or occasional monitoring of equipment are not required to comply with this part.

NETWORK RELATED (for all products)

**Static IP addresses assigned to Customer Service/Tech Support

- 10.2.100.170 through 10.2.100.179 (See list below)

10.2.100.170 Assigned to Eth1 of bottom server for Radius server interface
10.2.100.171 Assigned to our Legacy VelaSync
10.2.100.172
10.2.100.173 Assigned to the 1204-32 GB PTP card (located in .176)
10.2.100.174
10.2.100.175
10.2.100.176 Assigned to Eth0 of the **top** time server in our rack
10.2.100.177 Assigned to Eth0 of the **bottom** time server in our rack
10.2.100.178 Keith tried assigning to SAS-17E in rack (18 Feb 2014)
10.2.100.179

Assigning a temporary static address using MAC address (arp)

From the Model 9489 manual:

From a Windows Operating System

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

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

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

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

From a UNIX or GNU/Linux Operating System:

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

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

3-4

NetClock 94xx Instruction Manual, Rev G

Spectracom

NetClock 9400 Series

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

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

*nslookup (DNS lookup of hostnames/IP addresses)

- Run **nslookup** in a command prompt window to query DNS servers
- Refer to sites such as: <http://linux.die.net/man/1/nslookup>

*netstat commands

Function: Shows network connections, routing tables, network status

<https://www.tecmint.com/find-open-ports-in-linux/>

To list all open ports or currently running ports including TCP and UDP in Linux, we will use **netstat**, is a powerful tool for monitoring network connections and statistics.

```

List All Network Ports Using Netstat Command

$ netstat -ltnu
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp    0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:22              :::*                    LISTEN
tcp    0      0 0.0.0.0:80              :::*                    LISTEN
tcp    0      0 0.0.0.0:25              :::*                    LISTEN
udp    0      0 0.0.0.0:68              0.0.0.0:*

```

Where,

- **-l** - prints only listening sockets
- **-n** - shows port number
- **-t** - enables listing of tcp ports
- **-u** - enables listing of udp ports

- just type “**netstat**”, or can optionally add various combinations of switches (list together)
- For more parameters and info, refer to: <http://en.wikipedia.org/wiki/Netstat> and <https://www.tecmint.com/20-netstat-commands-for-linux-network-management/>

-a	Displays a ll active connections and the TCP and UDP p orts on which the computer is listening.
-b (Windows)	Displays the b inary (executable) program's name involved in creating each connection or listening port. (Windows XP, 2003 Server and newer Windows operating systems; not Microsoft Windows 2000 or older).
-b (macOS, NetBSD)	Causes -i to report the total number of b ytes of traffic.
-e	Displays e thernet statistics, such as the number of b ytes and packets sent and received. This parameter can be combined with -s .
-f (Windows)	Displays f ully qualified domain names <FQDN> for foreign addresses (only available on Windows Vista and newer operating systems).
-f Address Family (FreeBSD)	Limits display to a particular socket address family, unix , inet , inet6
-g	Displays multicast g roup membership information for both IPv4 and IPv6 (may only be available on newer operating systems)
-i	Displays network interfaces and their statistics (not available under Windows)
-m	Displays the m emory statistics for the networking code (STREAMS statistics on Solaris).
-n	Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.
-o (Windows)	Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the P rocesses tab in Windows Task Manager. This parameter can be combined with -a , -n , and -p . This parameter is available on Microsoft Windows XP, 2003 Server (and Windows 2000 if a hotfix is applied). ^[6]
-p protocol (Windows and BSD)	Shows connections for the p rotocol specified by <i>protocol</i> . In this case, <i>protocol</i> can be tcp , udp , tcpv6 , or udpv6 . If this parameter is used with -s to display statistics by protocol, <i>protocol</i> can be tcp , udp , icmp , ip , tcpv6 , udpv6 , icmpv6 , or ip v6.
-p (Linux)	Show which p rocesses are using which sockets (similar to -b under Windows) (you must be root to do this)
-P protocol (Solaris)	Shows connections for the p rotocol specified by <i>protocol</i> . In this case, <i>protocol</i> can be ip , ip v6, icmp , icmpv6 , igmp , udp , tcp , or rawip .
-r	Displays the contents of the I P r outing t able. (This is equivalent to the rout e p rint command under Windows.)
-s	Displays s tatistics by protocol. By default, statistics are shown for the T CP, U DP, I CMP, and I P protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over I Pv6, UDP over I Pv6, I CMpv6, and I Pv6 protocols. The -p parameter can be used to specify a set of protocols.
-t (Linux)	Display only TCP connections.
-W (FreeBSD)	Display wide output - doesn't truncate hostnames or IPv6 addresses
-v (Windows)	When used in conjunction with -b it will display the sequence of components involved in creating the connection or listening port for all executables.
Interval	Redisplays the selected information every Interval seconds. Press CTRL+C to stop the redisplay. If this parameter is omitted, netstat prints the selected information only once.

Function: Shows network connections, routing tables, network status


```

[spadmin@Spectracom ~]$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:42504         localhost:agentx        ESTABLISHED
tcp        0      0 localhost:agentx        localhost:42504         ESTABLISHED
tcp        0      0 10.2.100.3:telnet      pm-wing2.int.oro.li:4685 ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags               Type                   State
unix    2      [ ] DGRAM               1074 Cudevdev
unix   10      [ ] DGRAM               1214 /dev/log
unix    2      [ ] DGRAM               284693006
unix    2      [ ] DGRAM               260818169
unix    2      [ ] DGRAM               1907
unix    2      [ ] DGRAM               1660
unix    2      [ ] DGRAM               1547
unix    2      [ ] DGRAM               1486
unix    2      [ ] DGRAM               1398
unix    2      [ ] DGRAM               1229
[spadmin@Spectracom ~]$

```

Netstat -a (Shows Eth0, Eth1, Eth2 and Eth3, if 1204-06 card is installed)

- Displays all connections and listening ports.

Netstat -i (Shows Eth0, Eth1, Eth2 and Eth3, if 1204-06 card is installed)

The best way to determine if this is the issue being observed is to either telnet or SSH into any other Ethernet port that is still responding. After logging in, issue the **netstat -i** (as in the letter “eye”) command. In the response, there is a counter for each Ethernet connection for all received packets that have been dropped (these counters reset after each boot-up). This value should normally always be a “0”. But if this potential issue happens to occur, this number will begin to increment, while that port remains unresponsive (the screenshot shows the results of this command with all Ethernet ports responding to packets).

```

[spadmin@Spectracom ~]$ netstat -i
Kernel Interface table
Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0 1500 0 010660886 1 0 0 871517 0 0 0 0 BMRU
eth1 1500 0 3748182 0 0 0 4752 0 0 0 0 BMU
eth2 1500 0 31 0 0 0 0 0 0 0 0 BMU
eth3 1500 0 6552909 0 0 0 333 0 0 0 0 BMRU
lo 16436 0 024382172 0 0 0 024382172 0 0 0 0 LRU
[spadmin@Spectracom ~]$

```

Netstat -i -d (Shows received and dropped packets on all four ports)

```

[spadmin@Spectracom ~]$ netstat -i -d
Kernel Interface table
Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0 1500 0 010661696 1 0 0 871605 0 0 0 0 BMRU
eth1 1500 0 3748182 0 0 0 4752 0 0 0 0 BMU
eth2 1500 0 31 0 0 0 0 0 0 0 0 BMU
eth3 1500 0 6553586 0 0 0 333 0 0 0 0 BMRU
lo 16436 0 024382982 0 0 0 024382982 0 0 0 0 LRU
[spadmin@Spectracom ~]$

```

netstat -nr

- “-n” Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.
- “-r” Displays the contents of the [IP routing table](#). (This is equivalent to the **route print** command under Windows.)

```

Spectracom NetClock 9483 Version 5.6.0
spadmin@Spectracom ~ $ netstat -nr
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 10.2.1.1 0.0.0.0 UG 0 0 0 eth0
10.2.0.0 0.0.0.0 255.255.0.0 U 0 0 0 eth0
10.2.0.0 0.0.0.0 255.255.0.0 U 0 0 0 eth2
127.0.0.0 0.0.0.0 255.0.0.0 U 0 0 0 lo
spadmin@Spectracom ~ $

```

Note: All of the counters are reset upon a power cycle. They do not persist.

netstat -tulnpe (TCP, UDP, active tcp connections. names of protocols)

```
admin@SpectracomCS176 ~ $ netstat -tulnpe
Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)

```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	User	Inode	PID/Program name
tcp6	0	0	:::8080	:::*	LISTEN	0	7228	-
tcp6	0	0	:::80	:::*	LISTEN	0	7220	-
tcp6	0	0	:::21	:::*	LISTEN	0	9184	-
tcp6	0	0	:::22	:::*	LISTEN	0	9185	-
tcp6	0	0	:::443	:::*	LISTEN	0	7224	-
tcp	0	0	0.0.0.0:68	0.0.0.0:*		0	6298	-
tcp	0	0	0.0.0.0:68	0.0.0.0:*		0	6221	-
tcp	0	0	0.0.0.0:40283	0.0.0.0:*		0	6093	-
tcp	0	0	10.2.100.176:123	0.0.0.0:*		0	72759137	-
tcp	0	0	10.2.100.188:123	0.0.0.0:*		0	61752464	-
tcp	0	0	127.0.0.1:123	0.0.0.0:*		0	7320	-
tcp	0	0	0.0.0.0:123	0.0.0.0:*		0	7315	-
tcp	0	0	0.0.0.0:161	0.0.0.0:*		0	6979	-
tcp	0	0	0.0.0.0:65296	0.0.0.0:*		0	6277	-
tcp6	0	0	fe80::2d0:c9ff:feba:123	:::*		0	72759141	-
tcp6	0	0	fe80::20c:ecff:fe05:123	:::*		0	61752468	-
tcp6	0	0	:::1:123	:::*		0	7326	-
tcp6	0	0	:::1:123	:::*		0	7312	-
tcp6	0	0	:::1:161	:::*		0	6980	-
tcp6	0	0	:::26361	:::*		0	6094	-
tcp6	0	0	:::10240	:::*		0	6278	-

ss -ltnu command

- Refer to: <https://www.tecmint.com/find-open-ports-in-linux/>

You can also use ss command, a well known useful utility for examining sockets in a Linux system. Run the command below to list all your open TCP and UCP ports:

List All Network Ports Using ss Command					
\$ ss -ltnu					
Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
udp	UNCONN	0	0	*:68	:::*
tcp	LISTEN	0	128	:::22	:::*
tcp	LISTEN	0	128	*:22	:::*
tcp	LISTEN	0	50	*:3306	:::*
tcp	LISTEN	0	128	:::80	:::*
tcp	LISTEN	0	100	:::25	:::*
tcp	LISTEN	0	100	*:25	:::*

Make it a point to read through the man pages of the commands above for more usage information.

*Ping command

Options:

-t	Pings the specified host until stopped. To see statistics and continue - Type Control-Break; To stop - press Ctrl + C.
-a	Resolve addresses to hostnames.
-n	count Number of echo requests to send.
-l size	Send buffer size.
-f	Set Don't Fragment flag in packet (IPv4-only).
-i	TTL Time To Live.
-v	TOS Type Of Service (IPv4-only. This setting has been deprecated and has no effect on the type of service field in the IP Header).
-r count	Record route for count hops (IPv4-only).
-s count	Timestamp for count hops (IPv4-only).
-j host-list	Loose source route along host-list (IPv4-only).
-k host-list	Strict source route along host-list (IPv4-only).
-w timeout	Timeout in milliseconds to wait for each reply.
-R	Use routing header to test reverse route also (IPv6-only). Per RFC 5095 the use of this routing header has been deprecated. Some systems may drop echo requests if this header is used.
-S srcaddr	Source address to use.
-4	Force using IPv4.
-6	Force using IPv6.

Windows XP and lower syntax

```
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j  
host-list] | [-k host-list]] [-w timeout] destination-list
```

Desire to ping an entire subnet (all devices on the subnet respond)

- **Note:** (as of at least May, 2017) this command is available on **Linux only** – not available via Windows command prompt. So, can use a SecureSync's CLI to perform this command out to the network.
- Example to ping the entire 10.2.x.x network

At the command prompt, type: `ping -b 10.2.0.0` <enter> (where -b is for broadcast)

*HyperTerminal (for all products that can use RS-232 CLI interface)

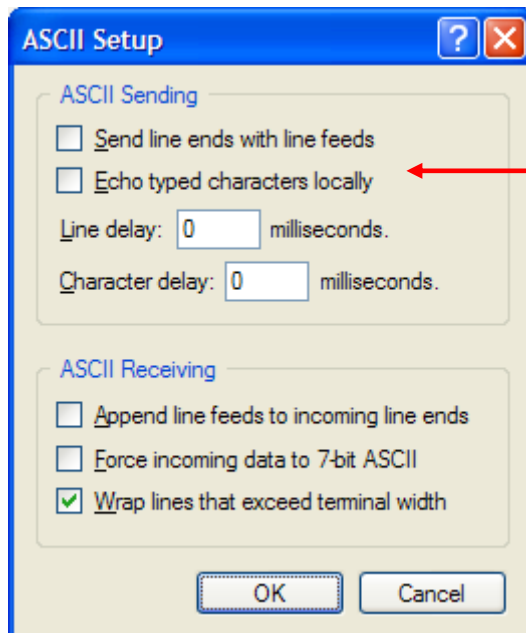
- Link to HyperTerminal document: <\\Rocfnp01\idrivedata\Customer Service\HyperTerminal>

Double characters being displayed when one character is sent to the Serial port

If Local echo is enabled in HyperTerminal, every character that is typed to be sent to the Serial Setup ports will show the same character next to it (type an A and AA is displayed).

To disable local echo in HyperTerminal (should be disabled by default):

- P) Go to File -> Properties (select Settings tab) -> ASCII Setup.
- Q) Uncheck "Echo typed characters locally"



**Logout button/ web browser opening a connection already logged in

Q. Whenever I log into the ntp server and I close browser without logging out of ntp server I can reopen the browser to the ntp address and it bypasses the login prompt and I go right to the Home menu with the credentials from the previous session.

A. As for the re-login, are you completely exiting out of Internet Explorer (or whichever browser you are using)? Or are you just closing out the single connection in the browser without hitting the logout button in the SecureSync's browser and not exiting completely out of Internet Explorer? Note that the browsers cache the login settings so if the browser stays open and you didn't press logout, it will start a new connection already logged in. To prevent the browser from opening already logged in, either press the logout button before closing (which is the only way to tell the browser you are closing out), or close out of the browser tool altogether and then re-open it.

There may be a way to disable the browser from remembering the login info while it remains open, but I'm not aware of any.

**Web browser page caching/refresh

If the web browser (such as Internet Explorer, Firefox or Chrome is caching pages (instead of refreshing every time a page is visited), it may appear that configuration changes aren't taking. Page caching should be disabled.

A) Disabling caching in Firefox:

refresh page every time visit

2 REPLIES 20 HAVE THIS PROBLEM LAST REPLY BY ZEDZEDTOP 1 YEAR AGO

ZedZedTop

How do I set the browser to refresh page every time visited? Didn't it used to do that?

Modified February 16, 2011 7:18:12 AM PST by ZedZedTop

Helpful replies

1. Type `about:config` into the location bar and press enter
2. Accept the warning message that appears, you will be taken to a list of preferences
3. Locate the preference `browser.cache.check_doc_frequency`, double-click on it and change its value to 1

http://kb.mozillazine.org/Browser.cache.check_doc_frequency

about:config - Mozilla Firefox

File Edit View History Bookmarks Yahoo! Tools Help

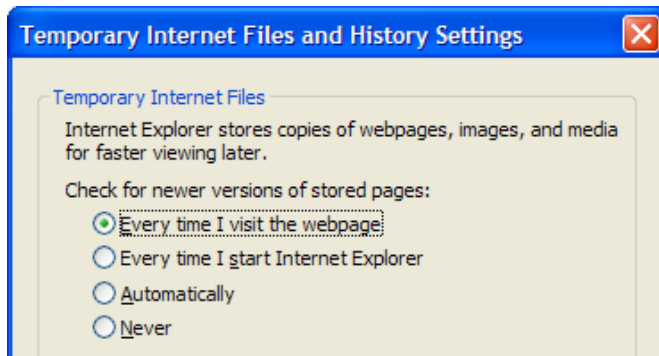
Case: 0000643... Open Cases about:config View Issues - M... GPS time synchron... LindMad's Area... Country Assign... Spectracom Disable cache o...

about:config

browser.blink_allowed	default	boolean	true
browser.bookmarks.autoExportHTML	default	boolean	false
browser.bookmarks.editDialog.firstEditField	default	string	namePicker
browser.bookmarks.max_backups	default	integer	10
browser.cache.check_doc_frequency	default	integer	3
browser.cache.compression_level	default	integer	0
browser.cache.disk.capacity	user set	integer	1048576
browser.cache.disk.enable	default	boolean	true
browser.cache.disk.max_entry_size	default	integer	51200
browser.cache.disk.smart_size.enabled	default	boolean	true
browser.cache.disk.smart_size.first_run	user set	boolean	false
browser.cache.disk.smart_size_cached_value	user set	integer	1048576
browser.cache.disk_cache_ssl	default	boolean	true

B) Disabling caching in Internet Explorer:

Navigate to **Tools -> Internet Options**. In the “**Browsing history**” section of the “**General**” tab, click on “**Settings**”. Under “Temporary Internet Files” select either “**Every time I visit the website**” or “**Automatically**”.



C) Disabling caching in Chrome

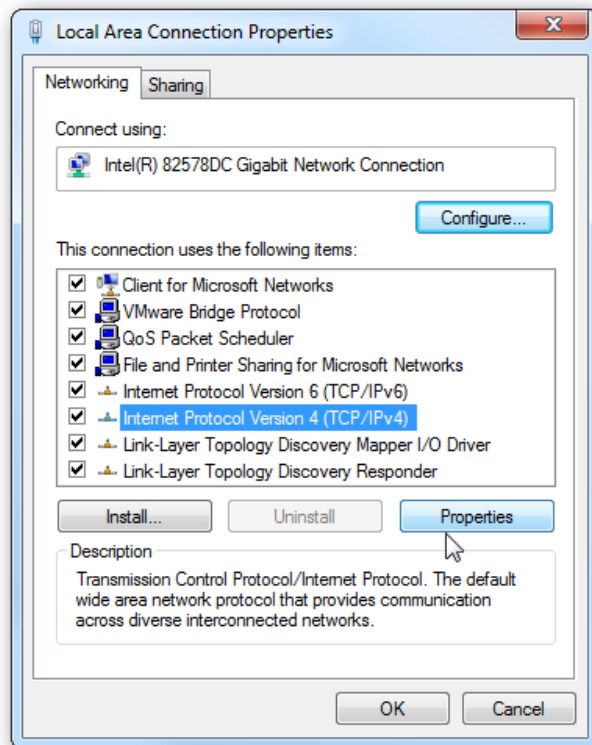
- Refer to sites such as: <http://christian.roy.name/blog/disable-cache-chrome>
-

Assigning a static IP address on a laptop/stand-alone PC

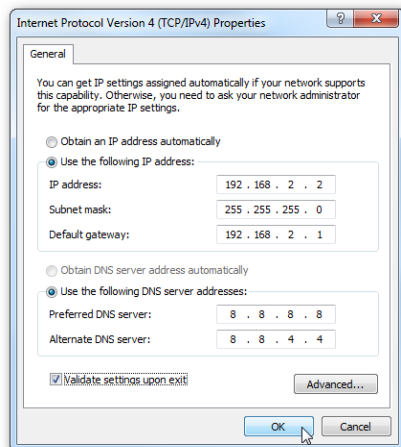
A) Windows 7

- Refer to <http://www.howtogeek.com/howto/19249/>

- 7) Type “network and sharing” in in Start Menu search field
- 8) Select Change adapter settings”
- 9) Right click on “Local Area Connection” and select Properties.
 - Selects Internet Protocol Version 4 (TCP/IP)

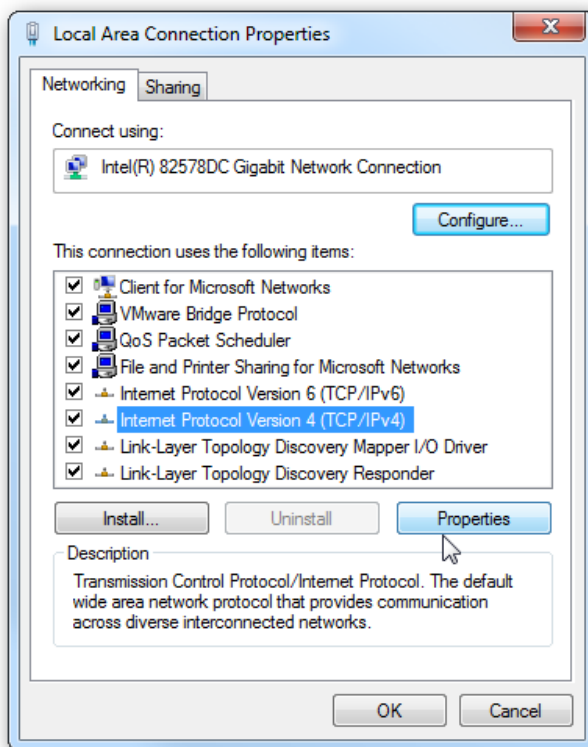


1) Select “Use the following address”:

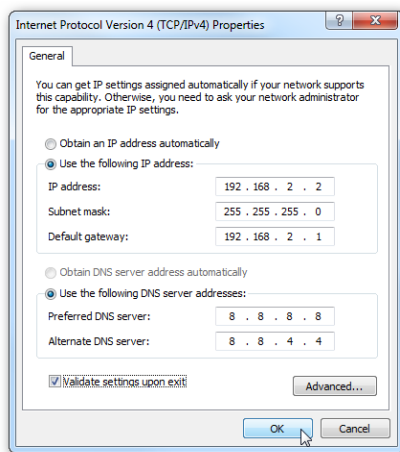


A) Windows XP

- R) Start -> Control Panel
- S) Select “Network Connections”
- T) Right click on “Local Area Connection” and select Properties.
- U) Selects Internet Protocol Version 4 (TCP/IP)



V) Select “Use the following address”

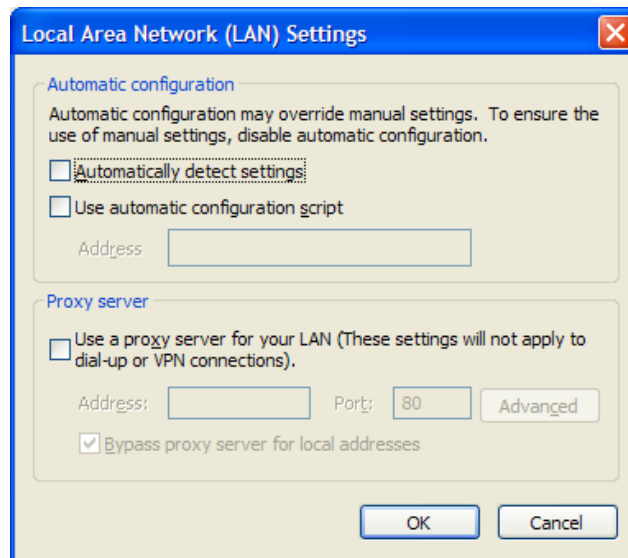


**Accessing the web browser using Internet Explorer (IE)

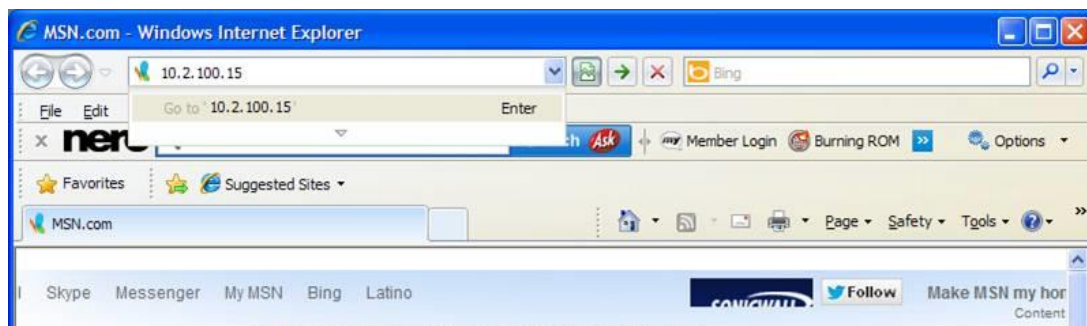
- Some versions of IE may not allow access to the web browser, when using the default Spectracom self-signed HTTPS certificate. This requires a new certificate first be created in the SecureSync.
- To create a new HTTPS certificate, refer to (email): EQUIPMENT\SPECTRACOM
EQUIPMENT\SecureSync\HTTPS certificate

I don't have any information specific to IE9 for it to interface with the Model 9383. However, I do have a couple of general items regarding IE/ Firefox that may help:

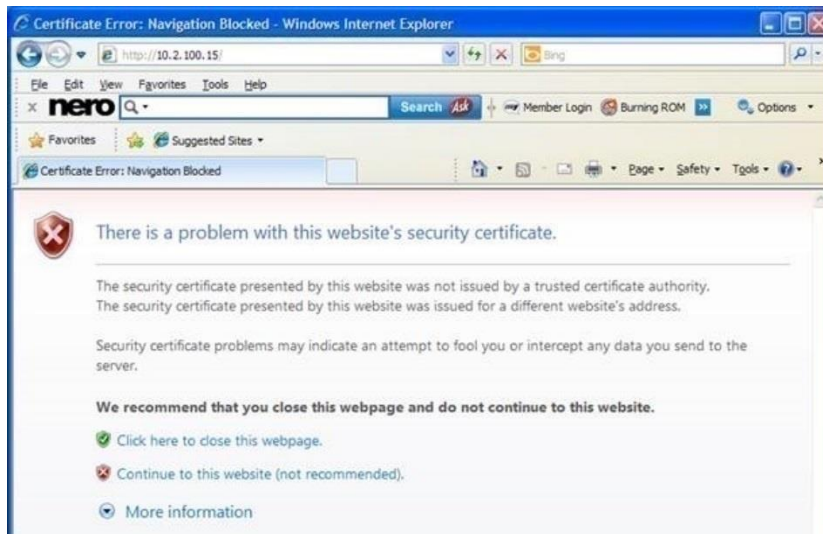
- In Tools -> Internet Options -> "Connections" tab, click on "LAN Settings".
- As shown below, make sure **"Use a Proxy server for your LAN"** is not selected.



- A) To open the web browser, highlight the entire address line and then enter only the IP address of the Model 9383 (see the example screenshot below, where "10.2.100.15" is the IP address of an NTP server).

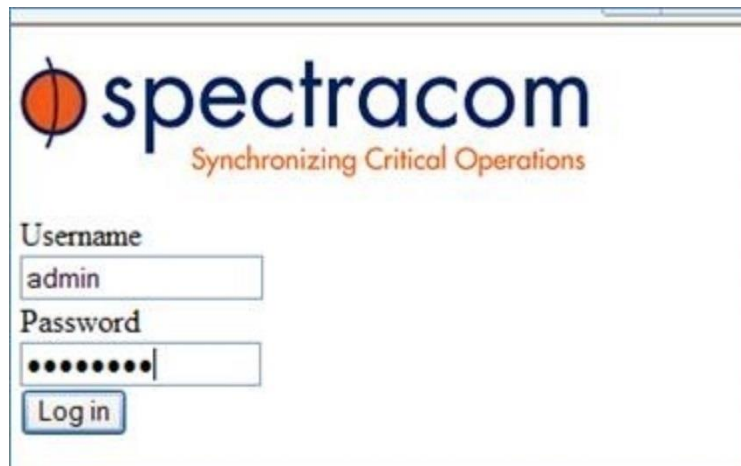


- A login page should now be displayed.



- Click on “Continue to this website”

This should open the login screen. FYI- the “username” is **admin** and the default password is **admin123**.



Note: If the login screen is not opening, you may need to create a new, custom HTTPS certificate before IE will let you in. From a PC running Firefox, login to the browser and follow the steps in the attached document to delete the default certificate and create a new one. Some versions of IE may not allow you to access a browser that is using a factory default HTTPS certificate. Firefox is less critical of this.

Please let me know if you have any other questions (or if you still aren't able to open the browser).

**Securing unused network RJ-45 ports

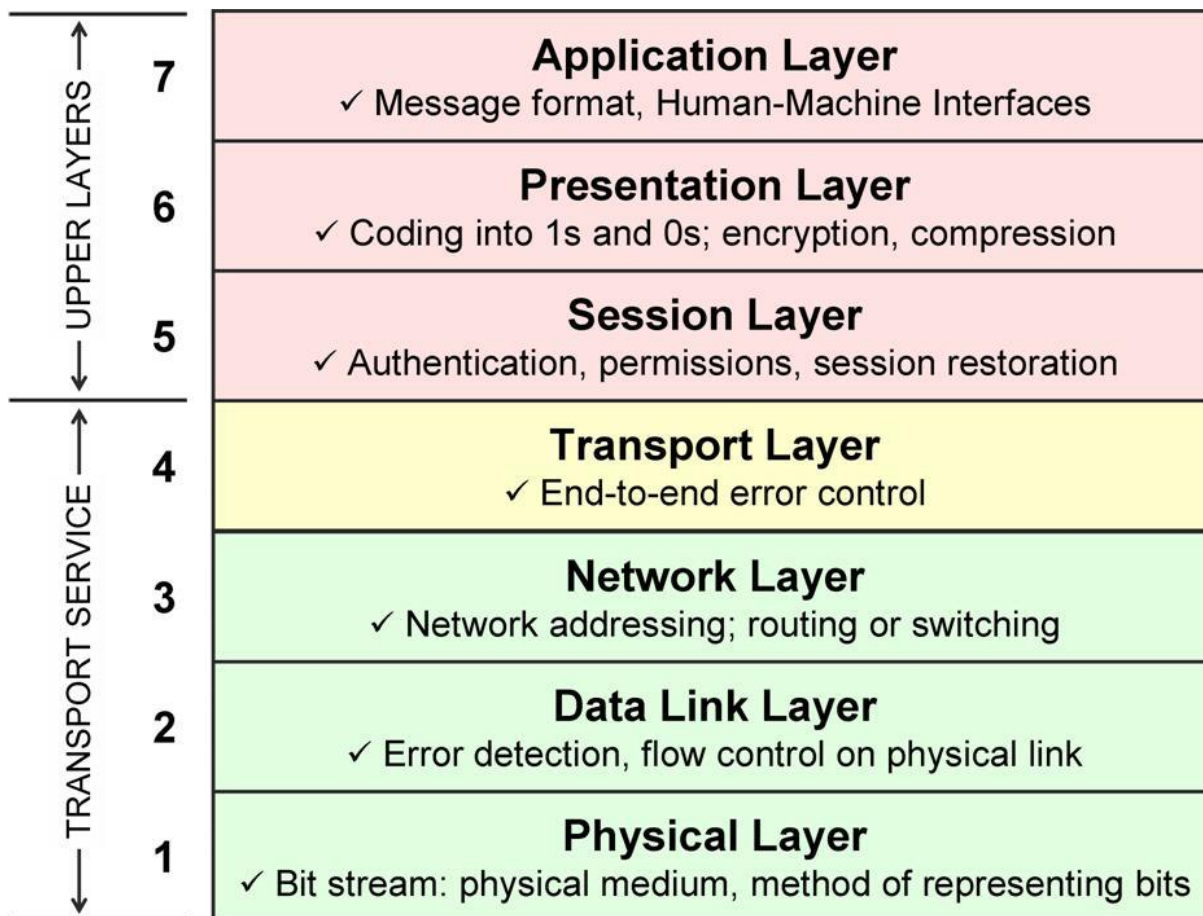
- Starting in Software update 5.1.2, GB ports can be enabled/disabled via software.
 - Can each of these three ports on the card be individually enabled/disabled via the Web control interface. This did not seem clear to me in the user's manual.
- A. Reply from Dave Sohn (2 Apr 2013)** There is no means through the user interface to enable/disable the Ethernet ports. Can now update software and disable Gb Ethernet ports via software.

If a customer has concerns of open (unconnected) Ethernet ports potentially being a potential security issues, there are devices available to lock unused Ethernet ports.

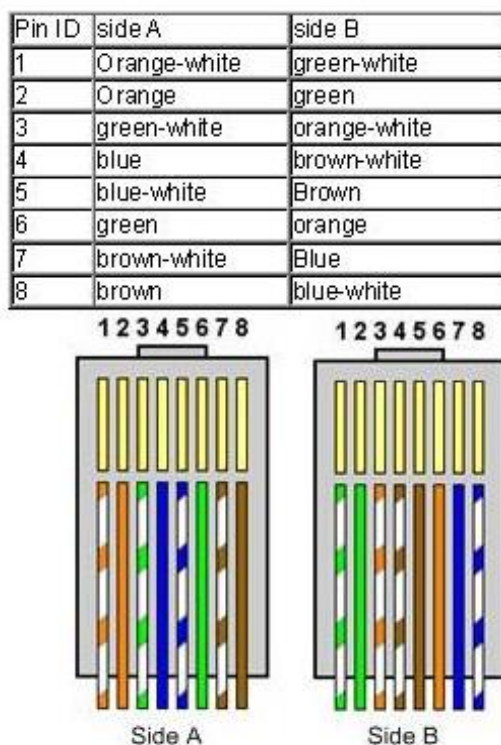
Email from Keith Regarding your customer's concern with unused Ethernet ports, I JUST received some additional information for a device that can be used to lock unused Ethernet ports. These are available devices that your customer can purchase locally, which are specifically designed to lock unused Ethernet RJ-45 ports.

The following is a link to a company that offers these Ethernet locks: <http://www.rjlockdown.com/> . In the top menu, click on "JACKLOCK" (There may be other companies that also offer this same type of device, but this link provides a great example for you).

**Packlayers



**Network cross-over cable



Email from Adam: Here's the info I use when making a crossover:

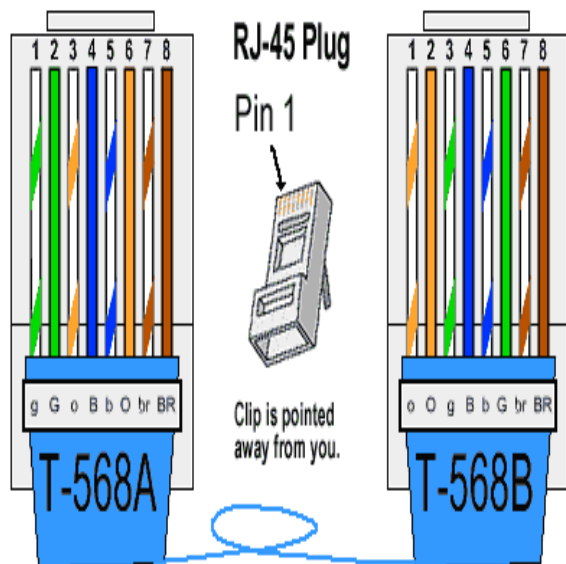
Wire one end using the T-568B standard...

OW,O,GW,B,BW,G,BW,B

Wire the opposite end using the T-568A standard. Under the T-568A standard, the G / GW wires are switched with O / OW:

GW,G,OW,B,BW,O,BW,B

Example:



****Port assignments and RFCs (NTP, HTTP, HTTPS, SNMP, Syslog, etc) for all products**

The Internet Engineering Task Force website (has a section titled "RFC pages". RFC's (Request For Comments) provide a breakdown of the many protocols used by computers and networks. Refer to <http://www.ietf.org/rfc.html> to query for a specific RFC.

MIB-2 is officially defined in RFC1213. Type in “1213” where it asks for the RFC number. This will give you Management Information Base for Network Management protocol for TCP/IP-based Internets (MIB-II).

- Refer to: http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

**Network ports

Services	Network Port	UDP/TCP	Direction (relative to NTP sever)	Notes	Link to RFC's http://www.ietf.org
Daytime protocol	12 or 13	TCP/UDP	Model 9383 NetClocks (v3.6.7) NTP disabled itself sometime after leap second was applied directional	Typically left disabled I've never seen used-typically disabled Time code is in ASCII characters	867
DHCPv4	67 and 68	UDP	Bi-directional		2131
DHCPv6	546	UDP	Bidirectional		
FTP	21	TCP	Bi-directional		
HTTP	80	TCP/UDP	Bi-directional		1945 and 2068
HTTPS	443	TCP	Bi-directional		
HTTPS for the Classic Interface	8080	TCP		This is the port used for the "classic interface" in Some versions of SecureSync and 9400 series	
LDAP	389 (TLS) and 636 (SSL)	TCP/UDP	Bi-directional		3494 (LDAPv2) [RFC4511] The Protocol [RFC4512] Directory Information Model [RFC4513] Authentication Methods and Security Mechanisms (TLS) [RFC 2253] String Representation of Distinguished Names [RFC4515] String Representation of Search Filters [RFC4516] Uniform Resource Locator [RFC4517] Syntaxes and Matching Rules [RFC4518] Internationalized String Preparation [RFC4518] [RFC4519] Schema for User Applications
NTPv4 Autokey SNMP MIB for NTPv4 NTP for DHCPv6	123	UDP	Bi-directional	Server provides a data packet that includes a 64-bit timestamp containing time in UTC seconds since 01/01/1900 with a resolution of 200 picoseconds. NTP client S/W normally runs	I:\Engineering\Specs and Standards\RFCs\NTPv4 1305 (NTPv3) 1769 (v3) 2030 (v4) and 43 4330 5905 (NTPv4)

				continuously and gets periodic updates from server	5906 5907 5908
PTP Event messages	319	UDP	Bi-directional	Sync and Delay Request messages PTP ports 319 and 320 are considered bi-directional. Both ports send PTP packets to /from PTP Masters and Slaves (inbound and outbound packets)	
PTP General messages	320	UDP	Bi-directional	Follow-up, Announce, and Delay Response messages PTP ports 319 and 320 are considered bi-directional. Both ports send PTP packets to /from PTP Masters and Slaves (inbound and outbound packets)	
Radius	1812, 1813 2868 and 2869 (radius extensions)	TCP/UDP	Bi-directional		http://www.ietf.org/rfc/rfc2865.txt 2865 and 2866
RADIUS Acctg:	1813	TCP/UDP			
SCP (Secure Copy)	22				
SMTP	25 or 587	TCP	Outbound	587 is used for GMAIL Sapling IP clocks use this port to send email alerts	
SNMP	161	UDP	Bi-directional		2574 (SNMPv3) 1157 (snmpV1,V2) 1213 http://www.apps.ietf.org/rfc/rfc2574.html
SNMP traps	162	UDP	Outbound		
SSH/SFTP	22	TCP/UDP	Bi-directional		
Syslog	514	UDP	Outbound		3164/5424
Telnet	23	TCP	Bi-directional		
TIME protocol	37	TCP/UDP	Bi-directional	I've never seen used- typically disabled Unformatted 32-bit binary number contains time in UTC seconds since 01/01/1900.	RFC-868

Note: When time servers are scanned with vulnerability scanners or nmap commands, UDP ports (such as Syslog port 514 and NTP port 123) may be detected as being open, even though they are really closed.

From <http://osdir.com/ml/os.openbsd.pf/2003-12/msg00190.html>

Ran scans with nessus and nmap, both show udp port 514 open. Turned off Nat's and redirects, this did not change anything though. Tried a block all quick on internet interface, it still shows it open. Does this make sense to anyone? IP address changed let me know if you need to see the whole ruleset.

Ah, how do you define 'open' for udp?

since udp is a connectionless protocol, the scanners `_assume_` that it is open if they do not receive an icmp port-unreachable packet. Your rules just drop the packet, and do not return anything.

Network Discovery/Network Auto Discovery/Auto-Discovery

per <https://www.bing.com/search?q=auto+discover+network&gs=SC&pg=autodiscover+network&sk=AS1&sc=6-20&cvid=E0055639B243408EA04BC4283BC25288&FORM=QBRE&sp=2>

“Based on the **network** location you choose, Windows will **automatically** assign a **network discovery** state to the **network** and opens the appropriate Windows Firewall ports for that state. **Network discovery** is a **network** setting that affects whether your computer can find other computers and devices on the **network** and whether other computers on the **network** can find your computer”

*NWay auto-negotiation (auto sensing) / port duplex

- Refer to <http://en.wikipedia.org/wiki/Autonegotiation>
- Refer to <http://searchnetworking.techtarget.com/definition/NWay>
- NWay (Auto-Negotiation) is defined in Clause 28 of the D4 draft of the ANSI/IEEE Std 802.3 MAC Parameters, Physical Layer, Medium Attachment Units and Repeater for 100 Mb/s Operation.

Normal order of precedence during auto-negotiation (per spec 802.3)

Upon receipt of the technology abilities of the other device, both devices decide the best possible mode of operation supported by both devices. The priority among modes specified in the 2002 edition of 802.3 is as follows:

1. 100BASE-T full duplex
2. 100BASE-T half duplex
3. 100BASE-T2 full duplex
4. 100BASE-TX full duplex
5. 100BASE-T2 half duplex
6. 100BASE-T4
7. 100BASE-TX half duplex
8. 10BASE-T full duplex
9. 10BASE-T half duplex

In other words, among the modes that are supported by both devices, each device chooses the one that is the topmost in this list.

Auto-negotiation fails because a switch is hard-coded to one particular setting

- Refer to <http://en.wikipedia.org/wiki/Autonegotiation> (*Duplex mismatch*)

A duplex mismatch occurs when two connected devices are configured in different duplex modes. This may happen for example if one is configured for autonegotiation while the other one has a fixed mode of operation that is full duplex (no autonegotiation). In such conditions, the autonegotiation device correctly detects the speed of operation, but is unable to correctly detect the duplex mode. As a result, it sets the correct speed but starts using the half duplex mode.

***Telnet (for all products)**

Telnet port: TCP port 23

Telnet is not available by default in Windows 7.

- For info on how to enable telnet in Windows 7, refer to:
<http://social.technet.microsoft.com/wiki/contents/articles/910.windows-7-enabling-telnet-client.aspx>

- B) Control Panel -> Programs
- C) Click on "Turn Windows features on or off"
- D) Select "Telnet Client" and press OK.
- E) Telnet should be available (via the Windows command prompt window) moments later.

***FTP (for all products)**

- **FTP** port is port 21
- **SCP** port is port 22

Freeware/evaluation FTP programs

- 1) CoreFTP lite (www.coreftp.com) Freeware
- 2) http://www.ipswitchft.com/Products/Ws_Ftp_Pro/Evaluation.aspx (eval software)

****IPv6 addresses (for all products that support IPv6)**

IPv6 formats: Refer to: http://en.wikipedia.org/wiki/IPv6_address#Stateless_address_autoconfiguration

Types of unicast IPv6 addresses (see additional info on each, further below)

- F) Global unicast addresses, which are conventional, publicly routable address, just like conventional IPv4 publicly routable addresses.
- G) Link-local addresses are akin to the private, non-routable addresses in IPv4 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). They are not meant to be routed, but confined to a single network segment. Link-local addresses mean you can easily throw together a temporary LAN, such as for conferences or meetings, or set up a permanent small LAN the easy way.
- H) Unique local addresses are also meant for private addressing, with the addition of being unique, so that joining two subnets does not cause address collisions.

From http://en.wikipedia.org/wiki/Unique_local_address

The address block **fc00::/7** is divided into two /8 groups:

- The block **fc00::/8** has not been defined yet. It has been proposed to be managed by an allocation authority, but this has not gained acceptance in the [IETF](#).^{[1][2][3]}
 - The block **fd00::/8** is defined for /48 prefixes, formed by setting the 40 least-significant bits of the prefix to a randomly generated bit string. This results in the format **fdxx:xxxx:xxxx::** for a prefix in this range. [RFC 4193](#) offers a suggestion for generating the random identifier to obtain a minimum-quality result if the user does not have access to a good source of random numbers.
- I) Special addresses are loopback addresses, IPv4-address mapped spaces, and 6-to-4 addresses for crossing from an IPv4 network to an IPv6 network.

****RFC-2462: SLAAC addresses (Stateless Address Autoconfiguration for IPv6)**

- Refer to: <https://datatracker.ietf.org/doc/rfc2462/> and http://en.wikipedia.org/wiki/IPv6_address#Stateless_address_autoconfiguration
- Refer to Salesforce cases such as 192442
- Refer on online SecureSync user guide at: http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/SETUP/NCSS_Netw_Ports.htm?Highlight=slaac

On system startup, a node automatically creates a [link-local address](#) on each IPv6-enabled interface, even if globally routable addresses are manually configured or obtained through "configuration protocols" (see below). It does so independently and without any prior configuration by stateless address autoconfiguration (SLAAC),^[29] using a component of the [Neighbor Discovery Protocol](#). This address is selected with the prefix **fe80::/64**.

NOTICE: IPv6 configurations require the applicable ethernet interfaces be actively attached to an IPv6 network while configuring. Otherwise, the config changes won't be accepted.

**** link-local / global unicast**

- SecureSync automatically generates a link-local address that is based on the hardware MAC address

Email from Lisa Perdue to Danny Loke (22 Apr 13) Unlike IPv4, IPv6 requires a link-local address to be assigned to every network interface on which the IPv6 protocol is enabled, even when one or more routable addresses are also assigned.[7] Consequently, IPv6 hosts usually have more than one IPv6 address assigned to each of their IPv6-enabled network interfaces. The link-local address is required for IPv6 sublayer operations of the Neighbor Discovery Protocol, as well as for some other IPv6-based protocols, like DHCPv6. That is why we will put it back, even if they delete it.

Email from Dave Lorah to Mark Goodlein (7/25/12) about Hughes Network

I have a customer that is using SecureSync with IPv6. They wish to have a static address configured. They can enter a static address

but are unable to delete the autoconfigured IPv6 address in the setup table. It keeps coming back. It is like DHCP is always on. Is there a way to disable the DHCP or Autoconfig feature in IPv6 so they can only have the static IPv6 address they have entered?

Reply from Mark:

The SecureSync automatically generates a link-local address that is based on the hardware MAC address. In general, machines using IPv6 will typically have several addresses, one of which is usually a link-local address. The SecureSync does not currently have support for permanently turning off the link-local address. It can be deleted, but will be recreated whenever the interface link is brought up or the system is rebooted.

You may use your static IP address but the auto configured link-local address will be there as well.

Hughes response:

The question was not deleting the link-local address, it will always be permanent. I want to delete the global-unicast address that is automatically generated when the device receives a router-advertisement (RA) from a router/firewall.

I want to assign a static entry for that section and permanently stop the global-unicast address from being auto-generated.

Mark Goodlein's reply to Dave Lorah:

The SecureSync automatically generates a link-local address that is based on the hardware MAC address. In general, machines using IPv6 will typically have several addresses, one of which is usually a link-local address. This is the first I have heard of a customer needing to delete or want to turn off the link-local address and I am not sure I understand the reason for doing it. Regardless of that, the SecureSync does not currently have support for permanently turning off the link-local address. I believe that it can be deleted, but will be recreated whenever the interface link is brought up or the system is rebooted.

****NTP support for IPv6**

(12/8/11 KW) a SecureSync customer asked if NTP supports IPv6 addresses. I spoke to both Mark G and Paul about this. As far as they are aware, NTP supports IPv6 addresses for the standard unicast operation. However, at least currently, NTP Autokey mode doesn't work with IPv6.

(9/25/12 KW) I confirmed with Mark Goodlein that 9300s should be fine with IPv6, except NTP Autokey.

Load Balancing / Load Balancers

- Refer to sites such as: <https://f5.com/glossary/load-balancer>

A load balancer is a device that acts as a reverse proxy and distributes network or application traffic across a number of servers. Load balancers are used to increase capacity (concurrent users) and reliability of applications. They improve the overall performance of applications by decreasing the burden on servers associated with managing and maintaining application and network sessions, as well as by performing application-specific tasks. Load balancers are generally grouped into two categories: Layer 4 and Layer 7. Layer 4 load balancers act upon data found in network and transport layer protocols (IP, TCP, FTP, UDP). Layer 7 load balancers distribute requests based upon data found in application layer protocols such as HTTP.

Requests are received by both types of load balancers, and they are distributed to a particular server based on a configured algorithm. Some industry standard algorithms are:

- Round robin
 - Weighted round robin
 - Least connections
 - Least response time
- Load balancing doesn't use any special routing protocols, so our products don't need to have any special functionality to be able to support load balancing.

Using Load balancing with NTP

Refer to sites such as: <http://c59951.r51.cf2.rackcdn.com/5471-281-knowles.pdf>

- Load balancing is handled inside routers/switches. The load balancer sends the NTP packet to the address it determines is less loaded- not to the address it was intended for.
- Can adversely affect NTP: NTP can be configured to point to multiple servers. But load balancing is likely to send NTP requests to another server than the one NTP thinks it's sending it to.
- So, there is a trade-off between "availability" of NTP servers on the network based on the number of packets being sent VERSUS how NTP normally selects and uses its references.
- Any time variations between multiple time servers may cause NTP to need to slew itself,
- because NTP may start to get time from another time server. without NTP selecting another time server (it won't know it received a response from a different time server)

Q. Is it best practice to use our load balancers or the master slave configuration on the NTP appliances?

A Reply from Keith (3 Dec 14) The short answer to the last sentence of your customer's email is "Yes" and "Yes". Load balancing and Master Slave configuration are two different entities, so either or both can be used simultaneously, as desired.

Master/Slave mode for NTP is more commonly referred to as NTP Peering, where if one time server loses sync with GPS, it can start to sync to another time server on the same network (and vice-versa). When one starts to get time from another server, it will drop to one less Stratum level than the one its getting time from. This peering capability can prevent a time server that is no longer synced to GPS from timing out of Holdover mode, which would cause it to go to Stratum 16. At Stratum 16, its NTP clients will stop using it as a time server. As long as its peered with one or more other servers, and others are still available, it will remain at a Stratum that is higher than 16 and will remain useable. Attached is a document that discusses NTP peering with SecureSync.

Load balancing is for network packet traffic control, to help prevent too many packets from being sent to a device. Load balancing can be used for NTP, but it wasn't intended to be used with NTP. NTP Clients are typically assigned multiple time server addresses to be able to get time from and compare against each. Without load balancing, NTP gets time from each server and is able to compare and select the time server it determines is the best reference from this list. Then when its selects a reference, unless it decides to select a different reference, it assumes it's still getting time from the same server it previously selected. If it deems at any point that another server is better, it selects that time server to be its current reference.

However, if the network is load balancing NTP packets, the network is "blindly" sending NTP requests to whichever time server that the balancer wants to send it to, based on the number of packets being sent to each server. NTP is not aware that its time requests to each server may actually all be going to the very same time server. So NTP thinks it's comparing multiple time servers to each other. But in reality, it may be getting all comparisons from the very same time server. It then decides which server is "best" based on just one-time server. After selecting a time server, it will sync to its return packets. But those packets may actually be returning from any one of the servers on the network- instead of the one NTP selected to be its reference.

So there is a trade-off between load balancing request versus how NTP selects and operates with its NTP references. Load balancing prevents a time server from not being able to respond because it's receiving too many time requests in any given second. But load balancing can adversely affect how NTP selects and syncs to its configured NTP servers. Deciding whether or not to use load balancing with NTP is based on which is more critical to the particular application. To help decide which is more important to a specific application, just keep in mind that the SecureSync is able to respond to over 9000 NTP requests every second before it's not able to respond to one (in that particular second) because of the number of time stamps its receiving. If it's feasible a SecureSync may receive more than 9000 time requests in the same second, using load balancing may be more important for the particular application, to allow more time requests to be sent to other time servers, instead of NTP selection/operation for optimum time synchronization of the client.

****LibreSSL/OpenSSL (Libraries for encryption)/ Ciphers List for encryption**

- OpenSSL in the NTP servers have a supported Ciphers list. The client also has its own list of supported ciphers.
- The supported ciphers list is in order of most secure to least secure, with the considered most secure at the top of the list and the least secure at the bottom of the list
- The client and NTP server negotiate which cipher to use, typically the first common one in both lists. This allows the most secure cipher, supported by both Server and Client to be selected for encryption.

A) LibreSSL

- Refer to www.libressl.org
 - Per Paul M- OpenBSD free OS decided they needed their own SSL.

B) OpenSSL

Ciphers list

- The SecureSync's supported Cipher list can be displayed by logging into telnet with the spfactory account. Then type: **openssl ciphers** <enter> (as shown below, with archive softwarev5.0.2 installed):

```

CNA Telnet 10.2.100.89

Spectracom NetClock 9483 Version 5.0.2
spadmin@Spectracom ~ $ openssl ciphers
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384
4:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:SRP-DSS
AES-256-CBC-SHA:SRP-RSA-AES-256-CBC-SHA:DHE-DSS-AES256-GCM-SHA384:DHE-RSA-AES256-
-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA256:DHE-RSA-AES256-SHA:DHE-D
SS-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:DHE-DSS-CAMELLIA256-SHA:EDH-RSA-AES256-GC
M-SHA384:EDH-ECDSA-AES256-GCM-SHA384:EDH-RSA-AES256-SHA384:EDH-ECDSA-AES256-S
HA384:EDH-RSA-AES256-SHA:EDH-ECDSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256
AES256-SHA:CAMELLIA256-SHA:PSK-AES256-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EDH-ECDSA
-DES-CBC3-SHA:SRP-DSS-3DES-EDE-CBC-SHA:SRP-RSA-3DES-EDE-CBC-SHA:EDH-RSA-DES-CBC3
-SHA:EDH-DSS-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:EDH-ECDSA-DES-CBC3-SHA:DES-CBC3
-SHA:PSK-3DES-EDE-CBC-SHA:EDH-RSA-AES128-GCM-SHA256:EDH-ECDSA-AES128-GCM-SHA
256:EDH-RSA-AES128-SHA256:EDH-ECDSA-AES128-SHA256:EDH-RSA-AES128-SHA:EDH-EC
-ECDSA-AES128-SHA:SRP-DSS-AES-128-CBC-SHA:SRP-RSA-AES-128-CBC-SHA:DHE-DSS-AES128
-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-DSS-AES128-SHA25
6:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:DHE-RSA-SEED-SHA:DHE-DSS-SEED-SHA:DHE-R
SA-CAMELLIA128-SHA:DHE-DSS-CAMELLIA128-SHA:EDH-RSA-AES128-GCM-SHA256:EDH-ECDSA
-AES128-GCM-SHA256:EDH-RSA-AES128-SHA256:EDH-ECDSA-AES128-SHA256:EDH-RSA-AES12
8-SHA:EDH-ECDSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:SEED-SHA
CAMELLIA128-SHA:IDEA-CBC-SHA:PSK-AES128-CBC-SHA:EDH-RSA-RC4-SHA:EDH-ECDSA-RC
4-SHA:EDH-RSA-RC4-SHA:EDH-ECDSA-RC4-SHA:RC4-SHA:RC4-MD5:PSK-RC4-SHA:EDH-RSA-DE
S-CBC-SHA:EDH-DSS-DES-CBC-SHA:DES-CBC-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-EDH-DSS-DE
S-CBC-SHA:EXP-DES-CBC-SHA:EXP-RC2-CBC-MD5:EXP-RC4-MD5

spadmin@Spectracom ~ $

```

How is the cipher chosen in an SSL or TLS session?

From <http://luxsci.com/blog/256-bit-aes-encryption-for-ssl-and-tls-maximal-security.html>

In general, when an SSL client, such as an email program or web browser, connects to a server and wishes to use SSL or TLS, the client sends the server a list of encryption ciphers that it supports. The server then goes through the list, in order, and chooses the *first match* that it also supports. Usually, the client orders the list with the most secure methods first, so that the most secure method supported by both the client and server is selected. Sometimes, the client orders the list based on other criteria to make a compromise between security and speed; this can result in a sub-optimal cipher being chosen.

Most modern web and email servers that support SSL encryption, like LuxSci.com's servers, support many different strong encryption techniques all the way up to 128-bit RC4 and 256-bit AES. They provide a variety, instead of just a single really good method, so that users who have old or broken software can still take advantage of encryption, even if it is weaker than it should be. Additionally, most companies that provide security services do not permit use of techniques that deemed are "too weak" and which can be broken very easily (like the old "[export grade ciphers](#)" that used to be in prevalent use). So, if you are connecting to a reputable service provided over SSL or TLS, the type of encryption that will be used is almost certainly determined by *your* client program (i.e. email program or web browser).

*Specific Ciphers

**AES (Advanced Encryption Standard)

- AES is a specification for the encryption of electronic data.

Q. What BIT (size) of AES encryption is supported?

A. Email from Paul Myers (2/2/12) "We support "AES 128, 192, and 256 bit ciphers"

**SHA-1(SHA1) vs SHA-2 (SHA2) family (SHA-224, SHA-256, SHA-384, SHA-512)

- Refer to <http://www.infoworld.com/article/2879073/security/all-you-need-to-know-about-the-move-to-sha-2-encryption.html>
- "SHA-2, the set of cryptographic hash functions to succeed SHA-1"

Intro to SHA

- SHA stands for (Secure Hash Algorithm) and was created by the NSA.
- The number after "SHA" is the hash value (number of bits).

SHA-1 was designed by the NSA and published as a federal standard in 1995. Hashes are used for digitally signing content for integrity validation and are a part of any digital certificate. Without cryptographically sound hashing algorithms, digital authentication and integrity would be very hard to do, if not impossible.

In 2002, SHA-2 became the new recommended hashing standard. SHA-2 is often called the SHA-2 family of hashes because it contains many different-size hashes, including 224-, 256-, 384-, and 512-bit digests. When someone says they are using the SHA-2 hash, you don't know which bit length they are using, but the most popular one is 256 bits (by a large margin). Although SHA-2 is constantly attacked and minor weaknesses are noted, in crypto-speak, it's considered "strong." Without question, It's way better than SHA-1, which experts believe will be fallible in the near term.

IP addresses/subnet masks

- A Subnet mask converter for unique subnets <https://www.dan.me.uk/ipsubnets>. Enter one IP address and it will show you which other IP addresses are on the same subnet.

Netmask settings

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

****HTTP/HTTPS web browser connection/ error messages (for all products)**

The need to enter "HTTPS://" before the IP address: "HTTPS re-direct" can only occur if HTTP is enabled in Services (The redirect is inside the Spectracom box, so it has to be able to get in through http first).

With HTTP enabled, all you need to type in the browser window is the IP address (don't have to type anything in front of the IP address. However, if the HTTP service is disabled in the spectracom box, you have to type "HTTPS://" in the browser (in front of the IP address) in order to be able to access the browser.

HTTP 500 error

- Refer to Salesforce case 11980 (<https://na8.salesforce.com/500C000000U1Psd>)

404 Page not found error

- Refer to Salesforce case 12434
- Check for potential duplicate address on the network.

Credentialed vulnerability scans (Credentialed scans) such as ACAS

- Refer to SR 6114 in SAP and Salesforce case 24044 (I believe both cases are for the same customer/same reason)
- For more info, refer to sites such as <https://www.tenable.com/tips/how-to-enable-credentialed-checks-on-unix>

Email from Paul Myers regarding the email below (4 Jan 17) We don't support this type of scan. Also, we do NOT give user's ability to elevate privilege to root user via 'sudo' command. There is no provision to enable local security checks as this is not a Linux server they have to maintain.

Email from Keith to customer mentioned above (4 Jan 17)

Your report

I'm trying to perform ACAS vulnerability scans on the SecureSync 1200. I'm getting an error message that reads "Local security checks have been disabled because of the following error: find: "/var/db/pkg/". No such file or directory.

I'm not able to create this directory because I'm getting permission denied. Any time I try to elevate privileges using sudo, I get an error message. I haven't been able to find anything online or in the manual. Would you happen to have a fix for this?

My reply

For your information, the SecureSync appliance does not support this particular type of vulnerability scanning. The SecureSync is a "closed/embedded product" (not simply a computer, for instance). The root login password for the SecureSync would be required to be able to perform a credentialed scan. However, for security and file integrity reasons, Spectracom does not divulge this password to anyone outside of our Engineering team!!

In case this additional info may be helpful, the SecureSync is normally scanned by many organizations (Defense/DOD/Financial enterprise users, as well as us), using security scanners such as Nessus or Qualys. These types of vulnerability scanners do not require root access to an appliance in order to scan it for any potential vulnerabilities.

Note: Paul Myers responded to me with Technically not all linux use/provide a root password. It is best not to mention root because just having a root password sets off all kinds of negative connotations.

Scanner needs root access to scan a Spectracom Product

Q Email from Keith to Engineering (9 Aug 2017) The USAF has reported a problem after updating v5.6.0 to 5.7.0. SecureSync v 5.7.0 fails to allow nessus credentialed scan after updating the firmware. It worked at version 5.6.0 they say.
The scan wants to have root access and it gives them a sudu.bin.bash error.

Has something changed in 5.7.0 that needs a workaround to allow this scan to work? Could it be the improved cypher security is causing the problem?

A Reply from Paul Myers

Tenable the seller of nessus has instructions below:

<https://www.tenable.com/tips/how-to-enable-credentialed-checks-on-unix>

This requires a username & password or a username and Public Key which is loaded to allow Linux login.

It does NOT provide root access.

OpenSSH and OpenSSL have been updated and security fixes also likely were applied. It is possible permissions were altered to improve security.

We need to know WHAT they are doing with more specifics:

1. Read the above link.
2. Ask them if they are using a username & password or a username and Public Key to run SSH nessus scan. Please find out enough detail to define technically what they are doing to login. Key type, cipher, login method, Version of OpenSSH/SSH etc.

3. Can they login to the SecureSync using ssh using the same credentials as above using a Linux/Unix SSH session?

Possible sources of this issue are:

1. We changed permissions
2. We broke SSH Login with Username and Public Key. (Retest here)
3. Another updated package blocks this feature.
4. They are using an unsupported SSH Key/cipher type

It is up to Product Management if this is an issue. We don't have NESSUS but David Sohn has run credentialed scans using QualysGuard Express.

We will need to test Release 5.7.0 to verify we can login with SSH correctly and run a credentialed scan on Release 5.7.0/5.7.1.

****Parallel Redundancy Protocol (PRP)**

From Wikipedia

The two LANs are completely separated and are assumed to be fail-independent. A source node sends simultaneously two copies of a frame, one over each port. The two frames travel through their respective LANs until they reach a destination node, in the fault-free case, with a certain time skew. The destination node accepts the first frame of a pair and discards the second, taking advantage of a sequence number in each frame that is incremented for each frame sent. Therefore, as long as one LAN is operational, the destination always receives one frame. This protocol provides a zero-time recovery and allows to check the redundancy continuously to detect lurking failures.

Non-PRP nodes are either attached to one network only (and therefore can communicate only with other nodes attached to the same network), or are attached through a *RedBox*, a device that behaves like a doubly attached node.^[1]

Node failures are not covered by PRP, but duplicated nodes may be connected via a PRP network.

Each node in PRP has two Ethernet interfaces that use the same [MAC address](#) and present the same IP address(es).

Therefore, PRP is a layer 2 redundancy, which allows higher network protocols to operate without modification.

Q. Email from Mark Day, regarding question from Aimil Could you please advise on Sunil's question below regarding support of the Parallel Redundancy Protocol in the SecureSync? I can find no mention of it on the datasheet or in the manual. My understanding is that identical data packets are sent out over two separate networks and assumed to be fail independent, allowing for zero-time recovery and check the redundancy continuously to detect lurking failures on the network as long as one network is operational– is that correct?

A. Reply from Dave Sohn (3 Apr 2013) We do not support parallel redundancy protocol in SecureSync.

**IPSec / IP Security (for all products)

- Refer to the following links

****Tutorial:** <http://technet.microsoft.com/en-us/library/cc783420%28v=ws.10%29.aspx>

******* IKE tutorial:** <http://technet.microsoft.com/en-us/library/cc784471%28v=ws.10%29.aspx>

<http://www.ciscopress.com/articles/article.asp?p=25474&seqNum=7>
http://en.wikipedia.org/wiki/X.509#Sample_X.509_certificates
<http://www.novoksharov.com/2012/01/managing-x-509-certificates-on-windows/>
<http://en.wikipedia.org/wiki/X.509>
http://en.wikipedia.org/wiki/Root_certificate
S:\Engineering\Projects\Lafayette\300_Verification_Test_Plan\Integration_Test_Plans\LIT_030_IPSec.doc
S:\Engineering\Projects\Lafayette\301_Verification_Test_Results\2010_May_Release\LIT_Documents\LIT_030_IPSec_2010_05_13.doc
S:\Engineering\Projects\Lafayette\301_Verification_Test_Results\IPSec\Testing_IPSec_for_Lafayette.docx
S:\Engineering\Projects\Lafayette\301_Verification_Test_Results\IPSec_...Engineering\Engineering_Shared\Security\Interpeak_ipsec.pdf

- Encryption occurs in a different layer. All devices on the network have to support IPSec to use it.

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

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

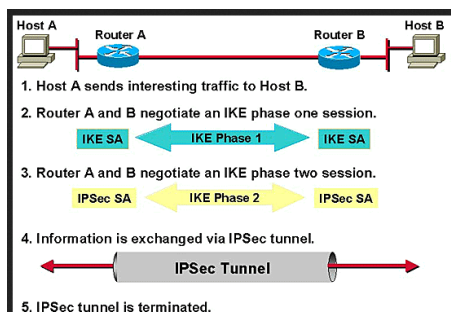
IPSec is a security feature to add encryption to TCP/IP based networking. It is most useful in situations where the customer has a network with other elements using IPSec. Similar security can be achieved more conventionally by using https and SSH.

A unit is configured with a set of Security Policies (SP) that describe whether communications from a particular IP require the use of IPSec and which features are used. Also required are Security Associations (SA) that specify the keys to use between particular IPs. SA can be entered manually or negotiated using the IKE protocol. IKE in Lafayette is implanted using the "racoon" IKE package. This document includes a flow chart that shows the options for configuring IPSec.

The NetClock implementation of IPSec uses SpecApp to perform actions that need to be done as root. These same actions will need to be done on Lafayette, without using SpecApp.

****How IPSec works

<http://www.ciscopress.com/articles/article.asp?p=25474&seqNum=7>



IPSec involves many component technologies and encryption methods. Yet IPSec's operation can be broken down into five main steps:

1. **"Interesting traffic" initiates the IPSec process.** Traffic is deemed *interesting* when the IPSec security policy configured in the IPSec peers starts the IKE process.
2. **IKE phase 1.** IKE authenticates IPSec peers and negotiates IKE SAs during this phase, setting up a secure channel for negotiating IPSec SAs in phase 2.
3. **IKE phase 2.** IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers.

4. **Data transfer.** Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.
5. **IPSec tunnel termination.** IPSec SAs terminate through deletion or by timing out.

Step 1—Defining Interesting Traffic



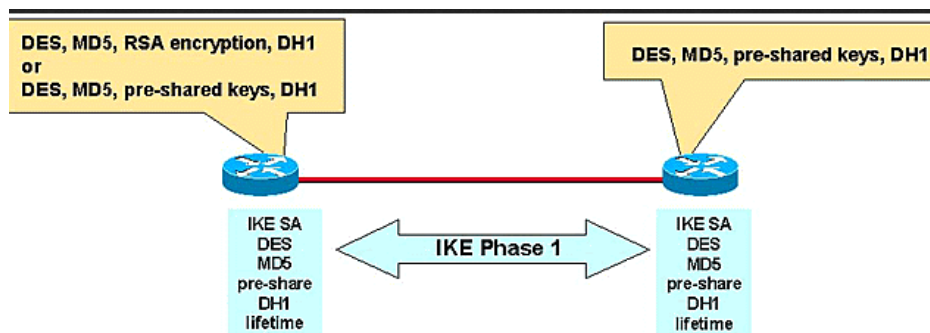
```
access-list 101 permit ip 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255
```

Access lists determine traffic to encrypt

- **Permit**—traffic must be encrypted
- **Deny**—traffic sent unencrypted

What type of traffic is deemed *interesting* is determined as part of formulating a security policy for use of a VPN. The policy is then implemented in the configuration interface for each particular IPSec peer. For example, in Cisco routers and PIX Firewalls, access lists are used to determine the traffic to encrypt. The access lists are assigned to a cryptography policy; the policy's *permit statements* indicate that the selected traffic must be encrypted, and *deny statements* indicate that the selected traffic must be sent unencrypted. With the Cisco Secure VPN Client, you use menu windows to select connections to be secured by IPSec. When interesting traffic is generated or transits the IPSec client, the client initiates the next step in the process, negotiating an IKE phase 1 exchange.

Step 2—IKE Phase 1



- **Authenticates IPSec peers**
- **Negotiates matching policy to protect IKE exchange**
- **Exchanges keys via Diffie-Hellman**
- **Establishes IKE security association**

The basic purpose of IKE phase 1 is to authenticate the IPSec peers and to set up a secure channel between the peers to enable IKE exchanges. IKE phase 1 performs the following functions:

- Authenticates and protects the identities of the IPSec peers
- Negotiates a matching IKE SA policy between peers to protect the IKE exchange
- Performs an authenticated Diffie-Hellman exchange with the end result of having matching shared secret keys
- Sets up a secure tunnel to negotiate IKE phase 2 parameters

IKE phase 1 occurs in two modes: main mode and aggressive mode. These modes are described in the following sections.

Main Mode

Main mode has three two-way exchanges between the initiator and the receiver.

- **First exchange:** The algorithms and hashes used to secure the IKE communications are agreed upon in matching IKE SAs in each peer.
- **Second exchange:** Uses a Diffie-Hellman exchange to generate shared secret keying material used to generate shared secret keys and to pass nonces—random numbers sent to the other party and then signed and returned to prove their identity.
- **Third exchange:** Verifies the other side's identity. The identity value is the IPSec peer's IP address in encrypted form. The main outcome of main mode is matching IKE SAs between peers to provide a protected pipe for subsequent protected ISAKMP exchanges between the IKE peers. The IKE SA specifies values for the IKE exchange: the authentication method used, the encryption and hash algorithms, the Diffie-Hellman group used, the lifetime of the IKE SA in seconds or kilobytes, and the shared secret key values for the encryption algorithms. The IKE SA in each peer is bi-directional.

Aggressive Mode

In *aggressive mode*, fewer exchanges are made, and with fewer packets. On the first exchange, almost everything is squeezed into the proposed IKE SA values: the Diffie-Hellman public key; a nonce that the other party signs; and an identity packet, which can be used to verify identity via a third party. The receiver sends everything back that is needed to complete the exchange. The only thing left is for the initiator to confirm the exchange. The weakness of using the aggressive mode is that both sides have exchanged information before there's a secure channel. Therefore, it's possible to "sniff" the wire and discover who formed the new SA. However, it is faster than main mode.

Step 3—IKE Phase 2

The purpose of IKE phase 2 is to negotiate IPSec SAs to set up the IPSec tunnel. IKE phase 2 performs the following functions:

- Negotiates IPSec SA parameters protected by an existing IKE SA
- Establishes IPSec security associations
- Periodically renegotiates IPSec SAs to ensure security
- Optionally performs an additional Diffie-Hellman exchange

IKE phase 2 has one mode, called *quick mode*. Quick mode occurs after IKE has established the secure tunnel in phase 1. It negotiates a shared IPSec policy, derives shared secret keying material used for the IPSec security algorithms, and establishes IPSec SAs. Quick mode exchanges nonces that provide replay protection. The nonces are used to generate new shared secret key material and prevent replay attacks from generating bogus SAs.

Quick mode is also used to renegotiate a new IPSec SA when the IPSec SA lifetime expires. Base quick mode is used to refresh the keying material used to create the shared secret key based on the keying material derived from the Diffie-Hellman exchange in phase 1.

Perfect Forward Secrecy

If *perfect forward secrecy* (PFS) is specified in the IPSec policy, a new Diffie-Hellman exchange is performed with each quick mode, providing keying material that has greater entropy (key material life) and thereby greater resistance to cryptographic attacks. Each Diffie-Hellman exchange requires large exponentiations, thereby increasing CPU use and exacting a performance cost.

Step 4—IPSec Encrypted Tunnel

After IKE phase 2 is complete and quick mode has established IPSec SAs, information is exchanged via an IPSec tunnel. Packets are encrypted and decrypted using the encryption specified in the IPSec SA. This IPSec encrypted tunnel can be seen in.

Step 5—Tunnel Termination

IPSec SAs terminate through deletion or by timing out. An SA can time out when a specified number of seconds have elapsed or when a specified number of bytes have passed through the tunnel. When the SAs terminate, the keys are also discarded. When subsequent IPSec SAs are needed for a flow, IKE performs a new phase 2 and, if necessary, a new phase 1 negotiation. A successful negotiation results in new SAs and new keys. New SAs can be established before the existing SAs expire, so that a given flow can continue uninterrupted.

Internet Key Exchange (IKE) security associations

[racoon](#) - Internet Key Exchange (IKE) daemon for automatically keying IPsec connections.

The IKE protocol is designed to securely establish a trust relationship between each computer, to negotiate security options, and dynamically generate shared, secret cryptographic keying material. The agreement of security settings associated with keying material is called a security association, also known as an SA. These keys will provide authenticity, integrity, and optionally, encryption of IP packets that are sent using the security association. IKE negotiates two types of security associations:

Firewall ports for IPsec

From a Google search- To make IPsec work through your firewalls, you should open UDP port 500 and permit IP protocol numbers 50 and 51 on both inbound and outbound firewall filters. UDP Port 500 should be opened to allow Internet Security Association and Key Management Protocol (ISAKMP) traffic to be forwarded through your firewalls. IP protocol ID 50 should be set to allow IPsec Encapsulating Security Protocol (ESP) traffic to be forwarded. Finally, IP protocol ID 51 should be set to allow Authentication Header (AH) traffic to be forwarded.

Troubleshooting IPsec

- 1) Ping is the best test to verify comms between the PC and the time server. If ping works, the PC and time server are successfully communicating.
- 2) Make sure the Windows computer can talk to another computer on the network that is also using IPsec!!
- 3) Make sure the PC can talk to the NTP server with IPsec disabled.
- 4) An IPsec filter needs to be created/configured in the PC. Pay close attention to limiters in this filter such as "Protocol" (UDP only, ICMP only, etc - better to choose "All" at least for testing/troubleshooting) "ports" (such as 123 only- better to choose "All" at least for testing/troubleshooting). Otherwise, they may be trying to ping, but if the filter is configured for UDP only, ping won't work.

IPsec with W32Time (seems to be the best reference)

Email I sent to Homer with Roots: I searched with Google for articles discussing W32Time and IPsec. Refer to Appendix A (Windows IP Security) starting on page 25 of the Windows document at: <http://download.microsoft.com/download/2/0/f/20f61625-7b2a-4531-b007-1c714f1e51b7/wintimeserv.doc>. This document discusses using IPsec with W32Time.

Other document that may also be helpful:

<http://www.elandsys.com/resources/ipsec/wincert.html>

<http://technet.microsoft.com/library/c042b3c5-dee1-4a31-ac35-e90e84629044>

<http://technet.microsoft.com/en-us/library/deploy-ipsec-firewall-policies-step-by-step%28v=ws.10%29.aspx>

Configuring IPsec in our NTP servers

A) IPsec for SecureSync/NetClock 9400s:

Refer to: [**IPsec \(IP Security\)](#)

B) IPsec for NetClock Model 9300s/9200s:

Refer to: [IPsec \(IP Security\)](#)

IPsec was enabled in the PC and NTP server but not able to communicate

If the IPsec Policy in the PC and ifl PSec in the NTP server have both been enabled, but still cannot connect to the NTP server, there is likely a configuration issue. Since there is no way to disable IPsec from the CLI interface, the unit will need to be cleaned to reset IPsec to back to off, in order to be able to communicate again.

Note: In at least the 9300/9200 series (possibly also in SecureSync) the IPsec certificates (stored in the **/certificate** folder) are not lost during a Clean process. They are retained.

NetClock 9300/9200 The “**Clean restart**” command can only be performed in Factory login, so customers won’t be able to clean the unit. We will have to remotely login or will need to send a new CF card to reset the configs (unless its application software version 3.6.0 or above)- refer to: [Admin password reset if password is not known](#) in this document.

SecureSync/9400: Initiate a Clean using the front panel menus (command menu)

Troubleshooting IPsec

IKE log entries

Rejected authmethod messages. Indicate phase 1 and phase 2 configs of the NetClock (first value at the end of the log and the PC –the second value at the end of the line).

NetClock PC

```
2013-05-08 08:23:29: ERROR: rejected authmethod: DB(prop#1:trns#1):Peer(prop#1:trns#1) = pre-shared
key : RSA signatures (for PSK, the NetClock is correct)
2013-05-08 08:23:29: ERROR: rejected dh_group: DB(prop#1:trns#1):Peer(prop#1:trns#1) = 768-bit MODP
group : 1024-bit MODP group (my tech note specifies 1024)
2013-05-08 08:23:29: ERROR: rejected authmethod: DB(prop#1:trns#1):Peer(prop#1:trns#2) = pre-shared
key : RSA signatures (for PSK, the NetClock is correct)
2013-05-08 08:23:29: ERROR: rejected hashtype: DB(prop#1:trns#1):Peer(prop#1:trns#2) =
= SHA : MD5 (my tech note specifies SHA)
2013-05-08 08:23:29: ERROR: rejected enctype: DB(prop#1:trns#1):Peer(prop#1:trns#3) = 3DES-
CBC : DES-CBC
2013-05-08 08:23:29: ERROR: rejected authmethod: DB(prop#1:trns#1):Peer(prop#1:trns#3) = pre-shared
key : RSA signatures
2013-05-08 08:23:29: ERROR: rejected enctype: DB(prop#1:trns#1):Peer(prop#1:trns#4) = 3DES-
CBC : DES-CBC
2013-05-08 08:23:29: ERROR: rejected authmethod: DB(prop#1:trns#1):Peer(prop#1:trns#4) = pre-shared
key : RSA signatures
2013-05-08 08:23:29: ERROR: no suitable proposal found.
**
```

Syslog (Remote logs/remote logging)

Example freeware Syslog server software:

- “Event Log Analyzer” <https://www.manageengine.com/products/eventlog/download-free.html>
- “**Syslog server 1.2.3**” (<http://www.softpedia.com/get/System/System-Miscellaneous/Syslog-Server.shtml>)

Free Syslog software for Windows:

More recently (Jan 2018) I downloaded/installed “Event Log Analyzer”

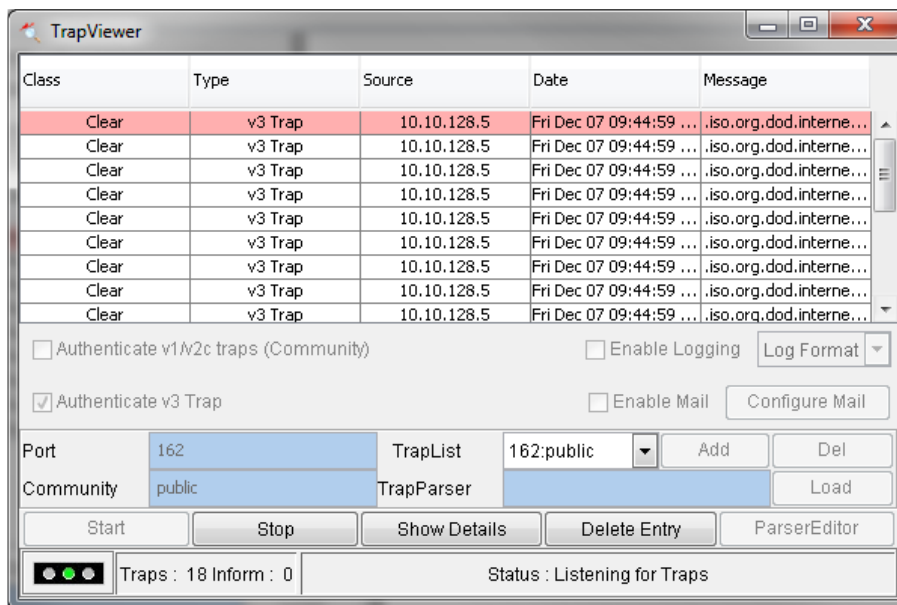
I downloaded/installed “Syslog Server 1.2.3” .

- Refer to <I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\Syslog>

SNMP/Net-SNMP from Sourceforge (for all products)

(From Paul Myers) Program used to analyze MIBs for errors <http://www.ibr.cs.tu-bs.de/projects/libsmi/tools/?lang=de>. Just upload the file and use the defaults.

- Open source SNMP software we use in the SecureSyncs/Netclocks/VersaSyncs: Net-SNMP (NetSNMP)
- Link to a free SNMP Trap Receiver program that supports v3 traps (called “**ManageEngine**” software): <http://www.manageengine.com/products/mibbrowser-free-tool/download.html>
- (Dec 2012) Dave Sohn confirmed SecureSync can send SNMPv3 traps (screenshot showing traps being received is below). Refer to the SecureSync SNMP Tech Note for the configurations/details regarding his testing, while using the ManageEngine SNMP software.



Q. Question on what it means in the datasheet SNMP (**noauth/auth/priv**).

A. (Keith's reply from the above website):

These are SNMP Security levels supported by the v3 agent

(Where “**Priv**” stands for Privacy Protocol – encrypts all the data. DES Symmetric Encryption Protocol is an example of this)

(Where “**Auth**” stands for Authentication Protocol (“authenticate who you are talking to” MD5 and SHA are examples of this)

- **noAuth (noPriv)**: Communication without authentication and privacy.
- **Auth (NoPriv)**: Communication with authentication and without privacy. The protocols used for Authentication are MD5 and SHA (Secure Hash Algorithm).
- **(auth and) Priv**: Communication with authentication and privacy. The protocols used for Authentication are MD5 and SHA; and for Privacy, DES (Data Encryption Standard) and AES (Advanced Encryption Standard) protocols can be used.

Linux SNMPWalks SNMPGets SNMPTraps

- **Note:** To perform an SNMPwalk in linux or SNMP get in linux) , use a SecureSync logged is as spfactory

Refer to “Linux SNMPWalks SNMPGets SNMPTraps’ in SNMP section of the SecureSyncCustAssist document

SNMPv3

(Secure SNMP)/ SNMP version 3 Traps/Notifications

- Refer to (RFC 2574) <http://www.apps.ietf.org/rfc/rfc2574.html> and http://www.webnms.com/simulator/help/sim_network/netsim_conf_snmpv3.html

From Wikipedia:

The snmpEngineID has a length of 12 octets.

The first four octets are set to the binary equivalent of the agent's SNMP management private enterprise number as assigned by the Internet Assigned Numbers Authority (IANA). For example, if Acme Networks has been assigned {enterprises 696 }, the first four octets would be assigned '000002b8'H.

The remaining eight octets are determined via one or more enterprise-specific methods. Such methods must be designed so as to maximize the possibility that the value of this object will be unique in the agent's administrative domain. For example, it may be the IP address of the SNMP entity, or the MAC address of one of the interfaces, with each address suitably padded with random octets. If multiple methods are defined, then it is recommended that the first octet indicate the method being used and the remaining octets be a function of the method.

Email from Dave Sohn (11/28/12) The mib browser I used generated a hex context ID, which I then used as the engineID. It needs to be a hexadecimal number entered starting with “0x”. If they don’t enter anything, we will default it to “0x01”.

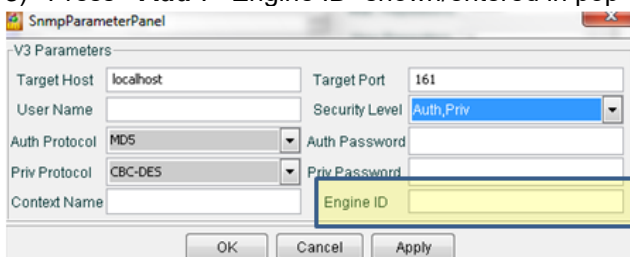
Email KW sent to a dealer This is not a value calculated in, or by, the SecureSync. It's a 12 octet, hexadecimal value that needs to be externally created by a user and then entered into the SecureSync's web browser.

“EngineID” field

- Required for SNMPv3 traps
- Not required for SNMPv3 gets and sets
-

“Engine ID” field with the ManageEngine software program

- 1) Main screen, Edit -> Settings, select “v3”
- 2) Select “**engineID** for adding V3 entry”
- 3) Press “ **Add**”. “Engine ID” shown/entered in pop-up window



- 4) Enter this same value in the SNMPV3 EngineID field in the time server
Note: a default value may be entered automatically in this field. If not, can manually enter a value (such as “80001f8880d7c92a1f7ed4b50” for example)

SNMP reg file

Appears to be a script file that automatically edits “SNMP” settings in Windows System Registry.

Refer to sites such as : http://www.experts-exchange.com/Programming/Languages/Visual_Basic/VB_Script/Q_26911165.html

Example .reg file:

Save the below as a .reg file

Try importing this reg file into a test server with the same production SNMP settings.

If this corrupts the SNMP Settings, then I am unsure how this can be done.

```
1: Windows Registry Editor Version 5.00
2:
3: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters]
4: "EnableAuthenticationTraps"=dword:00000001
5: "NameResolutionRetries"=dword:00000010
6:
7: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers]
8: "1"="10.10.10.10"
9:
10: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\RFC1156AgentCapabilities]
11: "sysContact"=""
12: "sysLocation"=""
13: "sysServices"=dword:0000004f
14:
15: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\TrapConfiguration]
16:
17: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\TrapConfiguration]
18: "1"="10.10.10.10"
19:
20: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities]
21: "public"=dword:00000004
22:
23: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Security]
24: "Security"=hex:01,00,14,80,b8,00,00,00,c4,00,00,00,14,00,00,00,30,00,00,00,02,\
25: 00,1c,00,01,00,00,00,02,80,14,00,ff,01,0f,00,01,01,00,00,00,00,00,01,00,00,\
26: 00,00,02,00,88,00,06,00,00,00,00,00,14,00,fd,01,02,00,01,01,00,00,00,00,\
27: 05,12,00,00,00,00,00,18,00,ff,01,0f,00,01,02,00,00,00,00,00,05,20,00,00,00,\
28: 20,02,00,00,00,00,14,00,8d,01,02,00,01,01,00,00,00,00,00,05,04,00,00,00,00,\
29: 00,14,00,8d,01,02,00,01,01,00,00,00,00,05,06,00,00,00,00,00,14,00,00,01,\
30: 00,00,01,01,00,00,00,00,00,05,0b,00,00,00,00,00,18,00,fd,01,02,00,01,02,00,\
31: 00,00,00,05,20,00,00,00,23,02,00,00,01,01,00,00,00,00,00,05,12,00,00,00,\
32: 01,01,00,00,00,00,00,05,12,00,00,00
```

Email Keith sent to Morgan Stanley (8 Feb 2013)

Up until now, I've never heard of a .reg file for SNMP.

FYI- With a Google search, an snmp.reg file appears to be a script file that makes automatic changes to SNMP entries in Windows System Registry. This type of file appears to configure System Registry variables to contain contact info and SNMP trap OIDs for SNMP on Windows PCs.

We don't provide any Windows-specific SNMP files that edit System Registry settings. However, we do provide contact info and define the SNMP traps in the SPECTRACOM-SECURE-SYNC-MIB file.

- Contact information is included at the beginning of this document (“**spectracomSecureSyncMibModule MODULE-IDENTITY**”).
- SNMP trap information is included towards the bottom of this document (“**ssEventsV2 [enterprises.18837.3.2.3.x]**”).

****Troubleshooting issues with SNMP**

- Refer to <http://www.net-snmp.org/FAQ.html> for lots of good info

A) SNMP polls stop working after a period of time

- Refer to <http://www.net-snmp.org/FAQ.html>
- Refer to Salesforce case 11013 <https://na8.salesforce.com/500C000000SMugB>

Email from Oleg (14 Aug 2013)

Not sure if you have seen this:

From http://www.net-snmp.org/FAQ.html#The_agent_worked_for_a_while_then_stopped_responding Why

The agent worked for a while, then stopped responding. Why?

There are three basic possibilities:

- the agent has crashed
- it is hanging
- it is temporarily overloaded

Detecting whether the agent has crashed should be fairly straightforward.

If you can reliably reproduce this crash (e.g. by sending a particular SNMP request), then contact the coders list for advice.

It's the other two cases that are probably more significant.

To tell the difference between these two, try leaving the agent undisturbed for a while, and then probe it using a single 'snmpget' request, specifying a longer timeout (e.g. '-t 120'). If it now responds, then something was probably sending requests (including duplicate retries) faster than the agent could process them, and it was building up a backlog. Try adjusting the timeout period and retry frequency of these client requests, or look at improving the efficiency of the implementation of the relevant MIB objects.

If the agent remains unresponsive (particularly if the load on the system is steadily climbing), then it's probably hanging, and all you can really do is restart the agent. If you can identify what causes this to happen, then contact the coders list for advice.

****SSH (for all products)**

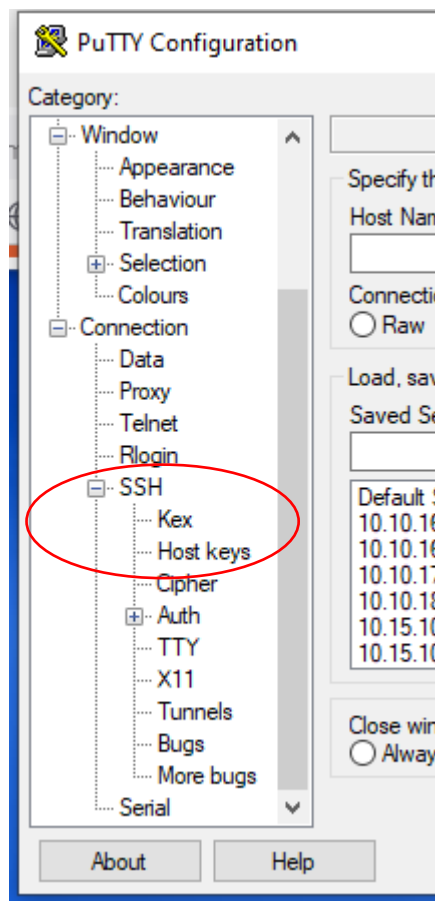
- SSH is a secure, remote CLI interface (Command Line Interface) with a network connection.
- It's a "Secure Telnet"- Same as telnet, but the user name and password are encrypted.
- Use programs such as PuTTY SSH to create an SSH session.
- Recommended key size is 2048.

SSH login

- Does not use Radius or LDAP server for login.
- User Account must be created in the unit (such as SecureSync)
- User Rights/privileges are set by the group permission set in the local user account (admin or user).

Not able to create an SSH session:

- A) SSH port (port 22) closed on a firewall between the device and PC.
- B) Entering wrong login password results in "access denied".
- C) Having SSH disabled in the list of Services (inside the NetClock/SecureSync, etc) results in "connection refused".
- D) Using a much older version of PuTTY on the PC (one that doesn't support Host Keys)
 - Make sure PuTTY has a "**Host Keys**" configuration section (under SSH) as shown below. I've found at least one version of PuTTY that was missing this section, and would not let the connection proceed past the Keys prompt, so it never gets to prompt for a password. Login attempt just stops/fails.



Email from Paul Myers:

If they can get an SSH prompt, they have the SSH port open and SSHD is running.

To better help them you need to know what the SSH client is and OS. Windows? Putty? Linux? Linux SSH command line?

Try to have them verify:

1. Is the Password valid? Reset the Password from the Web UI for the use they are using or create a new user and try logging in.
2. SSH keys might be invalid. Delete old SSH Keys on SSH Client and try connecting again AFTER regenerating SSH keys on SecureSync.
MAKE SURE THEY CHOOSE PUBLIC KEY OR PASSWORD.
3. SSH is failing or timing out. Try to do it from within the subnet.

****VLANS / VLAN Tagging**

- Refer to: [VLANS \(*IEEE 802.1Q trunking/VLAN tagging\)](#) (in the PTP information section of this document, further below)
-

****RLOGIN**

- RLOGIN is periodically used as an alias for SSH
- "RLOGIN" clients may actually be an SSH client "in disguise"
- RLOGIN uses port 513
- We do not support RLOGIN. Nothing listens to port 513 and RLOGIN daemon is not installed.
- Reference Salesforce Case 10032 for the below email exchange

What is RLOGIN?

- It's essentially telnet for UNIX

Abbreviated from Wikipedia:

rlogin is a software utility for Unix-like computer operating systems that allows users to log in on another host via a network, communicating via TCP port 513.

The rlogin homepage is at <http://rlogin.sourceforge.net>.

rlogin is also the name of the application layer protocol used by the software, part of the TCP/IP protocol suite. Authenticated users can act as if they were physically present at the computer. RFC 1282, in which it was defined, states that: "The rlogin facility provides a remote-echoed, locally flow-controlled virtual terminal with proper flushing of output." rlogin communicates with a daemon, **rlogind**, on the remote host. rlogin is similar to the Telnet command, but has the disadvantage of not being as customizable and being able to connect only to Unix hosts.

Q. We have a question for you. When we try to RLOGIN into the SecureSync, we see the RLOGIN screen splash up and then disappear as if it is listening on that port. Is there a way to disable the port (513) in the system?

A. Reply from Paul Myers (30 May 13)

I can't see any indication the insecure rlogin protocol is present or enabled.

However, I can make a ssh connection from an Ubuntu PC wthat is running rlogin which is a alias too for ssh client.

Can you make sure they are not using the rlogin client that is some type of alias for ssh client?

On a Ubuntu server I tried to login using rlogin which turned out to be tool that allowed ssh connections.

rlogin protocol is usually built into the TCP/IP stack, however, we do not have the rlogind daemon installed and xinet.d does not have support to make a connection.

ARE THEY SURE they are using rlogin and not the rlogin that is a veneer over ssh client?

I don't recall seeing that port open when security scanning in the past ever.

DO they have telnet enabled? Maybe if its in the TCP/IP stack its turned on too?

My reply to customer

As promised, I have some information for you regarding RLOGIN and Spectracom SecureSync that should help!!

Our engineering team has confirmed that there is nothing listening on port 513 of the SecureSync. They initially didn't believe there was, but they have confirmed this port is always closed, and with no way to enable it. They also mentioned that RLOGIN is often used as an old alias for SSH, which is considered a secure connection and one that is allowed by SecureSync (when enabled). However, SSH uses port 22, not 513. Is it possible your RLOGIN client is actually an SSH client, and not an RLOGIN client?

To add to this, I can also say that we do not have the rlogind daemon even installed in the SecureSync.

I hope this alleviates your concerns about port 513. If you have any additional concerns pertaining to this subject, or if you need anything else from us, please let me know!

****tcpdump/WireShark packet capture (all products with Ethernet connectivity)**

Tcpdump

- **Note:** Also refer to tcpdump in SecureSyncCustAssist document.

(Email from Denis Reilly on 11/30/11 regarding a customer that performed a tcpdump to capture PTP traffic).

The customer appears to be using PTPv2d. I'm not too familiar with it, but I know we do have customers using it so there must be a way to get it to work.

If he tells tcpdump to record binary packets, (instead of parsing the packet and converting it to ASCII), then I think we can open the packet dump with WireShark. Refer to this page for more info:

http://www.wireshark.org/docs/wsug_html_chunked/AppToolstcpdump.html

Wireshark is a free network packet capture tools

- TCP dump is a command line packet capture tool (these captures can be opened with wireshark)

Example packet capture: [I:\Customer Service\NTP-PTP](#)

Possible File extensions for capture files customers may send to us for review:

- 1) .txt
- 2) .dmp
- 3) .pcap
- 4) .cap

Notes about packet captures:

(10.8.8.101.320 > 224.0.1.129.320) the “.320” at the end of each IP address indicates the port number where:

- Port **319** is the port for PTP Sync messages
- Port **320** is the port for PTP Follow-up/ delay request/delay response messages

Wireshark filters for specific data

- Refer to <https://wiki.wireshark.org/DisplayFilters> and <https://wiki.wireshark.org/CaptureFilters>

Examples

A) Filter by IP Address: **ip.addr == 10.2.100.170**

B) Filter by port number: **port 53**

Need to use a mirrored port (port mirroring) on switches

- Applicable to unicast packets only (not applicable to multicast)
- Switches direct traffic to the appropriate port only, so packets not meant for other ports aren't router to that port
- Won't be able to capture packets unless on the same port or traffic is also directed to another port as well (this is port mirroring)
- Some, but not all switches support port mirroring.

Frame Check Sequence (FCS) errors in a packet capture

- Refer to http://en.wikipedia.org/wiki/Frame_check_sequence
- Usually due to delay Requests being received from certain Solarflare slaves
- Some Solarflare PTP slaves send longer than usual Delay Request packets which wireshark may report as Frame Check Sequence errors.

- Sort the capture by the “info” field.

No.	Time	Source	Destination	Protocol	Length	Frame	Info
48	0.678200	10.11.94.180	10.11.94.10	PTPV2	395	Yes	Delay_Req Message [ETHER

Good Delay Request packet

- Notice no “Trailer” of all 0’s is present (after “**Type: IP (0x0800)**”) like there is in the FCS error packet

Email from Denis Reilly (2 May 2014) When we have seen FCS errors in the past, they have been accompanied by packets generated by SolarFlare cards with excessive padding. The FCS is optional, and we don't even use it. But when the SolarFlare cards sent these packets with extra 0 bytes on the end, Wireshark assumes the Frame Check sequence is part of those extra bytes, because that's where you would put an FCS if you had one. And since it is extremely unlikely that the FCS would end up being 0, WireShark flags it as an error. And one of our cards (I think the 1204-32) doesn't like the abnormally large frames.

**PAUSE frames on the network

- Pause frames are sent by an Ethernet port that is being overwhelmed.
- Wireshark capture “Protocol” field for Pause Frames: “CTRL”.
- Refer to Salesforce cases such as 7429 (Bell Alliant)

Possible fix: Pause frames stopped occurring when: “ports were shut down and then re-enabled”.

Pause Frames are related to Ethernet flow control and are used to manage the pacing of data transmission on a network segment. Sometimes, a sending node (ESX/ESXi host, switch, etc) may transmit data faster than another node can accept it. In this case, the overwhelmed network node can send pause frames back to the sender, pausing the transmission of traffic for a brief period of time.

A PAUSE frame includes the period of pause time being requested, in the form of two [byte](#) unsigned [integer](#) (0 through 65535). This number is the requested duration of the pause.

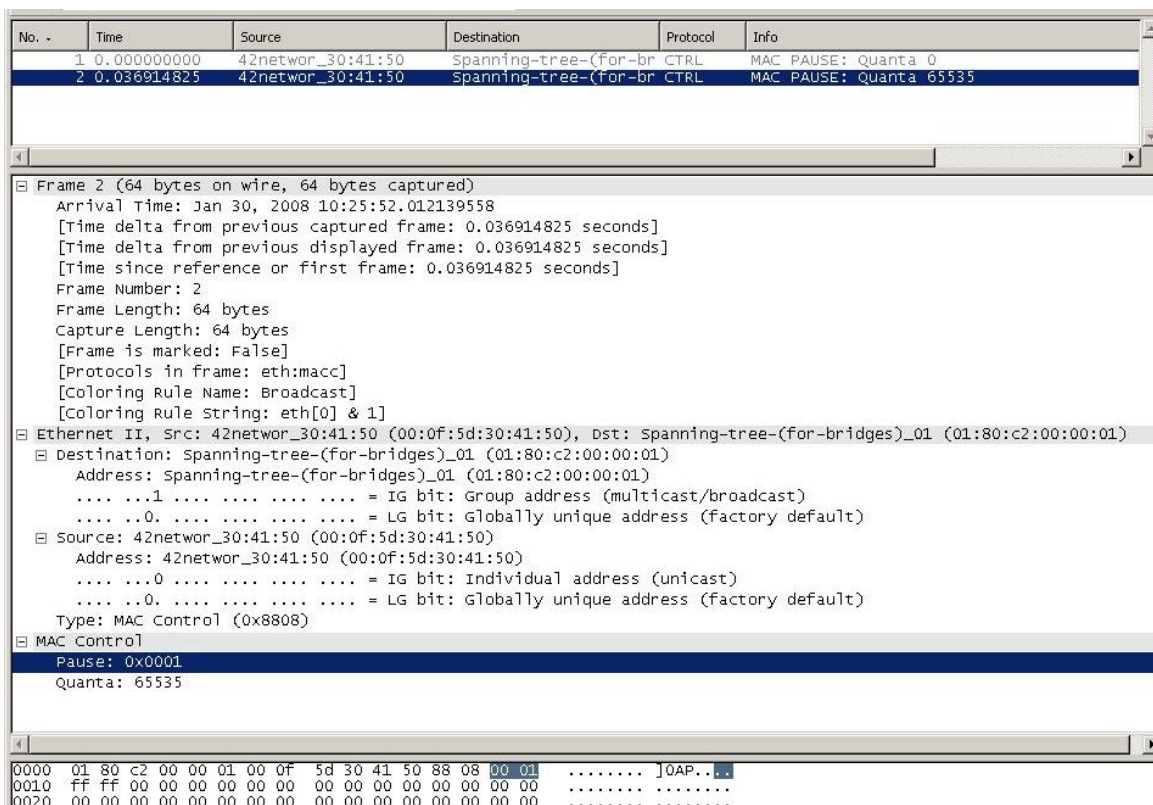
SecureSync can apparently both receive/transmit pause frames (configurable in the e1000e driver to be receive only, transmit only, or both) (in the E1000e driver, it's the **FlowControl** setting).

Flow Control

Ethernet Flow Control (IEEE 802.3x) can be configured with ethtool to enable receiving and transmitting pause frames for ixgbe. When tx is enabled, PAUSE frames are generated when the receive packet buffer crosses a predefined threshold. When rx is enabled, the transmit unit will halt for the time delay specified when a PAUSE frame is received.

Flow Control is enabled by default. If you want to disable a flow control capable link partner, use ethtool:

Example wireshark capture of pause frames (from: <http://en.wikipedia.org/wiki/File:EthernetPauseFrame.jpg>)



Question/comment from Gregory with BellAlliant regarding network switch configuration

Q. I'm wondering if the Ethernet ports need anything special parameters? The Alcatel is set force the 1 Gbps speed using the Auto negotiate limit function.

A. (reply from Dave Sohn 22 Jan 2013) I'm not aware of restrictions or configuration requirements for either the 10/100 or Gigabit ports. The pause frames wouldn't be a result of misconfiguration, but they could show an issue. I couldn't find anything definitive in the gigabit driver bug reports about flow control auto-negotiation. If they are causing problems maybe we need to disable them, but I'm not sure at this point.

Enterprise-level Network Monitoring Tools (NMS)/ NRPE (such as Nagios, Zabbix Cacti, Splunk Integration, QRadar, etc)

Refer to this same title (search for NMS) in the SecureSync tech note for info

Link to additional info: [I:\Customer Service\NMS-NNMI \(network monitoring\)](I:\Customer Service\NMS-NNMI (network monitoring))

Veritas NetBackup (“OS NetBackup”)

- Refer to “NetBackup” section in the SecureSync custassist document.
- Refer to sites such as <https://en.wikipedia.org/wiki/NetBackup>

Veritas NetBackup (earlier [Symantec](#) NetBackup) is an enterprise level [heterogeneous backup](#) and recovery suite. It provides cross-platform backup functionality to a large variety of [Windows](#), [UNIX](#) and [Linux](#) operating systems.

It is set up with a central master [server](#) that manages both media servers (containing the backup media) and clients. Core server platforms are, [Solaris](#), [HP-UX](#), [AIX](#), [Tru64](#), [Linux](#) and [Windows](#).

Oscillators/10MHz outputs (for all products)

Associated Terms (from <http://www.febo.com/pages/stability/>) and an Orolia presentations

Offset: the frequency error from the ideal (fast or slow).

Aging – change of frequency over time (also called drift).

Accuracy: refers to frequency offset of a device. is knowing that when I say I'll see you on 10 368.105 231 MHz, that's where you'll find me.

Stability how well an oscillator produces time or frequency offset over a given time interval.

Stability breaks down into three categories:

- **long term stability**, which is usually measured over periods of a day or more;
- **short term stability**, which is usually measured over periods of perhaps 0.1 second to one day.

Short term stability resembles noise and is not normally predictable. It reflects the uncertainty of the oscillator's frequency at a given instant in time.

Phase noise, which deals with very short time scales and effects that look more like unwanted modulation than a wandering frequency.

Precision or **resolution** is how many digits my measurement has. A measurement's precision can be, and frequently is, much greater than its accuracy. In other words, you can't always trust the last digits!

Drift Long term stability is dominated by a progressive change in frequency

Aging is often used synonymously with drift, but technically drift doesn't have to arise from an aging process. Drift often proceeds in one direction and may be predictable based on past performance, at least for a few days. In some oscillators drift may be more random and can change direction. Long-term drift will affect the accuracy of the oscillator's frequency unless it is corrected for.

Stability vs Accuracy

STABILITY AND ACCURACY

Often confused, it is important to know the distinction.

Another parameter

- Resolution
 - The granularity of the measurement
 - Examples: digital watches or digital scales
 - Not the same as accuracy

Stable, not Accurate

Accurate, not Stable

Not Stable or Accurate

Stable and Accurate

PNT Principles | 6/6/2018 9 orolia

FREQUENCY

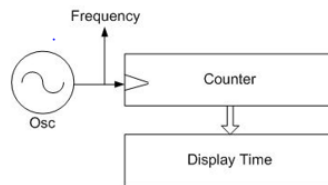
In mathematical terms, frequency is the first derivative of time.

Oscillators and Clocks

- 1/sec => Hertz
- Million/sec => MHz
- Billion/sec => GHz

Oscillator Types

- MEMs Oscillators
- Quartz Crystals
- Atomic Oscillators
 - Rubidium
 - Cesium
- H-Masers
 - Active
 - Passive
- Optical Clocks



Oscillator Types

- **MEMs Oscillators**
- **Quartz Crystals (TCXO/OCXO)**
- **Atomic Oscillators (Rubidium, Cesium, H-Masers)**
- **H-Masers (Active, Passive)**
- **Optical Clocks**

Fractional Frequency Error (FFE) for 10 MHz

Fractional Frequency Error (Fractional Frequency offset) which is calculated by dividing the frequency error (*i.e.*, the measured frequency minus the nominal frequency) by the nominal frequency. In other words:

$$\frac{\text{Frequency}_{(\text{measured})} - \text{Frequency}_{(\text{nominal})}}{\text{Frequency}_{(\text{nominal})}}$$

So, an error of +1.54 Hertz at 100 MHz is:

$$\frac{100\,000\,001.54 - 100\,000\,000}{100\,000\,000}$$

The result is 1.54×10^{-8} , often written in ASCII as $1.54 \times 10\text{e-}8$. You'll often hear rough performance described as "parts in the eleventh" or something similar. Using exponential notation like this gets you to very tiny numbers, very quickly. Here are some convenient reference points:

Offset:	Error of:
1×10^{-3}	1 Hz at 1 kHz
1×10^{-6}	1 Hz at 1 MHz
1×10^{-7}	1 Hz at 10 MHz
1×10^{-8}	1 Hz at 100 MHz
1×10^{-9}	1 Hz at 1 GHz
1×10^{-10}	1 Hz at 10 GHz
1×10^{-11}	1 Hz at 100 GHz

- Note: Fractional Frequency errors are reported in "Hertz" (Hz)
- Refer to sites such as: <http://www.nist.gov/pml/div688/generalpubs.cfm>
- Good conversion website: <http://www.convertworld.com/en/frequency/Millihertz.html>

Notes for using a scientific calculator:

- Use the "+/-" and the "Exp" buttons on the calculator to enter values in scientific notation
- The "F-E" button converts the value to scientific notation.

$$\text{FFE} = \frac{\text{Frequency error (which is the measured freq - nominal desired frequency of } 1 \times 10^7\text{)}}{1 \times 10^7 \text{ (Nominal desired frequency of "10MHz")}}$$

Therefore

$$\text{FFE for 10MHz} = \frac{\text{Frequency Error (which is the measured freq - } 1 \times 10^7\text{)}}{1 \times 10^7}$$

Examples

Email from Tom Richardson (26 Jan 15) Fractional Frequency error of 1×10^{-11} at 10 MHz is .0001 Hz. Take the error (1×10^{-11}) and multiply by the frequency (1×10^7) to get the error (1×10^{-4}) in Hertz.

The error on the screen below is the reverse, take the error in frequency, 0.000024 Hz or 2.4×10^{-5} , and divide by the frequency, 10 MHz or 1×10^7 , to get the fractional frequency error, 2.4×10^{-12} .

Given the measured frequency error. Calculate FFE

First Example: Measured frequency error in this example is 0.000024 Hz (2.4e⁻⁵)



(From **Management** -> **Disciplining** page of browser)

$$\text{FFE} = \frac{\text{Frequency Error (measured frequency - } 1 \times 10^7\text{)}}{1 \times 10^7}$$

$$= \frac{0.000024 \text{ Hz (or } 2.4 \times 10^{-5}\text{)}}{1 \times 10^7}$$

0.9999999999976 which is 2.4e⁻¹² (negative because <1)

Second Example: actual measured output frequency is exactly 1 Hz high (10,000,001 Hz)

$$\text{FFE} = \frac{1 \text{ Hz}}{1 \times 10^7 \text{ (10MHz)}}$$

So, **FFE** = .0000001 Hz, which is also 1 x 10⁻⁷ Hz (negative because <1)

Given the FFE. Calculate the measured frequency (Hz)

Note: use this to calculate expected frequency errors (+/-) based on specs in SecureSync data sheet:

10 MHz Frequency Output:

	TCXO	OCXO	Low Phase Noise OCXO	Rubidium	Low Phase Noise Rubidium	Fractional Frequency Error (FFE) values
Accuracy (average over 24 hours when GPS locked)	1x10 ⁻¹¹	2x10 ⁻¹²	1x10 ⁻¹²	1x10 ⁻¹²	1x10 ⁻¹²	

Example 1 for TCXO: The TCXO spec for “FFE” from the data sheet is 1x10⁻¹¹ typical

So the known **FFE value** in this case is 1e⁻¹¹

$$\text{FFE (} 1 \times 10^{-11}\text{)} = \frac{\text{Frequency error (which is the measured frequency - } 1 \times 10^7\text{)}}{1 \times 10^7 \text{ (10 MHz)}}$$

Measured frequency = multiply (1e⁻¹¹) by 1x10⁺⁷ = measured frequency of 0.0001 Hz (1x 10⁻⁴)

To calculate the typical Frequency range = add to and subtract from 10,000,000 the frequency above.

Example 2 for OCXO: The TCXO spec for “FFE” from the data sheet is 2×10^{-12} typical

So the known **FFE value** in this case is 2×10^{-12}

FFE (2×10^{-12}) = Frequency error (which is the measured frequency – 1×10^7)

1×10^7 (10 MHz)

Measured frequency = multiply (2×10^{-12}) by 1×10^7 = measured frequency of **0.00002 Hz** (2×10^{-5})

To calculate the typical Frequency range = add to and subtract from 10,000,000 the frequency above.

** TCXO/OCXO Oscillator disciplining

Q. With reference to, controlling the voltage to control frequency we would like to know how is it possible? The voltage will be from power supply giving out +/-5 volts and +/-12 volts as required. How can you alter the voltage?

A. Reply from Denis Reilly: Most oscillators that can be used as a frequency reference (including ours) have a control voltage that is used to fine-tune the frequency. This is because all free-running oscillators are subject to drift due to environmental factors, as well as general aging. We take the PPS signal coming from whichever reference we have chosen and “steer” the frequency of our oscillator to align with the reference.

While our particular control algorithm is proprietary, there is a good generic summary here:

http://en.wikipedia.org/wiki/GPS_disciplined_oscillator keeping in mind that we are not limited to GPS in SecureSync, and may use any of our other timing inputs (like PTP) as the timing reference.

***Simulcast radio systems 10 MHz inputs

Q. How many base stations can the 10mhz output port successfully drive?

A. Reply from Ed O'Connor (8 Dec 16) In general for some bases (such as Moto GTR8000, Harris Mastr 3, Kenwood NXR700/800) our output should drive just one base since 10MHz input on those bases have a 50 ohm termination. We can probably successfully drive 2 bases, it is up to the customer to verify, and I discourage any more than 2 bases.

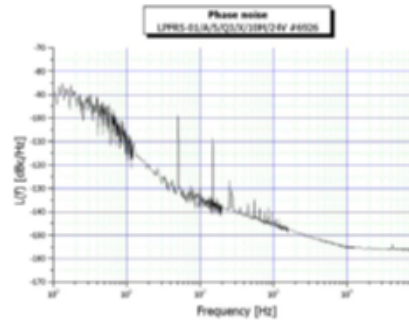
10MHz input on Tait bases has a high-z impedance. I have heard of customers driving 7-8 base stations off a single 10MHz output.

**10 MHz Phase Noise and distribution devices (for all products)

Phase Noise

PHASE NOISE

dB = decibel
= $10 * \log(\text{pwr})$
 $\log 1 = 0$
 $\log 10 = 1$
 $\log 100 = 2$
 $\log 1/10 = -1$
 $\log 1/100 = -2$
dBW = Watts
dBm = milliwatts
dBc = center freq

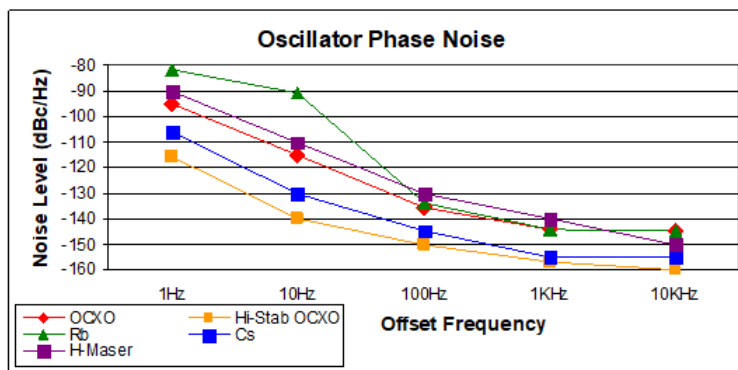


Unit of measure is – dBc/Hz

Power level below the center frequency (c) reference into the measuring receiver of (Hz) bandwidth.
Quartz crystal oscillators change frequency under acceleration.

Oscillators installed in equipment under mechanical vibration will have a higher phase noise.

OSCILLATOR PHASE NOISE



Phase noise is short term noise component indicative of the spectral purity of an oscillator signal.

(From an Orolia presentation)

Phase noise is a very short-term jitter (time domain) measurement. We measure it in terms of power levels (dB) relative to the main carrier (c). In the example of a 10 MHz oscillator, we look at the power levels generated in the offset frequencies (1Hz, 10Hz, 100Hz, 1kHz, and 10kHz). The measurement is displayed as dBc.

In this case (again OCXO vs. Cesium), we see at 1 Hz that there is less noise with an OCXO than with Cesium. The high-stability OCXO preserves the stability advantage out to 10kHz offset. Rubidium also has quite a bit of jitter close to the carrier. In low phase noise applications, an OCXO can be an excellent choice. As mentioned earlier two oscillators can be phase locked together to take advantage of the characteristics of each... such as locking an OCXO to a Cesium oscillator which provides a low phase noise output and long term stability.

****10 MHz output distribution units**

A) Epsilon Models SAS-17E and SAS-36E

Note: The Model SASe is **NOT** a 10MHz amplifier. It does not boost the signal- it only distributes it via its output ports.

- **Data sheet for SASe:** [I:\Marketing\ Product Data Sheets \(archive\)\Time & Frequency Distribution\SAS-E Epsilon_revA6.pdf](I:\Marketing\ Product Data Sheets (archive)\Time & Frequency Distribution\SAS-E Epsilon_revA6.pdf)

Note about data sheet specs: The phase noise measurements of the SASe are in addition to the phase noise of the Master Oscillator connected to the SASe.

- **Tech info about SASe:** Refer to “SASe” in the NetClock/Epsilon assist doc: <I:\Customer Service\1- Cust Assist documents\NetClockEpsilon.pdf>

B) Pendulum DA-36 (Fiber distribution)

- **Tech info for DA35 and DA36:** Refer to “SASe” in the NetClock/Epsilon assist doc: <I:\Customer Service\1- Cust Assist documents\NetClockEpsilon.pdf>
- **Datasheet for DA-36:** [I:\Marketing\ Product Data Sheets \(archive\)\Frequency Distribution \(T&M\)](I:\Marketing\ Product Data Sheets (archive)\Frequency Distribution (T&M))
- **Info on our website:** <https://spectracom.com/documents/da-36-datasheet>
- **Sales info on DA-36 (in Salesforce):** <https://na28.salesforce.com/01t80000001XvtZ?srPos=0&srKp=01t>

C) Pendulum DA-35 (discontinued)

- **Datasheet for DA-35:** [I:\Marketing\ Product Data Sheets \(archive\)\Archive\Pendulum](I:\Marketing\ Product Data Sheets (archive)\Archive\Pendulum)

D) Pendulum DA-34 (discontinued)

- **Datasheet for DA-34:** [I:\Marketing\ Product Data Sheets \(archive\)\Archive\Pendulum](I:\Marketing\ Product Data Sheets (archive)\Archive\Pendulum)

E) Pendulum DA-33 (discontinued)

- **Datasheet for DA-33:** [I:\Marketing\ Product Data Sheets \(archive\)\Archive\Pendulum](I:\Marketing\ Product Data Sheets (archive)\Archive\Pendulum)

F) Spectracom Model 8143 (discontinued)

- **Data sheet:** [I:\Marketing\ Product Data Sheets \(archive\)\Archive\Frequency Distribution\8143 - Signal Selector_Dist Amp](I:\Marketing\ Product Data Sheets (archive)\Archive\Frequency Distribution\8143 - Signal Selector_Dist Amp)
- **Tech info:** refer to “**Model 8143**” in the NetClock/Epsilon assist doc: <I:\Customer Service\1- Cust Assist documents\NetClockEpsilon.pdf>

G) Rapco Model 900, 909B module: (900 series is discontinued)

- **Refer to (spec-909module-Alava-Iss2.doc):** [EQUIPMENT\SPECTRACOM EQUIPMENT\Rapco \(Spectracom UK\)\Model 900 series](EQUIPMENT\SPECTRACOM EQUIPMENT\Rapco (Spectracom UK)\Model 900 series)

Spectracom 10 MHz generators/ phase noise

A) VersaSync

Data Sheet (VersaSync) : [I:\Marketing\ Product Data Sheets \(archive\)\Time & Frequency References\EC22S Epsilon-Clock_revB.pdf](I:\Marketing\ Product Data Sheets (archive)\Time & Frequency References\EC22S Epsilon-Clock_revB.pdf)

On our website: <https://spectracom.com/products-services/mobile-pnt/versasync-rugged-gps-time-and-frequency-reference-system>

B) SecureSync

- Data sheet:
- And [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\10 MHz Oscillators\10 MHz phase noise](#)

C) Model 9483

- Refer to datasheet
- and [EQUIPMENT\SPECTRACOM EQUIPMENT\9483 and 9489\10 MHz phase noise](#)

D) TSync series and TPRO/TSAT series timing boards

E) Epsilon Clock products (EC20S, EC22S) (discontinued products EC1S, EC2S)

- On our website: <https://spectracom.com/products-services/precision-timing/epsilon-gps-clock>

F) Models 9383 and 9389 (discontinued)

- Refer to [EQUIPMENT\SPECTRACOM EQUIPMENT\9283-9288-9289-9383-9389-9388\Phase noise](#)

10 MHz generators Phase Noise measurement comparisons

Refer to: (Product Phase noise.xls) [I:\Engineering\Products](#) and
[I:\Company Wide\Product Technical Specs\Phase Noise](#)

*Side-by-Side comparison

(listed in table: approximately lowest to highest Phase noise specs)

Note: Internal use only! Quick comparisons only. Don't spec the numbers in table. Refer to official docs, such as the Data Sheets, as listed below.

X= Not specified (all measurements in dBc/Hz)

Note: phase noise specs are not in the Model 9300 datasheet

Values are in dBc/Hz

X= Not specified

Model	1 Hz	10Hz	100Hz	1 kHz	10 kHz	100 kHz
SecureSync/9483 LPN Rubidium oscillator	-100	-128	-148	-153	-155	X
SecureSync/9483 LPN OCXO	-100	-128	-148	-153	-155	X
TSync OCXO osc	-95	-127	-144	-147	-156	-157
SecureSync/9483 OCXO	-95	-123	-140	-145	-150	X
EC31M HP OCXO	X	-120	-135	-145	-150	-150
EB03	X	-120	-135	-145	-145	-145
EC22S	X	-120	-130	-140	-145	-145
EC1S	X	-120	-130	-145	-145	-145
GPS-12R/HS	-90	-125	-135	-145	-145	X

EC-20 S	X	-120	-135	-145	-150	-150
GPS-12	-90	-120	-130	-140	-140	X
EC2S (OCXO or double oven OCXO)	X	-120	-130	-140	-145	-145
EC31M HP LPN Rb	X	-110	-130	-140	-145	-145
GPS-12R	-75	-95	-125	-140	-140	X
SecureSync/9483 Rubidium oscillator	-80	-98	-120	-140	-140	X
GPS-88 / GPS-89	-80	-90	-130	-140	-140	-140
GPS-12R	-75	-95	-125	-140	-140	X
EC2S (Rubidium OSC)	X	-80	-115	-135	-140	-140
SecureSync/9483 TCXO	X	X	-110	-135	-140	X
Pendulum Models 6688 and 6689	no known phase noise spec					

Model	Single or dual input	1 Hz	10Hz	100Hz	1 kHz	10 kHz	100 kHz
SAS-17E and SAS-36E	dual	-105	-130	-150	-155	-160	X
Rapco Model 900 series with 909B module	dual	X	-110	-135	-145	X	X
o (spec-909module-Alava-Iss2.doc): EQUIPMENT\SPECTRACOM EQUIPMENT\Rapco (Spectracom UK)\Model 900 series							
8143	dual						
DA-35 (Fiber)		Refer to: I:\Marketing\ Product Data Sheets (archive)\Frequency Distribution (T&M)					
DA-36 (Fiber)							
8140	single	Model 8140: Has poor phase noise due to how the product was designed (it was never intended to have low phase noise.). We haven't ever measured the phase noise of this product.					
8140MT (aux device)	single	We haven't ever measured the phase noise					
8140T10 (Aux device)	single	-102	-128	-142	-145	-145	-144
8140VT	Has poor phase noise due to how the product was designed (it was never intended to have low phase noise). We haven't ever measured the phase noise of this product.						
Model 1866 series	No known phase noise specs						

Model 1876 series	No known phase noise specs
-------------------	----------------------------

****Phase noise for**

other devices that don’t produce 10MHz

(listed approximately lowest to highest Phase noise specs)

Note: **Internal use only!** Quick comparisons only. Don’t spec the numbers in table. Refer to official docs, such as the Data Sheets, as listed below.

Note: Keep in mind that no matter how good the phase noise of the Frequency Standard, inserting a distribution switch will result in higher phase noise measurements, as shown below. The output of the switch will never be better than the Frequency reference.

Values are in dBc/Hz
X= Not specified

****Rubidium oscillators**

******SpectraTime SRO-100 Rubidium oscillators**

Links:

Refer to: (<\\Rocfnp01\drivedata\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\10 MHz Oscillators\Rb oscillator>)

- **link to SRO-100 manual:** http://www.spectratime.com/documents/iSync_SRO-100%20SynClock%20Manual_140522.pdf
- **Link to SRO-100 data sheet:** <http://www.spectratime.com/products/isync/gps-disciplined/SRO-100/>
- Available for /used in products such as NetClocks and SecureSync, for Rb oscillator option
- Called "Option 4" in Models 9483/9489 or 9383/9389

Part Numbers

Refer to: <https://app.bom.com/items/list-main>

- For both standard (not the low phase noise Rb) and Harris SecureSyncs: Y100R-0002-RC03
- For both Models 938x and 928x: should be Y100R-0002-RH01
- For SecureSync 447 (Low phase noise Rb): should be Y100R-0002-RC04.

Temperature specs

- Refer to Ed Saab with Motorola who have operated them above our spec.
- We spec the high temp for Rb oscillators at 55° C. Temperatures above about 60° C cause the oscillator to become highly unstable (worse than standard free-run operation). We do not recommend exceeding the temp specs!

MSDS/Hazardous material for Rubidium oscillators

- Refer to: "**Product Safety Data Sheet (PSDS)**" <..\Rubidium oscillators-MSDS - Hazardous material>
- Direct link to this document in Spectratime website: <https://www.rolia.com/sites/default/files/document-files/hazmat331.pdf>

Rubidium Oscillator Product Safety Data Sheet

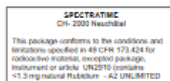
1. Introduction

The following PSDS (Product Safety Data Sheet) contains information which should answer any questions relating to handling/shipping of Rubidium (Rb) oscillators and products containing those oscillators.

2. Radioactivity

This analysis shows a total activity level of less than 1.6×10^{-4} micro-Curies per Rubidium oscillator due to Rb 87. The transportation of RbCl (Rubidium Chloride) in airplane is authorized. However, DOT (Department of Transportation) regulations require that shipping packages be labeled even when the level are within acceptable limit. Shipping documents or shipping containers need to show that the product is safe to handle.

Example of SpectraTime labeling / or shipping documents indications:



NOTICE OF NONHAZARDOUS RADIOACTIVE MATERIALS

2.1 ITEM

Frequency Standard: Rubidium

2.2 RADIOACTIVE MATERIAL

^{87}Rb , specific activity = 0.084 micro-curies/gram

2.3 DECAY MODE

Beta decay, 0.27 MeV

2.4 LOCATION & AMOUNT

The hermetically sealed glass rubidium lamp and cell assemblies each contain a small amount of rubidium metal. The rubidium is a mixture of natural rubidium containing:

73 atom percent of ^{85}Rb

27 atom percent of ^{87}Rb and separated ^{87}Rb isotope.

The ^{87}Rb is mildly radioactive with a half life of 4.88×10^{10} years. The total amount of radioactive rubidium in the frequency standard is <1.3 mg.

2.5 RADIOACTIVE MATERIAL SOURCE

SpectraTime obtains the rubidium from natural sources in the form of RbCl that is a stock item in many metal stores selling chemicals.

info@spectratime.com
www.spectratime.com

Rubidium Headquarters
+1 312 712 45 88

North American Sales Office
+1 512 471 3080

An Omega Group business

Rubidium Oscillator Product Safety Data Sheet

2.6 RUBIDIUM ACTIVITY LEVEL

Our calculations are based on the entire rubidium content being the most active ^{87}Rb so that the calculation is conservative and reflects a highest level possible. The total level of both cells combined would be less than 1.6×10^{-4} micro-curies.

2.7 EXEMPT FROM LICENSE

Since the used rubidium is a natural-occurring substance and the amount is less than 1 gram, neither the State of Arizona nor the NRC requires a license to manufacture or distribute this product.

2.8 TRANSPORTATION

The U.S. Department of Transportation under 49 CFR 173.424 allows for the unrestricted shipment of instruments containing rubidium conforming to the requirements of Table 7. Rubidium oscillators manufactured by SpectraTime are in conformance with the said Table and required limitations of the code.

3. Other Hazards Related to Rubidium Non-Radioactive Properties

3.1 DURING NORMAL OPERATION OF RUBIDIUM OSCILLATORS

No hazard

3.2 IN CASE OF RUBIDIUM RELEASE (GLASS CELL RUPTURE)

Despite the very reactive and corrosive properties of Rubidium, the limited amount of material (< 1.3 mg, < 1 mm³) contained in the oscillators does not present any hazard.

Nevertheless the following basic precaution must be taken in case of Rubidium release following a glass cell rupture:

- Do not inhale or ingest, and avoid contact with the skin and the eyes.
- Keep away from foodstuff, beverages and feed
- Wear gloves and pick-up mechanically.
- In case of contact with eyes, rinse immediately with plenty of water

4. Disposal

Material should be disposed in accordance with local, state and federal or national regulations.

info@spectratime.com
www.spectratime.com

Rubidium Headquarters
+1 312 712 45 88

North American Sales Office
+1 512 471 3080

Page 2 of 2
An Omega Group business

2.4 LOCATION & AMOUNT (of Rb material): The hermetically sealed glass rubidium lamp and cell assemblies each contain a small amount of rubidium metal. The rubidium is a mixture of natural rubidium containing:

73 atom percent of ^{85}Rb

27 atom percent of ^{87}Rb and separated ^{87}Rb isotope.

The ^{87}Rb is mildly radioactive with a half life of 4.88×10^{10} years. The total amount of radioactive rubidium in the frequency standard is <1.3 mg

Options for the oscillator

I have found this document regarding options: http://www.spectratime.com/documents/iSync_SRO-100%20SynClock%20Spec_140409.pdf

Page 4 for option explanation

SRO-100	/	XX	/	10 M	/	12 V
Type	/	Option	/	Frequency	/	Supply voltage

Rb Oscillator DAC training in NetClock SP360 / Frequency Error alarms asserted

- **Link to SRO-100 manual:** http://www.spectratime.com/documents/SRO_100%20Manual_1.pdf
- Rb oscillator takes 3 days to stabilize
- **(Application versions 3.6.3 and below)** Unlike Rb oscillators in SecureSync/9483 which only need a minimum of 3 ½ hours of continuously qualified GPS reception in order to set the newly calculated DAC value, Rb oscillators in 9383s (such as 9383 SP360) need continuous 24 hours of undisturbed (fully qualified) GPS reception in order to set the DAC. This repeats every day (not just the first day).

If there is never 24 hours of continuously qualified GPS reception, the DAC never gets set. Frequency Error alarms are likely to be asserted.

Note: NetClock 9300/9300 software version 3.6.4 added 3.5 hour set in NetClock 9300s also.

Rb Oscillator operation/training

Email from Lisa Perdue (30 Jan 14) In the SecureSync, the SRO-100 is used as the Rb oscillator. The Rb really does all the work as Keith mentions below. The SRO-100 is configured to use auto for the tracking constant (TC). The processor polls the KTS for the Freq, Phase, and DAC setting every second to display to the user. KTS uses the TC window that the RB sets in order to set the time the freq and phase error are calculated over. This window is a minimum of 1000s, but increases as the Rb becomes more stable. So as time goes on, expect that value to change less often.

The DAC value we read right from the Rb, so you can look at how the Rb calculates that in the SRO-100 manual. The SecureSync saves the DAC value every 24 hours that when we are in sync, or if the sync period is less than 24 hours (so no value has been saved yet), the value is saved at loss of lock as long as 3.5 hours have passed.

http://www.spectratime.com/documents/SRO_100%20Manual_1.pdf

1PPS alignment (both initial alignment and realignment after reference is lost/then restored)

- We tell the SRO-100 to use Track mode and then Sync Mode (Track State 1 and then Track State 2) for initial alignment and for re-alignment after a reference is restored.

The SRO-100 first snaps to within 133 ns. Then, it will start to very slowly slew in to the 1PPS input reference. Note this slewing can take hundreds of seconds to complete.

From the SRO-100 manual:

iSync+™ Smart SRO-100 SynClock+™ Manual

2.4.1 THE "TRACK" MODE AND THE "SYNC" MODE.

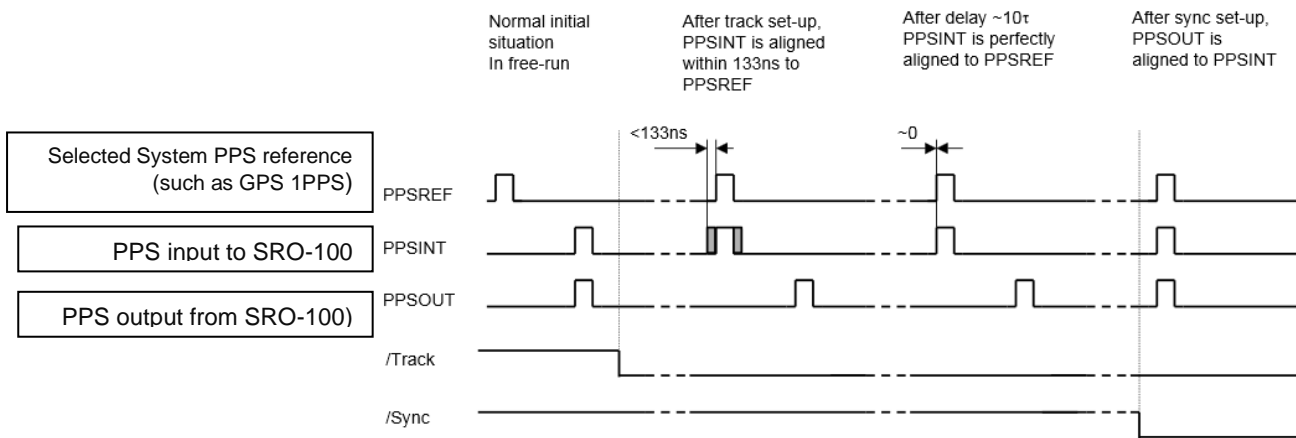


Fig. 2-6 : "Track" mode and "Sync" mode.

When "track" mode is set-up, the PPSINT is aligned to the PPSREF within 133 ns. Then the phase comparator starts the mid-term frequency stability analysis of the PPSREF. The tracking loop time constant is adjusted in consequence and the SRO-100 start to track the PPSREF.

During all of this operation, the position of the PPSOUT is not changed. The PPSREF timer is working on an independent way. So the PPSOUT will not suddenly jump when the SRO-100 starts to track a PPSREF.

When "sync" mode is set-up, the PPSOUT is aligned to PPSINT. "Sync" mode can only be set-up when the SRO-100 is already tracking successfully a PPSREF.

If "sync" mode is set-up just after the SRO-100 start to track a PPSREF, the phase-time difference between PPSOUT and PPSREF can be as big as 133 ns. Of course, the tracking loop will reduce this difference and will bring it nearly to null in case the noise of the PPSREF is low.

2.4.2 THE FREQUENCY LEARNING

Question/observations from Harris about SP360 (replies from Paul Myers)

Lock time

- Rb oscillator takes 3 days to fully stabilize
- Does the unit remember its training through a power cycle event or must it retrain after every power interruption?

A (from Paul Myers): Paraphrasing the manual.

When the Rb is tracking the PPSREF of a master oscillator, in reality, it aligns its frequency to the one of the master. The learning process is simply the memorization of this frequency from time to time to use it after a reset or Power-On. By default, when the Rb is continuously and successfully tracking a PPSREF, the average value of the frequency is saved in EEPROM every 24 hours.

- must this be a continuous 3 days or is it a total of 48 hours of disciplined operation that could have intervals of signal jamming interspersed?

A (from Paul Myers) The 3 days is time of POWERED SRO operation to allow the SRO-100 physics package to stabilize. The SRO-100 requires 24 hours of disciplined operation to set its DAC setting in persistent memory. I recommend disciplining the first 3 days, but being powered is all that is needed to stabilize the physics package.

Q. 1pps location when sync'ed seems to not be precise – the units do not settle to the same place each time.

A. (from Paul Myers) The 1PPS would be limited by the precision and accuracy of the GPS 1PPS and the recovery behavior of the

SRO-100. The 1PPS re-acquisition location does seem to vary. The SRO-100 Rb 1PPS is adjusted to within 133nsec and slews afterwards. This adjustment point is not the same. The GPS 1PPS accuracy might contribute also. Tom Richardson and I observed a slow trend towards recovery, but I did not observe it long enough between tests cycles to determine

Q. Saw 1pps jumping 100 nsec during and after the first site 4 recovery; this was not seen during holdover of after on the other three tests.

A. (from Paul Myers) The output Rb 1PPS is aligned to the nearest 10MHz clock edge. Normally, this Rb output 1PPS gets aligned with a clock edge and it appears stable. If the Rb 1PPS is between either edge, it can appear to choose one then the other one. Overtime, one edge is aligned with and the jumping can stop. The alignment in holdover is static typically.

Q. The amount of 'walk in' appears to vary quite a bit. The last run had 75 nsec of 'walk in' Is there a worst case number for this that would never be exceeded?

A. (from Paul Myers) I believe the worst case is the $\leq 133\text{nsec}$ Rb initial alignment plus the smoothed 1PPS GPS input accuracy. The SRO-100 internal 1PPS is aligned with the GPS 1PPS input smoothing it in the disciplining process reducing any jitter. I will double check with Tom Richardson, but my observations were around or less 133nsec. The Rb 1PPS seemed to slew slowly afterwards.

PEM: For how long is it dropping out each day?

- They are inquiring if loss of reception during initial 3 day power-up of the unit will affect the initial settling of the oscillator. I suspect not, but didn't know for sure.

I remember asking about training way back when we first were testing the Rb 9383 NetClock – but do not recall for sure what the answer was – and Secure sync may be different anyway. The rb need a three day training period; does losing satellites during training reset the rb training process or merely interrupt it? More to the point – would a daily loss of satellite tracking prevent the rb from ever completing training – and if rb training is not completed – how will that affect holdover operation?

PEM: The first day is critical. The Rb saves at the end of the first 24 hours. Recall during the first day, if I removed the GPS signal by pulling the antenna the drift of the Rb was so great we had Frequency alarms quickly? The initial value won't be saved.

If they go out of sync and the Rb is NOT tracking, they do NOT save a frequency correction value to the EEPROM.

http://www.spectratime.com/documents/SRO_100%20Manual_1.pdf

THE FREQUENCY LEARNING

- When the SRO is tracking the PPSREF of a master oscillator, in reality, it aligns its frequency to the one of the master.
- The learning process is simply the memorization of this frequency from time to time to use it after a reset or Power-On.

By default, when the SRO is continuously and successfully tracking a PPSREF, the average value of the frequency is saved in EEPROM every 24 hours.

With the command **FSx<CR>**, it is possible to cancel the learning or to make a immediate save.

PEM: The SecureSync I believe saves a value requiring a minimum of 3.5 hours continuous tracking by a change David Sohn made. The SecureSync will normally have the SRO-100 save the value every 24 hours of continuous tracking. IF it exits tracking in ≥ 3.5 hours it will save the current value. The performance of the Rb will be reduced.

The NetClock 93xx uses the default behavior saving at the end of 24 hours.

THE FREQUENCY IN USE

With the PPSREF facilities, a different frequency can be in use in different situations. Let know first, that the frequency just currently in use is located in a single register, and that this register can ever be read by the user. The command to read this register is: **FC+99999<CR>**.

On a SRO connected through the serial interface to a terminal, it is possible to follow the evolution of the tracking by this way.

The frequency, or frequency correction in use in different situations is as following:

- After a Reset or Power-On, the frequ. corr. is copied from the EEPROM to the RAM and then is used.
- After the start of a tracking, the internal frequ. corr. is the one of the EEPROM.
- During a tracking, the frequ. corr. in use changes continuously to align as good as possible the PPSINT to the PPSREF.

By default, the average value is saved in EEPROM every 24 hours.

- If the SRO is stopped in its tracking, and put in FREE RUN mode by the user, with the command TR0 for example, the frequency correction in EEPROM is retrieved and loaded in RAM to be used.
- If the tracking is stopped because the PPSREF signal disappears suddenly or is strongly degraded, the integral part value of the regulation loop becomes active. This is to avoid a frequency jump in case the PPSREF signal comes back again. This mode of operation is called hold-over.

- The other question from Joel “Additionally, Keith, will it be more susceptible to freq errors if it loses GPS signal daily?” If they have a newer version of software, they should only get the Frequency alarms if the oscillator is unstable – not due to loss of reception for a few hours- correct?

PEM: If tracking is lost dialing the SRO-100 in the 93xx will NEVER save a EEPROM DAC value. The tracking will be poor and every day is a First day of operation with HIGH DRIFT.

Yes for the first day definitely because the drift will be higher and during the GPS outage drift will occur and frequency errors could be detected. The oscillator will be unstable the first day and drift fast.

IT IS REQUIRED THEY IMPROVE RECEPTION AT THIS SITE FOR CORRECT OPERATION USING A 93XX. Either improved antenna placement if sky view due to satellite obscuration or if interference is an issue a filter must be installed to remove the interfering signal.

Rb Oscillator training in SecureSync and 9483 /Frequency Error alarms asserted

- Unlike Rb oscillators in 9383s which need 24 hours of continuously qualified GPS reception to set the newly calculated DAC value, Rb oscillators in SecureSyncs and 9483 only need a minimum of continuous 3 1/2 hours of undisturbed (fully qualified) GPS reception in order to set the DAC. This repeats every day (not just the first day).
- If there is never 3 1/2 hours of continuously qualified GPS reception, the DAC value never gets set. Frequency Error alarms are likely to be asserted.

Rubidium Monitor

From the SRO-100 manual:

HH: Read-back of the user provided frequency adjustment voltage on pin 2 (0 to 5V)

GG: reserved

FF: peak voltage of Rb-signal (0 to 5V)

EE: DC-Voltage of the photocell (5V to 0V)

DD: varactor control voltage (0 to 5V)

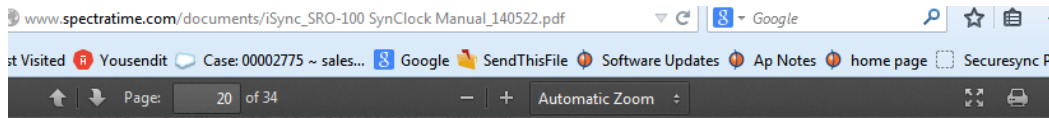
CC: Rb-lamp heating current (Imax to 0)

BB: Rb-cell heating current (Imax to 0)

AA: reserved

“State Retry limit met”: According to Paul Myers, we generate this message when we have trouble reading the monitor value (it isn’t generated in the oscillator),

A) Rb peak voltage error (0 to 5v)



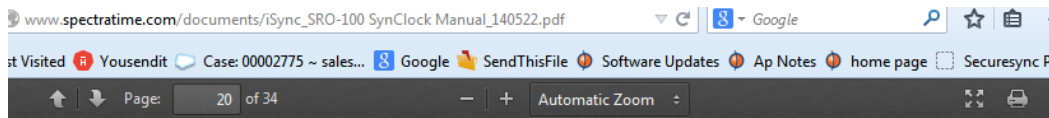
- **Rb signal level.**

FF: Peak voltage of Rb signal level (0 to 5V for \$00 to \$FF)

This signal monitors the rectified value of the AC signal produced by the interrogation process of the Rb dip absorption. During warm-up time this signal is approximately 0V and after it stabilizes to a nominal value of 1 to 5V. As long as this signal is too low the internal SRO-100 control unit sweeps the Xtal frequency in order to find the Rb absorption dip.

Jun 4 10:12:17 Spectracom Spectracom: [system] 2014 155 10:00:51 000 Rb peak voltage error (val=0, min=51, max=255)
Jun 4 10:12:16 Spectracom Spectracom: [system] 2014 155 10:00:50 000 Rb peak voltage error (val=0, min=51, max=255)
Jun 4 10:12:15 Spectracom Spectracom: [system] 2014 155 10:00:49 000 Rb peak voltage error (val=0, min=51, max=255)
Jun 4 10:12:14 Spectracom Spectracom: [system] 2014 155 10:00:48 000 Rb peak voltage error (val=0, min=51, max=255)
Jun 4 10:12:13 Spectracom Spectracom: [system] 2014 155 10:00:47 000 Rb peak voltage error (val=0, min=51, max=255)
Jun 4 10:12:12 Spectracom Spectracom: [system] 2014 155 10:00:46 000 Rb peak voltage error (val=0, min=51, max=255)

Keith's response: These are values reported by the SpectraTime SRO-100 Rubidium oscillator to the SecureSync. Below is the link to the SRO-100 manual and an excerpt from the manual which discusses what this value is.



- **Rb signal level.**

FF: Peak voltage of Rb signal level (0 to 5V for \$00 to \$FF)

This signal monitors the rectified value of the AC signal produced by the interrogation process of the Rb dip absorption. During warm-up time this signal is approximately 0V and after it stabilizes to a nominal value of 1 to 5V. As long as this signal is too low the internal SRO-100 control unit sweeps the Xtal frequency in order to find the Rb absorption dip.

From the above description, the entries you provided indicated the SecureSync was likely booted-up a couple times today (power cycled/rebooted, etc). There should be corresponding entries in the other logs that indicate if the unit was booted up just before these log entries were asserted. If the unit was booted-up just before these entries were asserted, these are expected entries.

B) DC-voltage of the photocell

- **DC-Voltage of the photocell.**

EE: DC-Voltage of the photocell (5V to 0 for \$FF to \$00)

This signal corresponds to the transmitted Rb light level. This is the light of the Rb lamp which is partly absorbed by the Rb cell. The nominal photocell voltage is in the range 2.0 to 3.5 V but must stay stable after the warm-up time. The photocell voltage is related to the internal reference 5 V voltage. The full scale corresponds to the coded value \$00 and the zero (no light) corresponds to the coded value \$FF

C) Frequency adjustment voltage

- **Frequency adjustment voltage.**
DD: VCXO control voltage (0 to 5V for \$00 to \$FF)

This parameter corresponds to the voltage applied to the varicap of the internal VCXO.

In normal operation this voltage is mainly temperature dependent in the range 2 to 3V in order to compensate the frequency versus temperature characteristic of the crystal resonator.

During warm-up the control unit generates a ramp of this parameter from 0.3 to 5V and from 5V to 0.3V until the Rb dip absorption is found.

D) Rb lamp heating limiting current

- **Rb lamp heating limiting current.**
CC: Rb lamp heating limiting current (Imax to 0 for \$00 to \$FF)

This parameter corresponds to heating limiting current applied to the lamp heating resistive element. In normal operation, this current depends on the ambient temperature but should stay between \$1A and \$E6. During warm-up, this current is set to its maximal value \$00 (no current limiting).

E) Rb cell heating limiting current

- **Rb cell heating limiting current.**
BB: Rb cell heating limiting current (Imax to 0 for \$00 to \$FF)

This parameter corresponds to heating limiting current applied to the cell heating resistive element. In normal operation, this current depends on the ambient temperature but should stay between \$1A and \$E6. During warm-up, this current is set to its maximal value \$00 (no current limiting).

**Stratum timing levels for all Frequency products

Link to document that discusses stratum level timing for frequency outputs: I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\sync_an02-StratumLevelDefined.pdf

Max cable distances for 10 MHz output

Q. How long of a 10 MHz cable can I run?

A. To calculate the recommended maximum cable length, you need to know the output level from the 10MHz reference and the sensitivity (expected signal level) of the device.

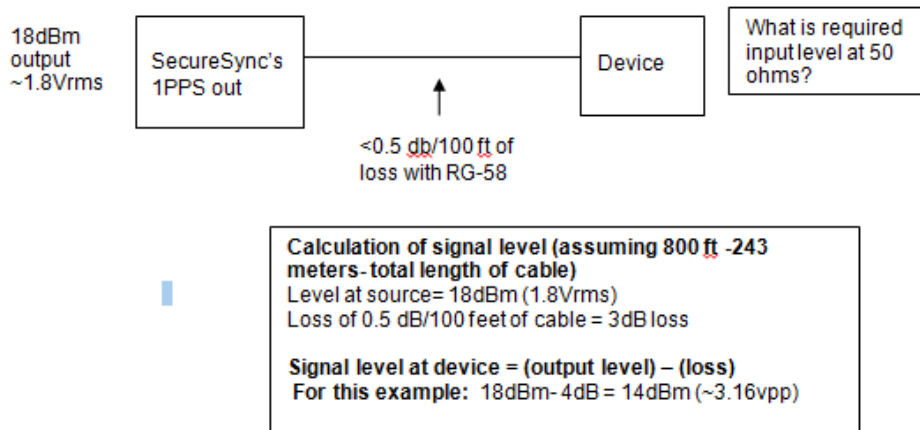
Attenuation of RG-58 at 10MHz: 1.5dB/100 feet

Example output levels:

SecureSync= +13dBm into 50 ohms (~3vpp or ~1Vrms)

EC20S= +12 +/-2 dBm (~3vpp or ~1Vrms)

Note regarding the SAsE: When an Epsilon SAsE is used, there is **no** gain or loss on its outputs (they have 0db gain) so the cable loss is the total distance from 10 MHz reference to 10MHz receiver.



****Link to a dBm / Vrms / Vpp calculator:** http://www.jneuhaus.com/volts_to_dBm.html

Email Keith sent to a customer

The total distance of 10 MHz cable that can be run is based on the output level of the EC20S versus the 10 MHz cable loss in between as well as the input sensitivity/required signal level of your test equipment. Before this recommended maximum length of cable can be calculated, you will need to know from the vendor of your test equipment, what the minimum input 10 MHz signal level is required. This information may be found in their user manual or you may need to contact directly the vendor of the test equipment and ask them for this information.

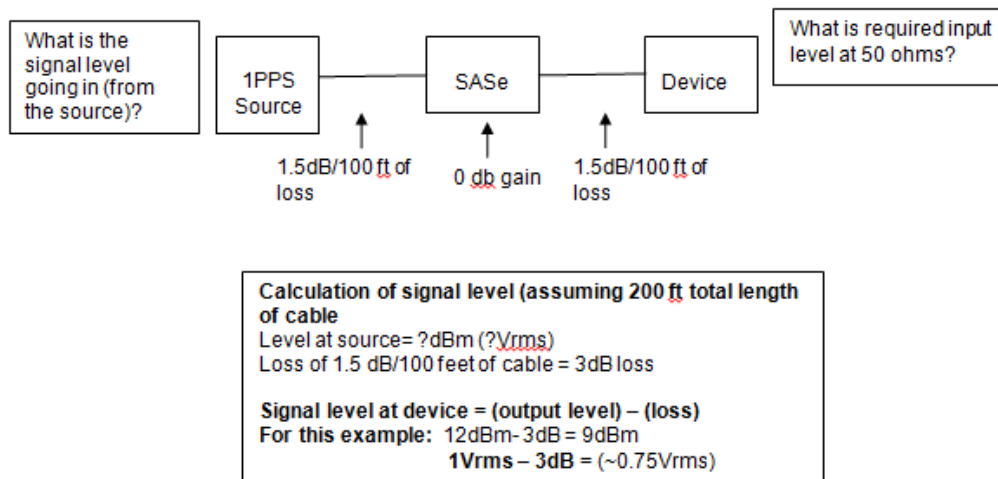
In general, the method to calculate the 10MHz signal level at the test equipment end of the 10 MHz cable is to subtract the cable loss of RG-58 from the output level of the EC20S. Please keep in mind that the SAS36E is a 0dB gain device (it provides no amplification of the 10MHz signal- it just provides multiple outputs). Based on this fact, the signal loss is based on the total length of cable attached to the EC20S to your test equipment.

As shown below, the 10MHz output of the EC20S is about 12dBm. The attenuation of the RG-58 cable (at 10MHz) is about 1.5dB per every 100 feet (30 meters) of cable that is between the EC20S and your test equipment. In this example below, a total cable distance of 200 feet (61 m) between the EC20S and the SAS36E (100 feet to the SAsE and 100 ft to the test equipment results in a 10MHz signal level of about 9.63Vrms.

Q. Is the coax line of 10MHz signal can be run along with 208V, 110V and 3phase 208V AC lines

A. Keith's reply: We do not recommend running the 10MHz cable near any power lines. Noise from nearby power cables can be coupled into the 10MHz cable (even though it's a shielded cable). This can become a factor with longer distance 10 MHz cables.

A) From an SAsE (SAS-17E, SAS-17E-IR or SAS-36E)



As the SAsE's output level is the same as the input level (+/- 10%) the output level is dependant upon the input levels.

****Link to a dBm / Vrms / Vpp calculator:** http://www.jneuhaus.com/volts_to_dBm.html

The total distance of 1PPS cable that can be run is based on the output level of the 1PPS generator versus the 1PPS cable loss in between the generator and the SAsE, as well as the input sensitivity/required signal level of your test equipment. Before this recommended maximum length of cable can be calculated, you will need to know both the level of the 1PPS output generator, as well as what the minimum input 10 MHz signal level is required. This information may be found in their user manuals or you may need to contact directly the vendors of the equipment and ask them for this information.

In general, the method to calculate the 1PPS signal level at the test equipment end of the 1PPS cable is to subtract the cable loss of RG-58 from the output level of the 1PPS generator. Please keep in mind that the SAsE is a 0dB gain device (it provides no amplification of the 1PPS signal- it just provides multiple outputs). Based on this fact, the signal loss is based on the total length of cable attached to the PPS generator to the SAsE

The attenuation of the RG-58 cable (at 1PPS) is about 1.5dB per every 100 feet (30 meters) of cable that is between the PPS generator and the SAsE, and from the SAsE to the equipment.

Note that as the SAsE provides no gain or loss of the 1PPS signal, the maximum cable distance from the PPS generator to the end devices is the same whether or not the SAsE is installed inline.

****Allan Variance measurements (for all products)**

Refer to: <I:\Company Wide\Product Technical Specs\Allan Variance>

Allan variance is a method of analyzing a sequence of data in the time domain, to measure frequency stability in oscillators. This method can also be used to determine the intrinsic noise in a system as a function of the averaging time.

From Wikipedia:

The **Allan variance (AVAR)**, also known as **two-sample variance**, is a measure of [frequency](#) stability in [clocks](#), [oscillators](#) and [amplifiers](#). It is named after [David W. Allan](#)

The *Allan variance* is intended to estimate stability due to noise processes and not that of systematic errors or imperfections such as frequency drift or temperature effects. The Allan variance and Allan deviation describe frequency stability, i.e. the stability in frequency. See also the section entitled "[Interpretation of value](#)" below.

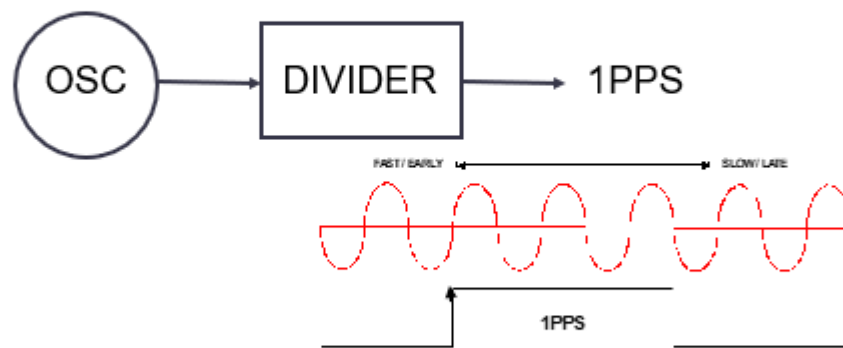
Time is derived from Frequency

TIME IS DERIVED FROM FREQUENCY

Time is simply a divided function of frequency.

The 1 pulse-per-second (PPS) is the epoch or definition of the on-time marker of a clock.

Further divisions of the 1PPS is used to keep track of seconds, minutes, hours, days, and years.



Clock 1PPS rising edge is typically on-time: HH:MM:SS.000000000

When deriving time from frequency, the oscillator (which is usually 10 MHz), is put through a divider (10 million), resulting in a 1 pulse per second (pps) output. The rising edge is the “on time” point of a clock (.000 point). It identifies the start of the 1 second period. The 1PPS output is a common output signal clock devices. The synchronization accuracy between two clocks can be easily measured by simply comparing the 1PPS output signal on an oscilloscope or counter.

RELATIONSHIP OF TIME AND FREQUENCY

If the frequency is fast the time moves early.

If the frequency is slow it moves late.

Frequency aging, offset, and temperature of the oscillator cause the time to move fast or slow.

Time is typically related to UTC.

Time is obviously impacted by frequency. If we have a fast frequency reference, our clocks will move early, and if they are slow they will move late. Temperature, aging, offset, etc. determine whether a clock moves fast or slow. Clocks continually locked to UTC allow for the correction and filtering of these variances. To include earth rotation variances, leap second etc.

1PPS outputs/1PPS cable delays/max cable distances (for all products)

- Recommended cable for 1PPS distribution: 50 ohm coax such as RG-58 cable.

**Max cable distances that can be run for 1PPS outputs

- Due to **slow rise-times**, we don't recommend using a cable length greater than **about 800 feet** (slow rise-times can cause false triggering)

Max recommended 1PPS cable distances

Q. How long can the RG-58 cable for the SecureSync's 1PPS output be to an SASe.

A. Reply from Dave Lorah on 9/16/11, based on engineering feedback:

We verified overnight running a 1PPS through a SAS synchronizing a SecureSync through around 800 feet (243 meters) of RG58 cabling. The maximum cable length is not determined. Hopefully 800 feet is longer than you need. Of course, running through that much cable, you will have to compensate for the propagation delay of the cable and the effects of the slower rise time. The propagation delay of RG-58/U cable is about 1.51 ns/ft.

Q. He also wants to send the signals 1000 ft (304 meters). Will twisted pair or coax work better for him? And I'm assuming he will need an amplifier.

A. Regarding the question on running 1PPS through 1000 feet (304 meters) of cable, I ran this one by our engineers. According to our calculations, we believe 1000 feet of cable will be acceptable, without the need for an amplifier. It may depend on the sensitivity of the receiver (the device at the opposite end of the cable). I would recommend using a 50-ohm coax cable, such as RG-58 cable for this connection.

Note that with this length of cable, it is extremely important to terminate the end of the cable (at the receiver end) into 50 ohms. If the receiver has a 50-ohm input, no additional termination will be required. However, if the device has a high input impedance, a 50-ohm load should be installed at the end of the cable. This will help preventing ringing/reflections of the signal occurring in the cable. This can easily be added with the use of a BNC "T" connector.

With our calculations, we estimate the signal will be reduced to about 3.3 to 3.5 volts peak, through a 1000 feet (304 meters) of cable and into a 50 ohms load. This should be sufficient signal levels for the use by the receiver.

Note: Below is a reply from Tom Richardson followed by reply from Mark McGregor about this

TR-I thought this had come up before. I think 1000 feet will work. Depends on sensitivity of receiver. Attenuation of frequencies will cause rise time to increase(slow). DC resistance of the cable will attenuate the signal level. 10.8 ohms/1000 ft.

MM-It will be estimated that the option card 18 will be down to 3.6V at a 50-ohm load at the end of 1000 feet (304 meters) of cable with 10.8/1000 feet DC resistance. I would say 3.5V to 3.3V to give a little margin on the estimate.

It is critically important that the long cable is terminated into 50 ohms for signal integrity, as the SecureSync driver is not 50-ohm source impedance. If the customer box does not present a 50-ohm load, they will need to add a T connector with a 50-ohm load in shunt to the customer input.

Estimation Details:

The SecureSync option card 18 1PPS signal lost due to DC resistance is estimated as follows. For the main board 1PPS output we make 4.3V into a 50-ohm load. This is $3.4V/50\text{ ohm} = 0.086A$. The supply to the SecureSync output driver is 5V. If we say 5V, we know that 0.7V is lost in the driver with a 50-ohm load. If you take the $0.7V/0.086A = 8.1\text{ ohms}$ for the main board 1PPS driver. The option card 18 output driver is slightly higher source impedance than the main board, due to using 5.6-ohm output resistors on the gate drivers instead of 4.75 ohms. This difference adds another 0.21 ohms to the source impedance for 8.3 ohms. Now if you have 1000 feet of cable at 10.8 ohms/1000 feet, we must add another 10.8 ohms to the driver source resistance for a total of 19.1 ohms. We can now do a voltage divider from 5V power supply of the option card 18 gate output drivers to the 50-ohm load including the Option card 18 driver source impedance and cable losses. $5V \cdot (50/(50+19.1)) = 3.6V$.

Q. What about running 1PPS through 1600 or 2400 ft of cable

A. Reply from Tom Richardson (4/4/12)

I would not recommend trying 1PPS through 1600 or 2400 feet of cable. Calculations show about 800 feet is max. Look for alternate methods. Slow rise times can cause false triggering.

Also in my experience ground loops on this length of cable can be a problem. A ground loop voltage might cause false triggering.

Look for differential or fiber optic solutions. I don't know what we have, Dave (Sohn) might know

Calculate the max cable distance for 1PPS

To calculate the recommended maximum cable length, you need to know the output level from the 1PPS output reference and the sensitivity (expected signal level) of the device.

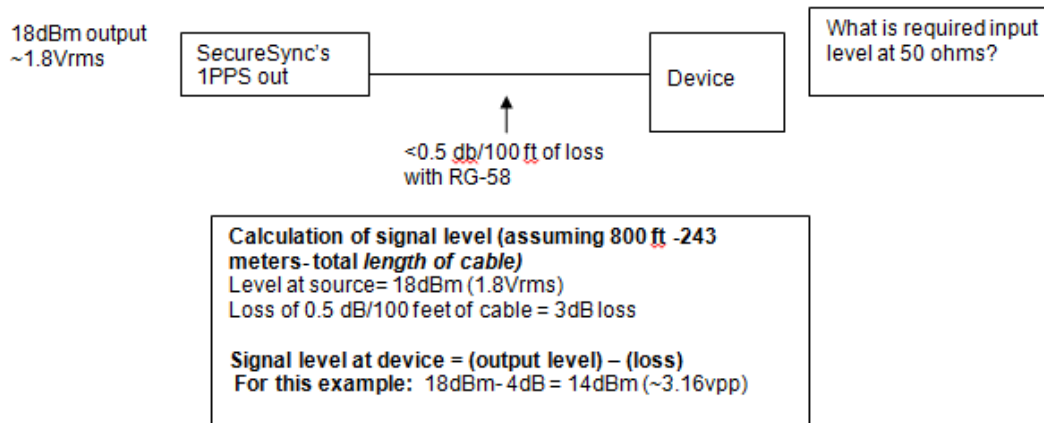
Attenuation of RG-58 at 1PPS: 1.5dB/100 feet

Example 1PPS output level:

SecureSync= +18dBm into 50 ohms (~5vp or ~1.8Vrms)

Example configurations:

SecureSync



****Link to a dBm / Vrms / Vpp calculator:** http://www.jneuhaus.com/volts_to_dBm.html

Email Keith sent to a customer

To begin, the SecureSync's 1PPS output can drive up to 50 ohms, at an amplitude of 5vp-p. The maximum recommended cable that can be run is dependent upon the cable loss at 1Hz, and the input sensitivity of the other device you are connecting the 1PPS output to (the other device's minimum required input level of the 1PPS signal, with 50-ohm end termination).

Cable loss of 1PPS into coax cable, such as RG-58 is extremely low (less than 0.5dB per every 100 feet of cable). This inherently helps the cable run be hundreds of feet long.

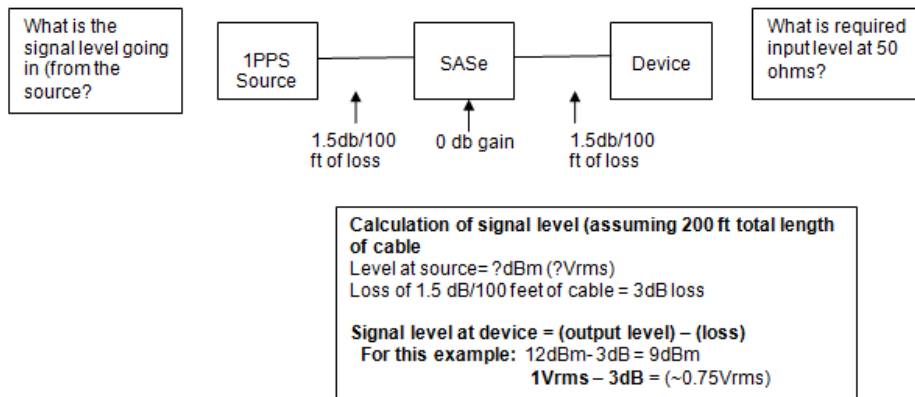
We recommend using a 50-ohm coax cable, such as RG-58 for 1PPS output. The total cable loss of 1PPS at 800 feet is about 4dB. With this loss, the 5vp-p output of the SecureSync will drop to around 3.2vp-p at the end of the 800 feet of cable (with a 50 ohm terminator applied, as recommended). If the other device can accept a 1PPS input signal at about 3.2 volts peak-to-peak, an 800 foot, 50 ohm cable run can be used.

If the other device has a 50 ohm input impedance, no additional termination at its input is required. However, if the other device has a high impedance input, it's very important to add a 50 ohm terminator/load at the input of the other device (don't add any termination at the output of the SecureSync). Otherwise, cable reflections (ringing of the 1PPS signal) are highly likely to occur, resulting in potential timing issues. Note that at 1000 feet of cable, the 1PPS signal is still about 3v peak to peak, into 50 ohms.

At these longer cable distances, the cable propagation delays for the 1PPS signal may need to be accounted for, to optimize its timing capabilities. The SecureSync's 1PPS output allows for cable propagation delays to be accounted for, as desired (via the **Setup -> Outputs -> 1PPS** page of the browser, **Offset** field- entered in total nanoseconds of cable delay).

Note the 1PPS propagation delay of RG-58/U coax cable is about 1.51 ns/ft. For an 800 foot cable run, this is about **1208** nanoseconds (1.2 microseconds).

A) From an SAsE (SAS-17E, SAS-17E-IR or SAS-36E)



As the SAsE's output level is the same as the input level (+/- 10%) the output level is dependant upon the input levels.

As the SAsE's output level is the same as the input level (+/- 10%) the output level is dependant upon the input levels.

****Link to a dBm / Vrms / Vpp calculator:** http://www.jneuhaus.com/volts_to_dBm.html

The total distance of 1PPS cable that can be run is based on the output level of the 1PPS generator versus the 1PPS cable loss in between the generator and the SAsE, as well as the input sensitivity/required signal level of your test equipment. Before this recommended maximum length of cable can be calculated, you will need to know both the level of the 1PPS output generator, as well as what the minimum input 10 MHz signal level is required. This information may be found in their user manuals or you may need to contact directly the vendors of the equipment and ask them for this information.

In general, the method to calculate the 1PPS signal level at the test equipment end of the 1PPS cable is to subtract the cable loss of RG-58 from the output level of the 1PPS generator. Please keep in mind that the SAsE is a 0dB gain device (it provides no amplification of the 1PPS signal- it just provides multiple outputs). Based on this fact, the signal loss is based on the total length of cable attached to the PPS generator to the SAsE

The attenuation of the RG-58 cable (at 1PPS) is about 1.5dB per every 100 feet (30 meters) of cable that is between the PPS generator and the SAsE, and from the SAsE to the and to the equipment.

Note that as the SAsE provides no gain or loss of the 1PPS signal, the maximum cable distance from the PPS generator to the end devices is the same whether or not the SAsE is installed inline.

****1PPS Propagation/Cable delays**

The propagation delay of:

- **For cable type RG-58/U (CA01-XXX) use 1.54ns per foot.**
Actual Cable used: Belden 8259
<http://www.belden.com/techdatas/english/8259.pdf> (page 2 nominal delay)
- **For cable type RG-8 (CAL7-XXX) use 1.17ns per foot.**
Actual cable type used: Belden 7810A
<http://pdf2.datasheet.su/belden/7810a%20010500.pdf> (page 2 nominal delay).
- For cable type LMR-400 (CAL7P-XXX) use 1.34ns per foot.
Actual cable used: Times Microwave LMR-400-LLPL
<http://www.timesmicrowave.com/products/lmr/downloads/82-85.pdf> (page 2 time delay)

If one or more SAS-17E/SAS-36E installed between SecureSync (or other 1PPS source) and the 1PPS Slaves.

- For each SASe installed, the internal 1PPS delay (**PPS input** to each **PPS output** is 35ns)

From the SASe datasheet

Pulse

- Regenerated pulse with same pulse width / period as input
- TTL level, BNC 50 Ω
- Pulse delay between input and output : 35 ns \pm 0.5 ns

- There are NO input/output delay compensations available within the SASe itself
- For more info/example draft emails for delays with an SASe installed, refer to “**1PPS output Delay and Jitter**” in the SASe section of: <..\NetClockEpsilon.pdf>

****1PPS Fiber Optic distribution**

*****SI Tech Fiber converter equipment**

Refer to: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SI Tech \(fiber converters\)](I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SI Tech (fiber converters))
for datasheets on these SI Tech products

Contact info for SI Tech

For application engineering assistance: 630-761-3640 FAX: 630-761-3644 S.I.Tech, P.O.Box 609, Geneva, Illinois 60134
U.S.A. Web site: <http://www.sitech-bitdriver.com>

Note regarding quote stored in this folder (email from Dave Sohn 4/11/12)

This was the quote I received a while ago. You may need to talk to SI Tech if you need something a little different than what was quoted. I can talk to you more directly about it if you want

Associated parts

Spectracom P/N	SI Tech P/N	Description
MP29-0000-0001	2817-T/R-SM	Fiber converter
MP29-0000-0002	2817-T-SM	Fiber converter
MP29-0000-0003	2121	Power supply for fiber converter
MP29-0000-0004	2166	Power supply for fiber converter
MP29-0000-0005	2817-T/R	
MP29-0000-0006	2856-4R	TTL to Fiber, 4 Chan RM, MM, ST, 110 AC (TTL to Fiber Optic Bit-Driver) S.I. Tech Model 2856 is designed to convert TTL data to a light signal so that information can be transmitted over fiber optics. At the remote end, another 2856 will convert this data from light to TTL format.
MP29-0000-0007	9024A-12	(Fiber Cluster) Fiber Optic Distribution Box, 1 to 12
MP29-0000-0008	9024A-4	(Fiber Cluster) Fiber Optic Distribution Box, 1 to 4
MP29-0000-0016	2817-R-SM	RECEIVER TTL to Fiber, RX, SM, ST, 1300nm
MP29-0000-0019	2062-MM-SM-ST (2062-MM/SM-ST)	Model 2062 - Optical Repeater Mini Bit-Driver

Purpose: useful for long distance cable runs

Email from Dave Sohn (4/11/12)

I thought this was coupled with an alternative for distribution.

We've proposed these units from SI Tech in the past. The 2856 is a TTL to F/O converter, the 9024 is a F/O distribution box.

Follow-up email from Jeremy Onyan (5/9/12) Thought I'd share some info on the SI Tech 2856 converter... I talked with them to get info for MS regarding the following:

Some answers for the questions you had:

- Jitter introduced by the conversion = ~3 ns
- TTL to optical conversation latency = between 55 ns – 60 ns; dependent upon signal strength, so if mounted in the same rack as the SAS device then 55 ns
- Variance across the ports = ~5 ns

- Latency across the cable = 5 ns / meter
- Optical cable uses a standard ST connector
- Re: single mode cable diameter, they said SM cable varies between 8.25 and 10 microns but uses the same standard sized ST connector
- They do not offer a dual power option...
- Our SAS uses 50 ohm coax which is compatible with the 2856 so no issues there.

In the datasheet diagram they show two cable connecting the converters – a T and an R connection. The T connection is the output port and the R is the input port. You only need to use two cables for passing the signal backwards... If you don't need to do this, they do offer a T and R version (2856 T to send the signal, 2856 R to receive the signal) which are a lower cost.

Regarding single v. multimode, although single mode is faster over long distances SI Tech says you won't see any appreciable difference over the distances for your use case. So you're likely better off going with multimode because of the cost difference.

Speaking of cost, I spoke with one of the engineers who did not have pricing info. If you can tell me which config(s) you are interested in. Then I'll price it out.

Use of Fiber converters with IRIG signals

- IRIG AM signals are not compatible with Fiber converters
- Must use IRIG DCLS signals when sending IRIG through fiber converters.
- The output line of the fiber converter needs to be terminated into 50 ohms (the opposite end of the cable) per Dave Sohn ("The fiber converter has a 50ohm driver on its output").

Shock testing of S.I. Tech products

2062-MM/SM-ST

- Refer to Salesforce Case 243287 (Aug 2020)

Reply from Mike Kass with S.I. Tech Hello Keith,

We do not have any data regarding shock testing of the 2062-MM-SM-ST. I can tell you that we have supplied thousands of units for military use with no failures related to shock and vibration. If you need samples to pursue your own shock testing, please let us know.

Mike Kass

Product Development Engineer



mkass@sitech-bitdriver.com

Various SI Tech products

Model 2062 - Optical Repeater Mini Bit-Driver®

- Up to 20 Mbps full duplex
- Designed to work with Arnet, Ethernet, & Token Ring fiber cabling
- Up to 2 Km of 50 or 62.5 micron fiber (10 dB budget)
- Powered by wall transformer 12 or 24 VDC supply (can # 2121)
- Multimode or single mode option
- Status indicators - TX and RX
- Can be used as fiber size converter e.g. 50 to 62.5 micron

8.1. Teem 2002 is designed to be used as a repeater on fiber optic networks. This repeater extends the distance of fiber optic Aloha. 8.2. Teem Ring, TTL or T1/E1 links up to 10 Km. This repeater can be configured to convert from multi-mode to single mode fiber. The 2002 can also be used to convert from one size of fiber to another: e.g. 50/125 to 62.5/125 micron.

UL Listed: Meets FCC requirements of Class A, Part 15 Computing Devices Standard.
Specifications subject to change without notice.

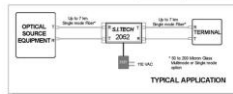
[View Complete Technical Data Sheet \(PDF\)](#)

References

ORDERING INFORMATION

Model Number	Description
2002-00-ST	1000 Micron Plastic Fiber to 50/92.5 Glass Fiber
2002-0-ST	Crimp 200 to 92.5 Micron - ST --
2002-ST	Multimode 50/92.5 to Multimode 50/92.5 Repeater - ST
2002-880-SH-ST	Multimode 50/92.5 to Single mode Converter - ST
2002-SH-SH-ST	Single mode to Single mode Repeater - ST

* Use with S.I. Tech 00402-0006-5006 Fiber Optic Cable Assembly



Contact Information: Phone: 630.761.3640 Fax: 630.761.3644 Email: sales@tech-connection.com
S.I. Tech, Bio-Drive®, and Fiber Cluster® are registered trademarks of S.I. Tech, Inc.
©2010 S.I. Tech, Inc. All copy and images.

****Issues with syncing nPulse cards**

- Point of Contact with nPulse tech support
 - Ashish Malik at nPulse. His email is am@npulsetech.com
- Refer to Salesforce cases such as 10697, 10607 and 10244
- Morgan Stanley and Allstrom both reported issues with this packet timestamping device
- Apparently, nPulse has issues with their 1PPS input disciplining which requires a patch be applied.

Email from Jason Heideloff with Allston (7/2/13)

Keith,

We will investigate the loss of GPS signals on our end. For the time being, I think you can hold off on any additional investigation regarding the PPS issue. I just received word from nPulse that they believe they found a bug in their PPS daemon and will be providing a patch tomorrow.

AFNOR NFS 87-500

AFNOR NFS 87-500 is a standardized French time code similar to IRIG-B but contains additional day, day-of-month and year information. AFNOR NFS 87 500 time code is widely used in Europe. The SecureSync specs do not list this protocol.

The IRIG 104-60 Standard was originally described in 104-60 in the year 1960 and subsequently updated to the latest version 200-04. I believe the SecureSync will comply with this requirement. We would need to define further exactly what particular IRIG message content the customer requires for example IRIG B-122.

General Time distribution (Master to one or more Slaves via IRIG, NTP, PTP)

PTP VS NTP VS IRIG

	PTP	NTP	IRIG
Peak time transfer error	>100 ns	>1 ms	10µs
Network type	LAN/WAN*	LAN/WAN	Dedicated coaxial cables
Spatial extent	A few subnets*	LAN/WAN	1 mile over coax
Style	Master/slave	Peer ensemble & Client/Server	Master/Slave
Protocols	UDP/IP – Multicast**	UDP/IP – Unicast (mainly)	
Cyber-Security	None as of yet	MD5 Auth	Closed loop, no network connectivity

* Hop Limit (TTL)

** Default Profile

ASCII, IRIG and STANAG/HAVEQUICK (for all products)

****Synchronous/Asynchronous:**

The data from Serial port is asynchronous (Meaning that it is not based on a specific clock frequency).

****DATA FORMATS/ NMEA 0183 (for all products)**

NMEA 0183 specs refer to [!\Engineering\Specs and Standards\NMEA \(National Marine Electronics Association\)](!:\Engineering\Specs and Standards\NMEA (National Marine Electronics Association))

SecureSync's two different modes of interrogation (immediate and on "on-time point")

With our newer SecureSync platform, there are now two ways to configure the interrogation mode. The Format can be configured to act like a NetClock where the data stream is not outputted until the next whole second (even if the request was received in the middle of a second). Or, it can be configured to output immediately, as soon as the request character is received. However, since Format 3 has no sub-second data received, the data stream will be exactly the same for the remainder of the second, until the next second has occurred (hitting the request character several times in the same sub-second would result in the same time stamp just being repeated).

ASCII Data Format accuracies

From Model 9383 data sheet: RS-232/RS-485: Time code ± 100 microseconds to ± 1 millisecond of UTC, format dependent

NMEA 0183 ASCII messages (such as GGA, RMC and ZDA)

- Refer to the following sites for a list of NMEA messages:
- http://ec-mobile.ru/user_files/File/ublox/ublox5_Protocol_Specifications.pdf
- <http://www.gpsinformation.org/dale/nmea.htm>

A) Data Format 90- “GPGGA” message (Fix information)

- Format GGA provides essential fix data which includes 3D location and accuracy data
- Refer to (in this same document): “Data Format 90 (NMEA 0183 “GPGGA”)”

Example message:

\$GPGGA,123519.00,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,,*47

Where:

GGA	=	Global Positioning System Fix Data
123519.00	=	Fix taken at 12:35:19 UTC
4807.038,N	=	Latitude 48 deg 07.038' N
01131.000,E	=	Longitude 11 deg 31.000' E
1	=	Fix quality: 0 = Invalid 1 = GPS fix (SPS) 2 = DGPS fix 3 = PPS fix 4 = Real Time Kinematic 6 = estimated (dead reckoning) (2.3 feature) 7 = Manual input mode 8 = Simulation mode
08	=	Number of satellites being tracked
0.9	=	Horizontal dilution of position
545.4,M	=	Altitude, Meters, above mean sea level
46.9,M	=	Height of geoid (mean sea level) above WGS84 ellipsoid
(empty field)	=	Time in seconds since last DGPS update
(empty field)	=	DGPS station ID number
*47	=	the checksum data, always begins with *

B) "RMC" message (Recommended minimum data for GPS)

Example message:

\$GPRMC,123519.00,A,4807.038,N,01131.000,E,022.4,084.4,230394,003.1,W*6A

GPRMC message

\$GPRMC,123519.00,A,4807.038,N,01131.000,E,022.4,084.4,230394,003.1,W*6A

Where:

RMC	=	Recommended Minimum Sentence
123519.00	=	Fix taken at 12:35:19 UTC
A	=	Status A=active or V=Void.
4807.038,N	=	Latitude 48 deg 07.038' N
01131.000,E	=	Longitude 11 deg 31.000' E
022.4	=	Speed over the ground in knots
084.4	=	Track angle in degrees True
230394	=	Date - 23rd of March 1994
003.1,W	=	Magnetic Variation
*6A	=	The checksum data, always begins with *

Q. Email from TOYO (forwarded from Dick Fox Oct 2011)

I received an email from Toyo our Japanese based distributor. One of their prospects has a couple of questions about Secure Sync that I can't answer 1 Is it possible to disable the 5 VDC on the GPS Antenna input port? Is there an external device you can put on the port to block the DC? According to Mitsubishi the NEMA format. "RMC" used in SS is old there is a newer format. See below. Do we have any plans to replace the current version with the newer version

A. Reply from Paul Myers:

The NMEA RMC message in NMEA 0183 revision 3.0x and greater (I assume) now has a field 12 now has a Positioning Systems Mode Indicator.

We added support for this in a branch a while ago and it was merged to the Trunk recently.

Upgrade them to 4.7.0 and they should have this field.

ONLY 2 of the possible enumerations outputs are supported.

A = AUTOMINOUS MODE –"Everything is OK"

N = DATA NOT VALID "Invalid Navigation Status"

Basically, if the navigation data is good it is 'A' when in Sync. If not, then it's 'N'

Q. Email from Masataka with TOYO (forwarded from Dick Fox Jan 2012)

When the ASCII time code is output from the SecureSync in the RMC format, the part indicating 'time' ("142329.00") has decimal fractions (".00") as shown below:

Message: \$GPRMC,142329.00,A,3523.422,N,13932.087,E,,,120112,,,A*56

However, some receivers may not be able to recognize the RMC format

because of the decimal fractions (".00").

In this connection, could you please answer the following questions, Is it possible to output the message excluding the decimal fractions from the time of the RMC format?

A My reply to him:

To answer your customer's question, the SecureSync's RMC serial data output formatting is not customer-configurable. It is hard-set to match the NMEA 0183 specifications for the RMC format, which contains the decimal point after the time and the two place-holders to the right of the decimal point.

If another vendor's system does not like the decimal point and two place-holders, the vendor of that system should refer to the NMEA 0183 specifications.

As for your request for a SecureSync software version that removes the decimal point and two place-holders, Richard Fox can provide you with the cost estimate of NRE fees for us to release a special version of software that provides this capability. If you and your customer are interested in the costs for this modification, let Richard know and then he can work with our Engineering team to provide you with a quote for this special release.

C) "GPZDA"/"ZDA" message (Date and Time)

- The Format ZDA Data message provides Date and Time information.

Example message:

`$GPZDA,HHMMSS.00,DD,MM,YYYY,XX,YY*CC`

Where:

HHMMSS.00	=	HrMinSec UTC)
DD,MM,YYYY	=	Day,Month,Year
XX	=	Local zone hours -13..13
YY	=	Local zone minutes 0..59
*CC	=	Checksum

The "ZDA" message provide whole second information only. It does not provide any sub-second information at all.

Per the NMEA specifications, the ZDA message format does not contain an on-time point, so there is no need to define to the time to the nearest hundredth of a second (without an available on-time point to reference, a hundredth of a second would not be a definable value). Because of this fact, the NMEA spec allows the message to include just the hours, minutes and whole seconds without any sub-second information reported. The SecureSyncs ZDA message will only provide the time of the current whole second with no decimal places reported after the decimal point. For this reason, the accuracy of the time data that is reported in the ZDA message is only accurate to the nearest second.

Examples: At time 12:10:58.01, the ZDA time will be reported as "58" seconds (not as either 58.01 or as 58.00)

Less than one second later, at time 12:10:58.99, the ZDA time will still be reported as "58" seconds (not as either 58.99 or as 58.00)

In summary, no sub-second time information is provided in the ZDA output data stream. Just whole seconds only.

Note: Software Version 4.4.S (and later production versions) adds tenths and hundredths place holders ".00" to the time stamps for compatibility with other systems.

Other requested (but not currently supported) NMEA Formats

A) ALM (Almanac data)

- Refer to Salesforce case **25056** (not available in at least v5.6.0 and below)

Per Dave Sohn (17 Apr 17) We likely would not in the near term. However, would they be interested in the assisted GNSS option? It provides almanac and ephemeris data for GPS and Galileo in RINEX-3 format available for download from the SecureSync.

- Refer to “**A-GPS** Rinex server option (“**SS-OPT-AGP**”) in SecureSync assist doc: [..\SecureSync-VersaSync CustAssist.pdf](#)

B) GSA (overall Satellite data)

- Refer to Salesforce case **25056** (not available in at least v5.6.0 and below)

Other Data Formats (besides NMEA messages)

Refer to: <I:\Customer Service\Data Formats>

Sync Status Character (info below is referring to document linked above)

Attached is a great earlier document regarding Spectracom formats, such as Format 2. Each of the three ASCII characters (space, question mark or asterisk) which reports the Sync state are listed on the right side of the first page of this document (and excerpted below for your reference):

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

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

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

Data Format 0 (Data Format 00):

271 12:45:36 DTZ=08

11 12:45:36 DTZ=08

FORMAT 0

Includes a time sync status character, day of year, time

CR LF I ^^ DDD ^ HH:MM:SS ^ DTZ=XX CR LF

Example: 271 12:45:36 DTZ=08

The example provides the following information:

Sync Status: Time synchronized to reference

Date: Day 271

Time: 12:45:36 Pacific Daylight Time

D = DST, Time Zone 08 = Pacific Time

Data Format 1 (Data Format 01):

THU 19DEC02 12:45:36

FORMAT 1

Provides the fully decoded time data stream. Format 1 provides a fully decoded date consisting of day of week, month, and day of the month. Format 1 also contains a time sync status character, year, and time reflecting time zone offset and DST correction when enabled. Format 1 data structure is:

CR LF I ^ WWW ^ DDMMYY ^ HH:MM:SS CR LF

Example: * THU 19DEC02 12:45:36

The example provides the following information:

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

Date: Thursday, December 19, 2002

Time: 12:45:36

Data Format 1S: (modified day of month)

- As I recall, converts one digit day of month (such as days “1” thru “9”) to two digit day “(such as days “01” thru “09”), but may be just the opposite.

THR 22AUG19 18:00:10

Data Format 2 (Data Format 02):

- Refer also to: <I:\Customer Service\Data Formats>

Example string: ?A02 271 12:45:36.123 S

FORMAT 2

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

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

Example: ?A02 271 12:45:36.123 S

The example provides the following information:

Sync Status: The clock has lost time sync. The inaccuracy code of “A” indicates the expected time error is <10 milliseconds.

Date: Day 271 Time: 12:45:36 UTC time, standard time.

Sync Status Character (info below is referring to document linked above)

Attached is a great earlier document regarding Spectracom formats, such as Format 2. Each of the three ASCII characters (space, question mark or asterisk) which reports the Sync state are listed on the right side of the first page of this document (and excerpted below for your reference):

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

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

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

TYPICAL NETCLOCK/GPS TABLE

Inaccuracy Code	Time Error (mSec)	Time Since Unlock (Hours)
Space	<1	Locked
A	<10	<10
B	<100	<10
C	<500	<10
D	>500	>500

• •

CHARACTER DESCRIPTOR:

- CR** = Carriage Return
- LF** = Line Feed
- I** = Time Sync Status (space, ?, *)
- ^** = space separator
- Q** = Quality Indicator (space, A, B, C, D)
- YY** = Year without century (02, 03, 04 etc.)
- DDD** = Day of Year (001-366)
- HH** = Hours (00-23)
- :** = Colon separator
- MM** = Minutes (00-59)
- SS** = Seconds (00-60)
- .** = Decimal Separator
- sss** = Milliseconds (000-999)
- L** = Leap Second Indicator (space, L)
- D** = Daylight Savings Time indicator (S,I,D,O)
- TZ** = Time Zone
- XX** = Time Zone offset (00-23)
- WWW** = Day of Week (MON, TUE, WED)
- DD** = Numerical Day of Month (^1-31)
- MMM** = Month (JAN, FEB, MAR)

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

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

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

The Daylight Saving Time indicator D is defined as:

- S** = During periods of standard time for the selected DST schedule.
- I** = During the 24-hour period preceding the change into DST
- D** = During periods of Daylight Saving Time for the selected DST schedule
- O** = During the 24-hour period preceding the change out of DST

The quality indicator Q provides an inaccuracy estimate of the output data stream. When the receiver is unable to track the reference, a timer is started. The table below lists the quality indicators and the corresponding error estimates based upon the internal oscillator stability and the time elapsed tracking no satellites. The timer and the quality indicator reset when the receiver requires its reference.

Data Format 3 (Data Format 03):

FORMAT 3

Provides a format identifier, time sync status character, year month day, time with time zone and DST corrections, time difference from UTC, standard time/DST indicator, leap second indicator and on-time marker. Format 3 data structure is:

FFFF^YYYYmmdd^HHMMSS±HHMM L # CR LF

CHARACTER DESCRIPTOR:

FFFF = Format Identifier (0003)
I = Time Sync Status (Space, ? *)
^ = space separator
YYYY = Year (2002, 2003, 2004 etc.)
mm = Month Number (01-12)
dd = Day of the Month (01-31)
HH = Hours (00-23)
MM = Minutes (00-59)
SS = Seconds (00-60)
± = Positive or Negative UTC offset (+,-) Time Difference from UTC
HHMM = UTC Time Difference Hours, Minutes (00:00-23:00)
D = Daylight Saving Time Indicator (S,I,D,O)
L = Leap Second Indicator (space, I)
= On time point
CR = Carriage Return
LF = Line Feed

The time difference from UTC, ±HHMM, is selected when the serial comm or remote port is configured. A time difference of -0500 represents eastern time. UTC is represented by +0000.

Example: 0003 20021219 124536-0500S #

The example provides the following information:

Data Format: 3

Sync Status: Time Synchronized to GPS

Date: December 19, 2002

Time: 12:45:36 EST, The time difference is 5 hours behind

UTC Leap

Second: No leap second is scheduled for this month.

Example: 0003 20021219 124536-0500S #

Email sent to Steve Widmer 4/28/11

Format 3 is one of the few available time stamps where the on-time point is not at or near the start of the data stream. Most formats have the on-time point at the beginning of the message. The on-time point for Format 3 is near the end of the data stream (it is the 29th character in the data stream), as indicated by the "#" character in the data stream. Example format below:

FFFF^YYYYmmdd^HHMMSS±HHMM L # CR LF

The time at the on-time point is the actual time that was reported just before the on-time point of the message is outputted.

As Data Format 3 does not contain any sub-second information, the on-time point indicates a whole-second value, each time its

outputted. Format 3 can be, but doesn't have to be, broadcasted each second from a NetClock or SecureSync. It can be used in an interrogation mode, where the time is not outputted, unless its requested by a request character (such as a capital letter T). With the NetClocks (such as the Model 9383 for example, since there is no sub-second data provided in Format 3, if the capital letter T is received sub-second, the NetClock will hold off outputting the data stream until the on-time point mates with a whole-second value (it won't send out this format in between two whole seconds). So, with a NetClock whether the format is broadcasted automatically every second or if its requested with request character, the on-time point (and its time message) will always be for the whole second value only.

With our newer SecureSync platform, there are now two ways to configure the interrogation mode. The Format can be configured to act like a NetClock where the data stream is not outputted until the next while second (even if the request was received in the middle of a second). Or, it can be configured to output immediately, as soon as the request character is received. However, since Format 3 has no sub-second data received, the data stream will be exactly the same for the be the remainder of the second, until the next second has occurred (hitting the request character several times in the same sub-second would result in the same time stamp just being repeated).

Data Format 4 (Data Format 04):

FORMAT 4

Provides a format indicator, time sync status character, modified Julian date, time reflecting UTC with 0.1 millisecond resolution and a leap second indicator. Serial Comm ports configured for interrogation mode output this data stream immediately upon receiving the time request character. The data stream is output every second for the Remote Outputs or Serial Comm port configured for continuous output. Format 4 data structure is:

FFFFIMJDXX^HHMMSS.SSSS^L CR LF

CHARACTER DESCRIPTOR:

FFFF = Format Identifier (0004)
I = Time Sync Status (Space, ? *)
IMJDXX = Modified Julian Date
HH = Hours (00-23 UTC time)
MM = Minutes (00-59)
SS.SSSS = Seconds (00.0000-60.0000)
L = Leap Second Indicator (^, I)
CR = Carriage Return
LF = Line Feed

The leading edge of the first character's start bit marks the on-time point of the data stream.

Example: 0004 52627 124536.1942 L

The example provides the following information:

Data Format: 4

Sync Status: Time synchronized to GPS.

Modified Julian Date: 52627

Time: 12:45:36.1942 UTC

Leap Second: A leap second is scheduled at the end of the month.

Example: 0004 52627 124536.1942 L

Data Format 9 (Data Format 09) and Data Format 9S (SecureSyncs 5.4.5 and above)

- Provides Day of Year and time information.

Data Format 9 and Data Format 9S

THR 22AUG19 18:00:10
234:18:02:13
234:18:02:14
234:18:02:15
234:18:02:16
234:18:02:17
234:18:02:18
234:18:02:19

I. Format 9: Used for Sysplex Timer

II. Format 9S: Modified Format 9 to include sync status indicator for Sysplex timer

- Ability to select Data Format 9S was added in software Version 5.4.5.

Format 9

<SOH>DDD:HH:MM:SSQ<CR><LF>

Where:	=	Start of header (ASCII Character 1) (Note: this is not the sync status indicator (refer to "Q" below for sync status))
SOH	=	
DDD	=	Day of Year (001-366)
:	=	Colon Separator
HH	=	Hours (00-23)
MM	=	Minutes (00-59)
SS	=	Seconds (00-59), (00-60 for leap second)
Q	=	Time Quality Status character (see characters below)
CR	=	Carriage Return (ASCII Character 13)
LF	=	Line Feed (ASCII Character 10)

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

Quality Indicators

Note:

- All 9300s (Ricky- Option 11 for FAA) and VERY early versions (like version 4.1.0) of SecureSync software only supported either a "space" or "?".
- Newer SecureSync software versions software supports all the possible characters.
- For SecureSync: Quality flag Number is based on the current TFOM value (in bold below).

From: <http://www.manualslib.com/manual/167770/Symmetricon-XI-Gps.html?page=56>

The time quality character, "Q", is one of the following characters:

- **SPACE** = Time error is less than time quality flag 1's threshold (**TFOM < or = 3**)
- **"."** = Time error has exceeded time quality flag 1's threshold (**TFOM = 4**)
- **"*"** = Time error has exceeded time quality flag 2's threshold(**TFOM = 5**)
- **"#"** = Time error has exceeded time quality flag 3's threshold (**TFOM = 6**)
- **"?"** = Time error has exceeded time quality flag 4's threshold OR A reference source is unavailable (**TFOM >=7**)

Email and code snippet from Paul Myers (5 Nov 2013)

The SecureSync followed the specification given to us to be a drop in replacement.

The creation of message Format 9 is derived from the TFOM which maps to the Quality Flag.

We mimic the TrueTime XL-DC

From libspecfmt.h

```
#define FL_QUAL_LT1      ('.') // Error >= 1 us (thr 1) (FAA)
#define FL_QUAL_LT2      ('*') // Error >= 10 us (thr 2) (FAA)
#define FL_QUAL_LT3      ('#') // Error >= 100 us (thr 3) (FAA)
#define FL_QUAL_LT4      ('?') // Error >= 1 ms (thr 4) (FAA)
```

From libspecfmt.c

```
////////////////////////////////////
// Function:  FL_TfomToSpecFmt9
// Description: The FL_TfomToSpecFmt9 function converts a TFOM value to the
//              quality character for a Spectracom format 9 message. The
//              quality characters are related to the TrueTime XL-DC
//              implementation of the 3-208 SERIAL FUNCTION F08. These
//              quality characters are used by a NTP Type 25 generic receivers
//              reference clock driver.
//
//              The reference clock driver used for GPS-TM/TMD Receivers
//              (default quality codes for XL-DC) maps the quality codes
//              to the accuracies listed below.
//              '.' < 1 microsecond (space)
//              '.' +/- 1 microsecond
//              '*' +/- 10 microseconds
//              '#' +/- 100 microseconds
//              '?' +/- 1 milliseconds
//
//              Note our quality thresholds err on the side of more
//              accuracy.
//
////////////////////////////////////
static char FL_TfomToSpecFmt9(TFOM tfom)
{
    if (tfom == TFOM_MIN) { return (FL_QUAL_LT4); }
    else if (tfom <= TFOM_3) { return (FL_QUAL_LOCK); }
    else if (tfom == TFOM_4) { return (FL_QUAL_LT1); }
    else if (tfom == TFOM_5) { return (FL_QUAL_LT2); }
    else if (tfom == TFOM_6) { return (FL_QUAL_LT3); }

    // Default to this value if TFOM is >= TFOM_7
    return (FL_QUAL_LT4);
} // End FL_TfomToSpecFmt9
```

Data Format 9S:

Data Format 90 (NMEA 0183 “GPGGA”)

FORMAT 90

Provides a position data stream in NMEA 0183 GPGGA GPS Fix data format. The Format 90 data structure is shown below:

\$GPGGA,HHMMSS.SS,ddmm.mmmm,n,dddmm.mmmm,c,Q,SS,YY.y,AAAAA.a,M,,,,*CC CR LF

CHARACTER DESCRIPTOR:

\$GP = GPS System Talker
GGA = GPS Fix Data Message
HHMMSS.SS = Latest time of Position Fix, UTC. This field is blank until a 3D fix is acquired
ddmm.mmmm,n = Latitude
 dd = degrees, 00...90 mm.mmmm = minutes, 00.0000....59.9999
 n = direction, N = North, S = South
dddmm.mmmm,e = Longitude
 ddd = degrees, 000...180
 mm.mmmm = minutes, 00.0000....59.9999
 e = direction, E = East, W = West
Q = Quality Indicator;
 0 = No 3D fix
 1 = 3D fix SS = Number of satellites tracked, 0...8
YY.Y = Dilution of precision, 00.0...99.9
+AAAAA.a,M = Antenna height in meters, referenced to mean sea level
 ---- = Fields for geoidal separation and differential GPS not supported
 cc = Check sum message, HEX 00...7F Check sum calculated by Xoring all bytes between \$ and *.
CR = Carriage Return
LF = Line Feed

Example: **\$GPGAA,151119.00,4307.0241,N,07729.2249,W,1,06,03.2,+00125.5,M,,,*,3F**

The example data stream provides the following information:

Time of Position Fix: 15:11:19.00 UTC
Latitude: 43° 07.0241' North
Longitude: 77° 29.2249' West
Quality: 3D fix
Satellites Used: 6
Dilution of Precision: 3.2
Antenna Height: +125.5 meters above sea level
Check Sum: 3F

Where:

GGA	=	Global Positioning System Fix Data
123519.00	=	Fix taken at 12:35:19 UTC
4807.038,N	=	Latitude 48 deg 07.038' N
01131.000,E	=	Longitude 11 deg 31.000' E
1	=	Fix quality: 0 = Invalid 1 = GPS fix (SPS) 2 = DGPS fix 3 = PPS fix 4 = Real Time Kinematic 6 = estimated (dead reckoning) (2.3 feature) 7 = Manual input mode 8 = Simulation mode
08	=	Number of satellites being tracked
0.9	=	Horizontal dilution of position
545.4,M	=	Altitude, Meters, above mean sea level
46.9,M	=	Height of geoid (mean sea level) above WGS84 ellipsoid
(empty field)	=	Time in seconds since last DGPS update
(empty field)	=	DGPS station ID number
*47	=	the checksum data, always begins with *

Email sent to ArgonST on 6/24/09: Per the NMEA specifications, the UTC time reported in NMEA 0183 (Format 90) is not the current UTC time. It is the time that the GPS receiver last calculated its 3-D fix. For the receiver to have a 3-D fix, the receiver has to continuously track at least four satellites at all times (This is greater than the normal minimum of just one satellite while in Position Hold mode). While tracking at least four satellites, the 3D fix is able to be calculated every second. However, the receiver is not able to calculate the 3-D fix and report the time in its output data stream in the same second. It reports the calculated time of that fix in its next output data stream. Therefore, the reported lags the current time by one second. So, your finding of the one second error is true. There is a one second lag on this time stamp. This is the reason that the time is reported as "time since last 3-D Fix" and not as the "current UTC time". In order to use Format 90 as a time stamp of the current time, you have to account in your system for this one second lag.

Another factor of using NMEA 0183 is even more crucial to account for when using it for synchronization. Because the time that is reported in NMEA 0183 is the "time of last 3D fix" and not the "current UTC time", if the GPS receiver drops below tracking 4 satellites for any length of time- even one second, the time in the data stream will stop incrementing altogether. The time in the Format 90 data stream will still be present and will remain the same every second until the GPS receiver starts to track at least four satellites again. At that time, the reported time will just jump to the time that it started tracking 4 satellites again. To demonstrate this operation, just temporarily disconnect the GPS antenna and observe the reported time stamps, keeping in mind that the reported time in all of outputs thereafter (until the antenna is reconnected) are showing the last time that it WAS tracking four satellites- not what the current time should be at that particular moment.

Accounting for the one second lag in the reported UTC time of Format 90 is likely fairly easy to handle in the receiving equipment.

However, the time stamps being reported consecutively as the same value upon any loss of GPS reception is the reason that most vendors decide not to use this data stream for synchronization. If your system can detect that the time stamps have stopped incrementing and can start to ignore them until they start to increment again, you'll be able to use this Format for synchronization. However, if your system is unable to handle the same time being reported every second, I don't recommend using this data stream for your external synchronization.

(Email from Keith to Sylvain on 8/31/10)

Unfortunately, there is a significant limitation with the use of the GPGL format 90 data stream as an input to the Spectracom NTP servers, as I previously mentioned. This ASCII Data does not provide current time- it only provides the time since the last fix. This is a limitation of the format itself and not a limitation of the Spectracom products. Because it's a Format issue, the Model 9300s outputs are affected in the same way as the SecureSync product's input. Also, keep in mind that the only product line that can accept Data Format 90 as an input is the SecureSync products. The Model 9300 series cannot sync to Data Format 90 (The Model 9388 is the only one in the Model 9300 series that can accept an ASCII time-code input and it can only sync to Formats 0 and 2. It does not accept Format 90 as an input).

In summary, SecureSync with the ASCII time code module is the only configuration to allow Format 90 as an input. In this configuration, the output time of the SecureSync will be one second off. Both the Model 9300s and SecureSync outputs have this limitation with Data Format 90. This time offset has to be accounted for in the customer's system. If they can't handle this one second offset, I recommend your customer uses a different type of input to SecureSync, such as GPS or IRIG input instead of GPGL input.

Format 90 Checksum- All Model 918x series as well as all 928x/938x prior to v3.4.2 have the wrong checksum value being calculated and displayed at the end of each data stream. The calculator can be found at: <http://www.hhhh.org/wiml/proj/nmeaxor.html>. Just paste any Format 90 output data stream, beginning (AFTER the "\$" and BEFORE the "***") into the Command window and it should match the displayed calculated value shown at the end of the data stream.

For the NMEA message specs, refer to [I:\Engineering\Specs and Standards\NMEA \(National Marine Electronics Association\)](#)

Horizontal Dilution of Position (HDOP) field becomes a null (no value) upon completion of GPS survey (Trimble Res-SMT-GG receiver only, in Standard/Stationary mode)

- Refer to Salesforce cases **206133** and **164286**
- By design (this is not a software/firmware bug) Trimble receivers populate the HDOP field with a null, once the GPS survey has completed and the receiver goes into overdetermined clock mode.

Per Ron Dries (28 Oct 2019) The customer is using the NMEA GGA message output from the ASCII card. With a Trimble GG receiver once the survey completes and the receiver is in over-determined clock mode the DOP value in the NMEA string becomes blank. With a u-blox receiver it is set to a constant value

- ublox receivers, instead populate this field with a constant value, which doesn't ever change.

Available work-around (if the null value after GPS survey is an issue for other devices receiving the data stream)

- Configure the Trimble receiver for Mobile mode (instead of Standard mode)

Per Dave Sohn (29 Oct 2019) If they put the receiver in Mobile mode (even though application is stationary) the DOP fields will remain populated as the system doesn't complete a survey and go into overdetermined clock mode.

Relating to Salesforce case 164286

(per Dave L 11 Sept 2018) We have done some testing and were able to duplicate the issue. This is isolated to SecureSync products equipped with the Trimble Resolution-GG receivers. The U-Blox receivers are not affected.

When the Survey has completed (about 31 minutes after start) the receiver will change states and the HDOP information will not be reported to the GPGL sentence.

We were able to switch the receiver mode to MOBILE mode and restore the missing HDOP data in the GPGGA message.

SecureSync/948x Software issues/changes associated with GPGGA

v5.8.5 added the geoid height to the NMEA GGA output message

- *Per the Version 5.8.5 (July 2019) release notes:* “Added the geoid height to the NMEA GGA output message”

V5.8.3: “Fix Quality” field of the GPGGA output with SAASM receiver installed doesn’t switch to “PPS” (applicable to versions 5.8.2 and below)

- v5.8.2 and below- “PPS” was not reported when receiver is keyed. Remains “SPS” (which is the correct value for not keyed)
- Applicable to at versions 5.8.2 and below (fixed in 5.8.3)
- Refer to Salesforce case 163026/JIRA-SSS-463

Customer report ...The GGA statement that is being outputted by the SecureSync, and in Field 6 (GPS Quality Indicator) in that statement are my concern here.

When I have no SAASM keys and the unit it fully synced it will display.

Example: \$GPGGA,172814.0,3723.46587704,N,12202.26957864,W,1,9,0.9,203.893,M,,,*4F

Field 6 (highlighted) will show that it is operating with GPS fix with Standard Positioning service (SPS), this is expected output from the unit with no SAASM keys installed. Even in the SAASM Receiver Addendum 1200-500-0053 Rev.E it says the GPS info on LCD display will even show this. So this NMEA output matches the info I can see in the unit.

When I have SAASM keys installed the unit should be in Precise Positioning Service (PPS), even the GPS info on LCD display will show this (per the Addendum). The NMEA GGA statement with SAASM keys seems to match the statement with no SASSM keys, even though the unit is in PPS fix.

My point is I believe we should expect a value of 3 in field 6 of the GGA message when SAASM keys are being used and the unit is in PPS fix. I am unsure if this is due to configuration and I have not enabled the change to happen either to the base unit or for the option card that is handling the output. If the 5.6 version we are running won't do this, but a different version can.

Status Change (29 Jan 2019) per the Version 5.8.3 release notes

“GGA Fix Quality field is now based on overall sync state—not solely on GPS sync”

EndRun data formats

These are formats right from the Endrun (competitor) products

Made available starting in version 4.6.0 of SecureSync software.

T YYYY DDD HH:MM:SS zZZ m<CR><LF> Example: 9201121001:22:13+00U

Where:

T is the Time Figure Of Merit (TFOM) character and is one of:

9 indicates error > +/- 10 milliseconds, **or unsynchronized condition**

8 indicates error < +/- 10 milliseconds

7 indicates error < +/- 1 millisecond

6 indicates error < +/- 100 microseconds

YYYY is the year,

DDD is the day of the year,

HH is the hour of the day,

MM is the minute of the hour,

SS is the second of the minute,

z is the sign of the offset to UTC, + implies time is ahead of UTC

ZZ is the magnitude of the offset to UTC in units of half-hours. Non-zero only when Time Mode is Local.

M is the Time Mode character and is one of:

G = GPS,

L = Local,

U = UTC

<CR> is Carriage Return control character (0x0D)

<LF> is Line Feed control character (0x0A)

*****China Mobile Format**

Per Paul Myers (20 Nov 14) As of at least NetClock 9300 series software 3.6.7 and SecureSync/9400 software version 5.1.7) this format is not currently supported. But could be made available inputs/outputs as they are very similar to already supported formats.

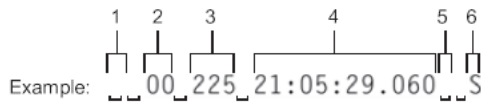
"This Format is NOT supported, but could be implemented using data normally used for GGA and other formats"

*****Cisco TOD**

Per Paul Myers (20 Nov 14- As of at least NetClock 9300 series software 3.6.7 and SecureSync/9400 software version 5.1.7) this format is not currently supported. But could be made available inputs/outputs as they are very similar to already supported formats.

This format is ALMOST Format 2 and could be easily implemented.

Below is an excerpt from Chapter 6 of the Symmettricon TimeSource 3500 User's guide



- 1 Alarm field: blank space = receiver has satellite availability; ? = no satellite available
- 2 Year (2000 in this example)
- 3 Day of year (the 225th day of the year in this example)
- 4 Hours:minutes:seconds:milliseconds
- 5 Leap second: blank space = no leap second; L = upcoming leap second
- 6 Daylight savings time indicator: S = standard time; D = daylight savings time

Figure 6-1. NTP Type 4 Data Format

Cisco Systems

Connector Type:	RJ-45
Connector Label:	TOD
Connector Location:	Rear panel
Electrical Interface:	RS-485
Baud Rate:	9600 b/s
Bit Configuration:	8 data bits, No parity, 1 stop bit
Data Format:	See Figure 6-2



- 1 Satellite availability: * = valid, ! = not valid
- 2 Revision
- 3 Modified Julian date (number of days past midnight, Nov 17, 1858)
- 4 Year/month/day
- 5 Hours:minutes:seconds
- 6 Indicator of time zone offset (+, -, or 0)
- 7 Time zone offset
- 8 Leap second indicator
- 9 Latitude
- 10 Longitude
- 11 Altitude above mean sea level in meters
- 12 Alarm severity: EV = event, MN = minor, MJ = major, CL = critical
- 13 Alarm source
- 14 Alarm cause: holdover, BT3 warm-up, or hardware fault

Figure 6-2. Cisco Systems Data Format

**NAV-TIMEGPS with UBX format

Email from Keith to Richard Fox (2 Jan 2013 - Refer to Salesforce case 7053) From page 170 of the following link, this Serial format appears to be a specific output from a Ublox GPS receiver (which we don't currently support): <http://dlmh9ip6v2uc.cloudfront.net/datasheets/Sensors/GPS/760.pdf>.

I don't believe any of the currently available Data Formats emulate this data stream. The closest "match" we currently have available is the BBC-02 format, but it does not appear to be the same. So it's not going to meet their request.

RS-232 data

Distance from Serial port to equipment is greater than 50 feet

Standard RS-232 cable can run up to 50 feet. If need exists to exceed 50 feet, contact Black Box to order RS-232 "quiet cable" (low capacitance/shielded cable). They spec up to 500 feet with this cable. We don't recommend it and can't be responsible for ground elevation/data corruption from using this cable. However, I have heard of customer running 300 feet with no problems.

Resolution: (email from Sam Otto)

The Maximum Distance recommended by the RS-232 Standard is directly related to the Data rate you're communicating at and the type of cable that you're using. For the most part the higher the data the shorter the maximum cable length.

For a standard shielded cable the Data Rate and corresponding Maximum cable lengths are as follows:

- 2400 bps – 60m – 200ft
- 4800 bps – 30m – 100ft
- 9600 bps – 15m – 50ft
- 19200 bps – 7.6m – 25ft
- 38400 bps – 3.7m – 12ft
- 56000 bps – 2.6m – 8ft
- 115200 bps – 1.3m – 4ft

Of course it is possible to exceed these distances with different cable types but this is a pretty standard rule of thumb.

RS-485 Cable Length limitations

Unshielded – 457.2m – 1500ft
shielded – 1219.2m – 4000ft

Daisy chain up to 32 (Might be flexible depending on third party converters)

When using the default RS485 receivers with an input resistance of **12 k Ω** it is possible to connect **32** devices to the network.

Currently available high-resistance RS485 inputs allow this number to be expanded to **256**.

ASCII Data Format accuracies

From Model 9383 data sheet: RS-232/RS-485: Time code ± 100 microseconds to ± 1 millisecond of UTC, format dependent

RS-232 DISTRIBUTION OVER T1 LINE

- No distance limitation
- Need one dedicated channel on the 24 channel voice MUX.
- Can convert RS-232 to RS-485 once-per-second with a BlackBox converter.
- Can't do IRIG
- Can do interrogation but will need two dedicated channels.
- Signal gets digitized by a modem.

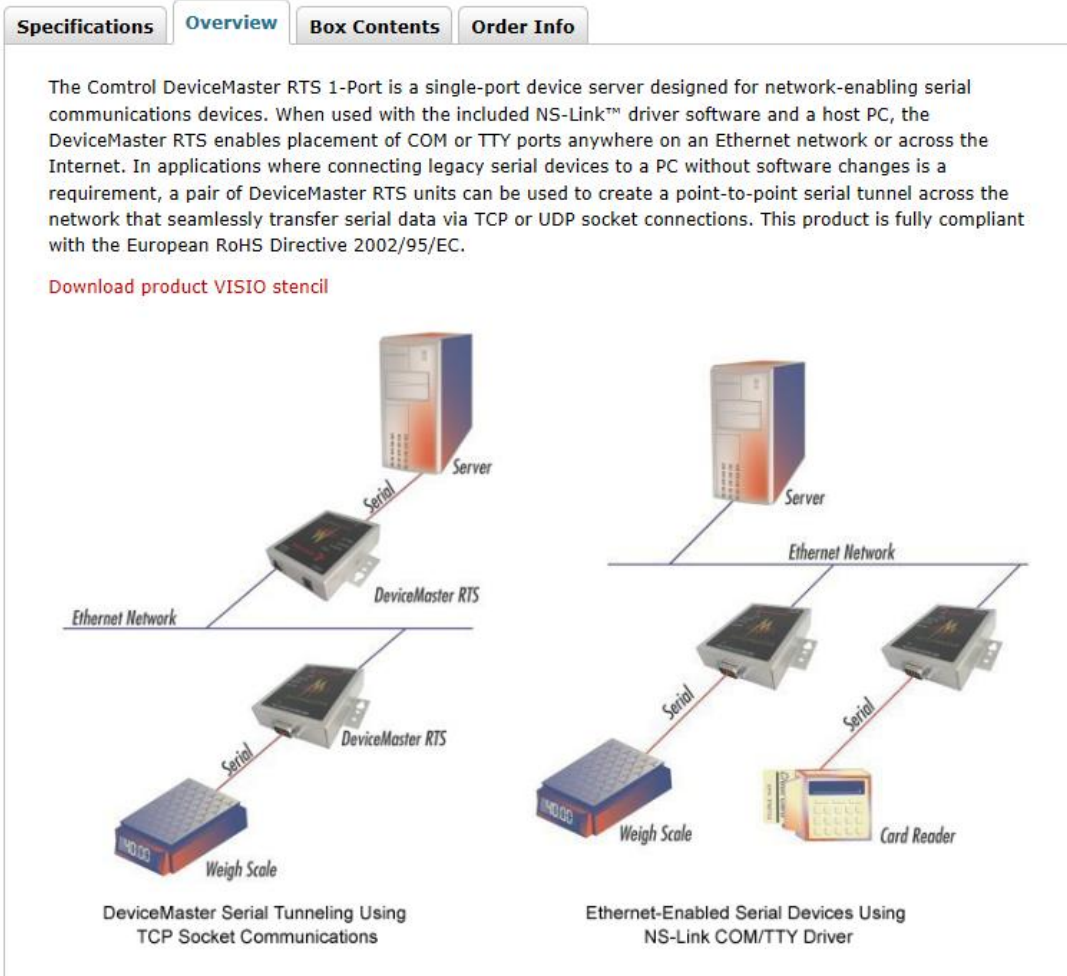
****Short Haul Modem:** Used to convert RS-232 to RS-485 to allow run of 4000 feet using shielded twisted pair. Requires one at each end. Can't be used in conjunction with any other signal (ie RS-485 once-per-second).

**** RS-485/RS-232 distribution over Ethernet connection (RJ-45)**

Email from Richard Fox (5 Apr 2013) This looks to me like the way to build a scalable RS-232 and RS-485 distribution network. You put one of these devices on the RS-485 or RS 232 interface and send the data over the Ethernet. At each PLC you put another device that converts Ethernet to serial. Bingo RS—232 and RS-485 unlimited distances.

There are several companies that make them:

<http://www.comtrol.com/pub/products/product/pid/167>
<http://www.perle.com/products/Device-Server.shtml>



Per Dave Sohn (7 Oct 2013) The serial over RJ-45 pinout can depend on the equipment he is interfacing to. Check link below looking at columns under 8P8C ("RJ45"). http://en.wikipedia.org/wiki/Serial_port#Pinouts

****IRIG for all products**

- Refer also to [I:\Customer Service\IRIG](#)

******IRIG Distribution amps from Spectracom**

A) Single IRIG input (no redundant IRIG input) / IRIG outputs

- **SecureSync (with at least one IRIG Input/Output Option Card installed)**

Slightly modified Email from Dave Sohn (19 Mar 2013) The SecureSync can accept at least one IRIG input. It can then generate additional IRIG, 1PPS, and 10MHz based on that synchronization. How many signals of which type do they need to generate?

- [Model 7535 \(7535-001\) IRIG distribution amplifier](#) (1) IRIG input
- [Rapco Model 1876](#) (1) IRIG input, (10) or (14) IRIG outputs (not listed on our website)
- [Rapco Model 1896](#) (1) IRIG input, (10) or (14) IRIG outputs (not listed on our website)

B) Dual IRIG inputs (for redundant IRIG input) / IRIG outputs

- **SecureSync (with more than one IRIG input Option card installed and at least one IRIG output installed)**

Slightly modified Email from Dave Sohn (19 Mar 2013) Also, the SecureSync can do automatic failover. It may not be suitable for all situations, but the SecureSync can take in two separate IRIG inputs, selecting between them for synchronization. It can then generate additional IRIG, 1PPS, and 10MHz based on that synchronization. How many signals of which type do they need to generate?

- [RAPCO Model 1866E \(IRIG distribution switch\)](#) : (2) IRIG inputs, (14) IRIG outputs
- [Epsilon SAS-17E-IR \(Option 10\)](#) (2) IRIG inputs, (1) IRIG output

Notes:

- E) SAS-17E-IR is not a standard product configuration. Availability needs to be verified with Spectracom France before quoting it.
- F) Also note that with only one IRIG output (but two IRIG inputs), this is not really so much a distribution amp as much as it is just a switch between two IRIG generators.
 - [Model 8143](#) (Requires special modifications) (2) IRIG Inputs, (12) IRIG outputs

Fiber converters for long distance IRIG runs

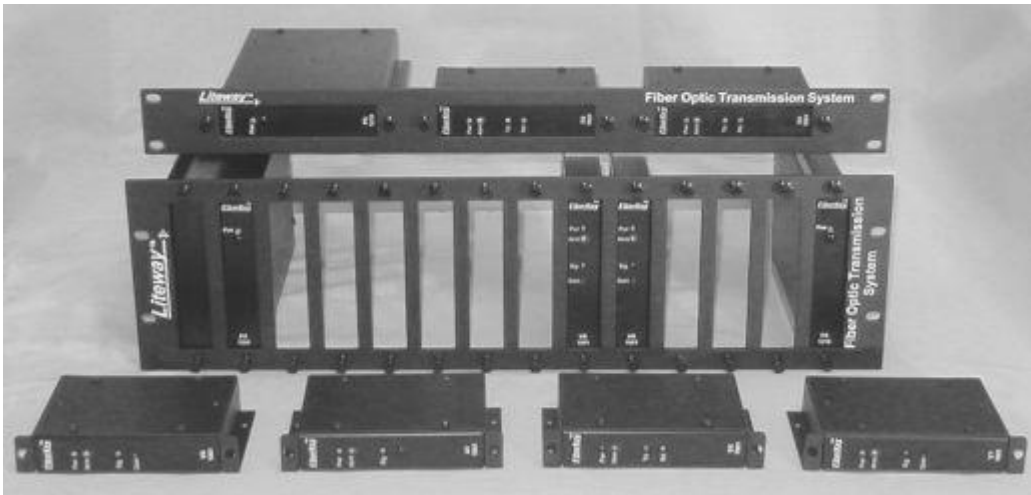
Use of Fiber converters with IRIG signals

- **IRIG AM signals** are **not** compatible with Fiber converters
- Must use IRIG DCLS signals when sending IRIG through fiber converters.

A) SI Tech Fiber Optic converters for IRIG

- We have resold these as a Special in a couple of cases
- Refer to: [..\EQUIPMENT\SPECTRACOM EQUIPMENT\SI Tech \(fiber converters\)](..\EQUIPMENT\SPECTRACOM EQUIPMENT\SI Tech (fiber converters))
- For data sheets and all other info on these SI Tech products info on these products, refer also to (in this document): [:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SI Tech \(fiber converters\)](:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SI Tech (fiber converters)) for data sheets on these SI Tech products

B) Luxlink IRIG Fiber Optic transmitters and receivers for IRIG



- These appear to be devices we have resold
- Refer to “Arena” for additional info

LuxLink® Fiber Optic Transmission Systems

(516) 931-2800

www.LuxLink.com

166 Haverford Road

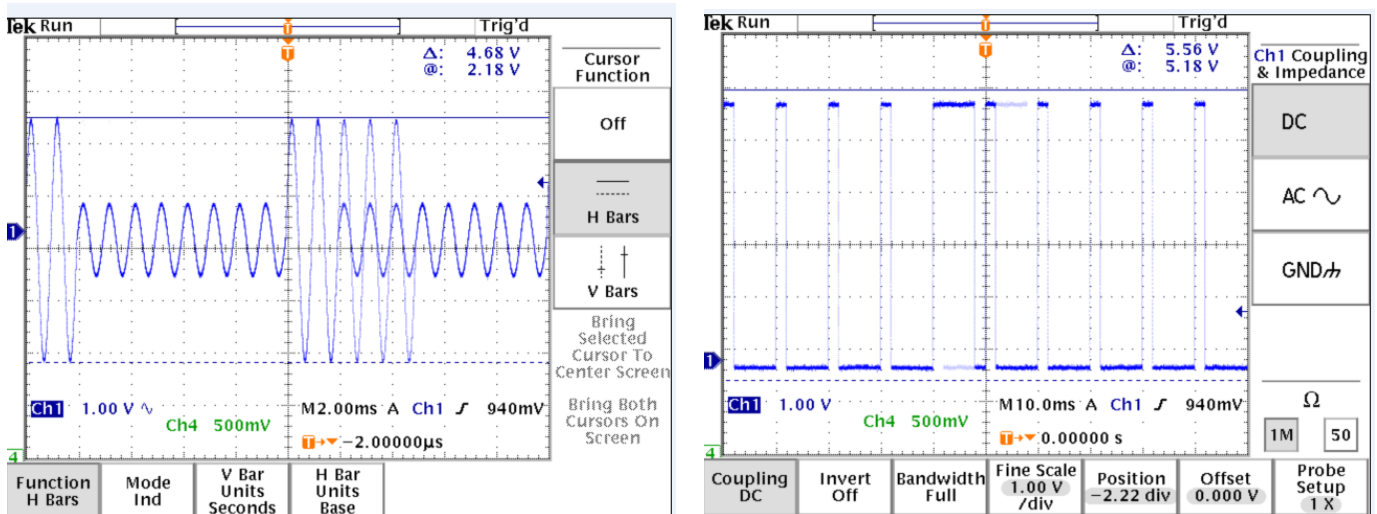
Hicksville, NY 11801

Associated parts

Spectracom P/N	Luxlink P/N	Description	(link to Arena)	picture
MP29-0000-0009	INST-1001	Transmitter, Analog Data 20 Hz to 10 MHz, 3 Volt pp	https://app.bom.com/items/detail-spec?item_id=1214274278&version_id=10401123338	
MP29-0000-0010	INSR-1001	Receiver, Analog Data 20 Hz to 10 MHz, 3 Volt pp	https://app.bom.com/items/detail-spec?item_id=1214274283&version_id=10401123408	
MP29-0000-0011	IRGT-1001	Fiber Transmitter, Analog (Modulated) IRIG Time Code Transmission	https://app.bom.com/items/detail-spec?item_id=1214274287&version_id=10401123478	
MP29-0000-0012	IRGT-7001	IRIG Fiber Transmitter, DC Time Code (IRIG DCLS, Unmodulated Digital) Transmission	https://app.bom.com/items/detail-spec?item_id=1214274292&version_id=10401123538	
MP29-0000-0013	ALM-1000	Alarm module	https://app.bom.com/items/detail-spec?item_id=1214274300&version_id=10401123638	
MP29-0000-0014	IRGR-1001	IRIG Fiber Receiver, Analog (Modulated) IRIG Time Code Transmission	https://app.bom.com/suppliers/detail-sourced_items?entity_id=896733756&orb_msg_single_search_p=1	
MP29-0000-0015	IRGR-7001	TTL ENCODED DC TIME CODE FIBRE OPTIC RECEIVER MODULE	https://app.bom.com/items/detail-spec?item_id=1214320694&version_id=10402159158	

*IRIG Cabling/Surge Protection/Output

Range Commander's Council (RCC) Inter-Range Instrumentation Group (IRIG) Standards. The Range Commanders Council (RCC) publishes several IRIG Standards with various time code formats. <http://www.wsmr.army.mil/RCCsite/Pages/default.aspx>



Note: IRIG.TIF pictures are stored in: <I:\Customer Service\IRIG>

IRIG Cable termination (50 ohm load for IRIG DCLS)

- 50 ohm termination recommended for IRIG DCLS outputs

Q We are using the SecureSync 1200 and are interested in using the 1205-04 option card for IRIG output. We will have the output connected to a separate IRIG distribution amplifier with a 600 ohm input/output impedance. I was hoping to get some guidance on what type of coaxial cable would be best to connect up from the 1204-05 card (looks like 50 ohm impedance) to the amplifier with 600 ohm impedance.

A (reply from Keith 12 May 2020) The coax cable recommended for IRIG distribution from the Model 1204-05 card is indeed RG-58 (50 ohm cable). This type cable is "readily available".

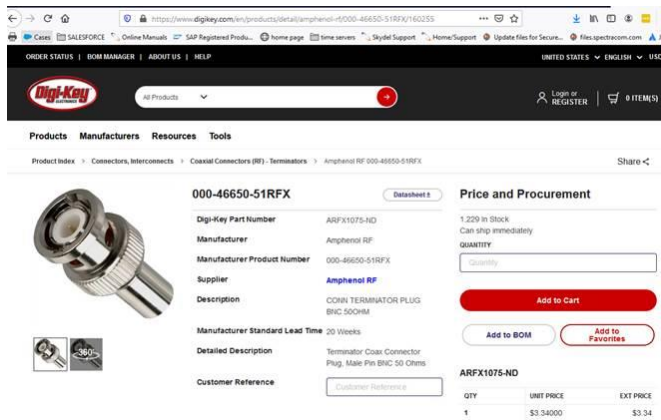
FYI: the IRIG signal is a very low frequency (such as 1kHz), so there is very little cable loss. RG-58 cables for IRIG can be run very long distances (hundreds of feet of cable should not be a problem at all).

When the Model 1204-05 Option Card's output ports are configured to output IRIG DCLS modulation (Instead of IRIG AM) it's recommended to place a 50 ohm load terminator on the cable end (opposite the end connected to the Model 1204-05 Option Card). This terminates the IRIG DCLS signal into a 50 ohm load, to help prevent reflections within the cable (when the end of the cable is attached to a device which has a 50 ohm load built-in, there is no need to add an additional terminator at the end of the cable).

"BNC" type 50 ohm load terminators can be readily found online, and can be attached to the end of the coax cable via the "open" side of a BNC "T" connector (the "T" connector attaches the end of the cable to the IRIG distribution amp, and has an additional connection that the BNC 50 ohm terminator is attached to).

Below is a good example of a recommended 50 ohm load terminator:

Amphenol P/N: 46650-51-RFX (Digi-Key P/N: ARFX1075-ND) <https://www.digikey.com/en/products/detail/amphenol-rf/000-46650-51RFX/160255>



***IRIG design specs

Refer to <https://wsmrc2vger.wsmr.army.mil/rcc/PUBS/pubs.htm> for all range master IRIG specs. Some of these have been saved to: [I:\Engineering\Specs and Standards\IRIG](#).

Link to 200-04 specs: http://www.scribd.com/doc/25690688/Irig-Standard-200-04#outer_page_37

Copy of IRIG specs (IRIG folder) : [I:\Engineering\Specs and Standards\IRIG](#)

“Demodulated IRIG” versus “unmodulated IRIG” (IRIG modulation types)

- IRIG AM: Sometimes referred to “modulated IRIG”.
- IRIG DCLS: Sometimes referred to “demodulated IRIG”, “unmodulated IRIG” and “RS-422 IRIG”

****IRIG Format codes

Manual or Automatic format selection		
First Letter: Rate Designation	A B D E G H	1000 PPS 100 PPS 1 PPM 10 PPS 10,000 PPS 1PPS
1 st Digit Form Designation	0 1 2	DC Level Shift (DCLS) width coded, no carrier Sine Wave carrier, amplitude modulated Manchester modulated
2 nd Digit Carrier Resolution	0 1 2 3 4 5 6	No carrier (DCLS) 100 Hz / 10 millisecond resolution 1kHz / 1 millisecond resolution 10 kHz 100 microsecond resolution 100 kHz / 10 microsecond resolution 100 kHz / 10 microsecond resolution 1 MHz / 1 microsecond resolution
3 rd Digit Coded expressions	0 1 2 3 4 5 6 7	BCD _{TOY} , CF, SBS BCD _{TOY} , CF BCD _{TOY} BCD _{TOY} , SBS BCD _{TOY} , BCD year, CF, SBS BCD _{TOY} , BCD year, CF BCD _{TOY} , BCD year, BCD _{TOY} , BCD year, SBS
Control Field (not part of the three digits)	0 1 2 3 4 5	Unknown - All bits ignored Fields conform to RCC 200-04 Fields conform to IEEE C37.118-2005 (1344 extensions) Fields conform to Spectracom format Fields conform to Spectracom FAA format Fields conform to NASA formats

BCD (binary Coded decimal) coding of time (HH, MM, SS, DDD) contains Seconds, Minutes, Hours, Day of Year
SBS is a counter with the number of seconds that have occurred since midnight (0...86400) (note- no year info)
CF (Control Functions) varies depending on the application

Available SecureSync IRIG Input / Output Formats:

RIG Code Format Provided	Code Description
A000	IRIG A, DCLS, BCD, CF, SBS
A001	IRIG A, DCLS, BCD, CF
A002	IRIG A, DCLS, BCD
A003	IRIG A, DCLS, BCD, SBS
A004	IRIG A, DCLS, BCD _{TOY} , BCD _{YEAR} , CF, SBS
A005	IRIG A, DCLS, BCD _{TOY} , BCD _{YEAR} , CF
A006	IRIG A, DCLS, BCD _{TOY} , BCD _{YEAR}
A007	IRIG A, DCLS, BCD _{TOY} , BCD _{YEAR} , SBS
A130	IRIG A, AM, 10kHz, BCD, CF, SBS
A131	IRIG A, AM, 10kHz, BCD, CF
A132	IRIG A, AM, 10kHz, BCD
A133	IRIG A, AM, 10kHz, BCD, SBS
A134	IRIG A, AM, 10kHz, BCD _{TOY} , BCD _{YEAR} , CF, SBS
A135	IRIG A, AM, 10kHz, BCD _{TOY} , BCD _{YEAR} , CF
A136	IRIG A, AM, 10kHz, BCD _{TOY} , BCD _{YEAR}
A137	IRIG A, AM, 10kHz, BCD _{TOY} , BCD _{YEAR} , SBS
B000	IRIG B, DCLS, BCD, CF, SBS
B001	IRIG B, DCLS, BCD, CF
B002	IRIG B, DCLS, BCD
B003	IRIG B, DCLS, BCD, SBS
B004	IRIG B, DCLS, BCD _{TOY} , BCD _{YEAR} , CF, SBS
B120	IRIG B, AM, BCD, CF, SBS
B121	IRIG B, AM, BCD, CF
B122	IRIG B, AM, BCD
B123	IRIG B, AM, BCD, SBS
B124	IRIG B, AM, BCD _{TOY} , BCD _{YEAR} , CF, SBS
B125	IRIG B, AM, 1kHz, BCD _{TOY} , BCD _{YEAR} , CF
B126	IRIG B, AM, 1kHz, BCD _{TOY} , BCD _{YEAR}
B127	IRIG B, AM, 1kHz, BCD _{TOY} , BCD _{YEAR} , SBS
G001	IRIG G, DCLS, BCD, CF
G002	IRIG G, DCLS, BCD
G005	IRIG G, DCLS, BCD _{TOY} , BCD _{YEAR} , CF
G006	IRIG G, DCLS, BCD _{TOY} , BCD _{YEAR}
G141	IRIG G, AM, 100kHz, BCD, CF
G142	IRIG G, AM, 100kHz, BCD
G145	IRIG G, AM, 100kHz, BCD _{TOY} , BCD _{YEAR} , CF
G146	IRIG G, AM, 100kHz, BCD _{TOY} , BCD _{YEAR} ,
G147	IRIG G, AM, 100kHz, BCD _{TOY} , BCD _{YEAR} , SBS

***IRIG Year info

- Available with “**CF**” and **BCDyear**” (third digit of: 0, 1, 4, 5, 6 or 7)

Sample list of codes that provide year info

IRIG Code	Description of IRIG string	Notes about year
B000	IRIG B, TTL, BCD, CF and SBS	Can provide year info in CF
B120	IRIG B, AM, 1 kHz , BCD, CF and SBS	Can provide year info in CF
B121	IRIG B, AM, BCD, CF	Can provide year info in CF
B122	IRIG B, AM, 1 kHz, and BCD _{TOY}	No year info provided. (Must set year in the device(s) receiving the IRIG signal)
B123	IRIG B, AM, 1 kHz , BCD _{TOY} , SBS	No year info provided (Must set year in the device(s) receiving the IRIG signal)
B124	IRIG B, AM, BCD _{TOY} , BCD_{YEAR} , CF , SBS	Can provide year info in BCDyear and/or CF
B125	IRIG B, AM, 1kHz, BCD _{TOY} , BCD_{YEAR} , CF	Can provide year info in BCDyear and/or CF
B126	IRIG B, AM, 1kHz, BCD _{TOY} , BCD_{YEAR}	Can provide year info in BCDyear
B127	IRIG B, AM, 1kHz, BCD _{TOY} , BCD_{YEAR} , SBS	Can provide year info in BCDyear
E000	IRIG E TTL, BCD _{TOY} , CF and SBS	Can provide year info in CF
E110	IRIG E AM, 100 Hz, BCD _{TOY} , CF and SBS	Can provide year info in CF
E120	IRIG E AM, 1 kHz, BCD _{TOY} , CF and SBS	Can provide year info in CF

IRIG B120 contains data in all portions of the IRIG B data stream, including data in the optional Control Field section, BCD data and SBS (straight Binary Seconds) data. IRIG B120 does contain more data than IRIG B122 and so IRIG B122 is a subset of IRIG B120. IRIG B120 indicates that the system requires an IRIG B signal with BCD data, but does not require any data be present in the Control Field section (it ignores the Control Field and does not require the SBS data to be present).

Most IRIG input systems commonly ignore the Control Field section altogether, so this system is not unique in this respect. If there is any data present in this section of the data stream (such as the Model 9383 populates), they usually just ignore this data (the primary data that is usually contained in the section of the data stream is the current year information). Since most systems (such as those that are B122) ignore the Control Field section, the year value in that system cannot be automatically set by the Model 9383 and so it will need to be manually set. Otherwise, a B122 system ignoring the Control Field is not a problem. As far as B122 not reading the SBS data, this should not be a problem either. With B122, the other system should just ignore the SBS data also contained in the B123 data stream.

In summary- Any system that is IRIG B122 input should just ignore the additional data that is contained in an IRIG B120 data stream and so it should interface with the Model 9383 with no problem, other than the need for the year to be manually set in that system because the year is only contained in the Control Field section, which the system ignores.

**Control functions (CF) info

- For more info, refer to IRIG specs, such as 200-04 <I:\Engineering\Specs and Standards>

3.2.8 **Control Functions.** All time code formats reserve a set of bits known as control functions (CF) for the encoding of various control, identification, and other special purpose functions. The control bits may be programmed in any predetermined coding system. A binary 1 bit has duration equal to 0.5 of the index count interval, and a binary (0) bit has duration equal to 0.2 of the index count interval. Control function bits follow position identifiers P_5 , P_6 or P_7 for formats A, B, E, and G beginning at index count 50, 60 or 70 with one control function bit per index count, except for each tenth bit which is a position identifier. The number of available control bits in each time code format is shown at Table 3-4.

TABLE 3-4. NUMBER OF AVAILABLE CONTROL BITS IN EACH TIME CODE FORMAT	
Format	Control Functions
A	18
B	18
D	9
E	36
G	27
H	9

Format B Control Function bit assignments

TABLE 6-7. FORMAT B CONTROL FUNCTIONS (45 BITS)					
Control Function BIT	BIT Time	Control Function BIT	BIT Time	Control Function BIT	BIT Time
1	Units of Year 01 $P_i + 5.0$ sec	10	$P_i + 6.0$ sec	19	$P_i + 7.0$ sec
2	Units of Year 02	11	$P_i + 6.1$ sec	20	$P_i + 7.1$ sec
3	Units of Year 03	12	$P_i + 6.2$ sec	21	$P_i + 7.2$ sec
4	Units of Year 04	13	$P_i + 6.3$ sec	22	$P_i + 7.3$ sec
5	$P_i + 5.4$ sec	14	$P_i + 6.4$ sec	23	$P_i + 7.4$ sec
6	Tens of Year 10	15	$P_i + 6.5$ sec	24	$P_i + 7.5$ sec
7	Tens of Year 20	16	$P_i + 6.6$ sec	25	$P_i + 7.6$ sec
8	Tens of Year 40	17	$P_i + 6.7$ sec	26	$P_i + 7.7$ sec
9	Tens of Year 80	18	$P_i + 6.8$ sec	27	$P_i + 7.8$ sec
Position Ident. (P_0)	$P_i + 5.9$ sec	Position Ident. (P_1)	$P_i + 6.9$ sec	Position Ident. (P_6)	$P_i + 7.9$ sec
Control Function BIT	BIT Time	Control Function BIT	BIT Time	Control Function BIT	BIT Time
28	$P_i + 8.0$ sec	37	$P_i + 9.0$ sec	BLANK	BLANK
29	$P_i + 8.1$ sec	38	$P_i + 9.1$ sec		
30	$P_i + 8.2$ sec	39	$P_i + 9.2$ sec		
31	$P_i + 8.3$ sec	40	$P_i + 9.3$ sec		
32	$P_i + 8.4$ sec	42	$P_i + 9.4$ sec		
33	$P_i + 8.5$ sec	43	$P_i + 9.5$ sec		
34	$P_i + 8.6$ sec	44	$P_i + 9.6$ sec		
35	$P_i + 8.7$ sec	45	$P_i + 9.7$ sec		
35	$P_i + 8.8$ sec		$P_i + 9.8$ sec		
Position Ident. (P_9)	$P_i + 8.9$ sec	Position Ident. (P_0)	$P_i + 9.9$ sec		

***IRIG G format and IEEE 1344

Q Is there any specific reasons why the IRIG-G output has only RCC 200-04 control bit support but IRIG-B has RCC 200-04 , IEEE1344,Spectracom FAA Format...

A reply from Dave Lorah (9 May 16) The IRIG G signal does not use a IEEE 1344 standard format. It only has the RCC 200-04 format. The Special FAA and Spectracom formats were not written for IRIG G. IRIG G is a less popular IRIG Format. Most users select IRIG B as the choice.

*****Year value/ “Spectracom Format” versus “RCC 200-04” format

Supported IRIG output configurations / 200-04 versus “Spectracom Format” (Model 8182/8183)

Q. From Wade Sober- What is IRIG rev 200-04? What IRIG formats does the 9383 support?

A. reply from Tom Richardson (11 July 2014) All the IRIG outputs included time information.

IRIG version 200-04 was an update to the IRIG standard to add year information.

This goes back a ways but referring to the 8183 manual, which the 9383 uses the same IRIG generator, we supported IRIG B and E version 200-98(1998) with Spectracom additions to the control codes for Time Sync Status at position P55 and Year information at P60 to P70. Because the year information was not included in version 200-98 this was a vendor specific implementation of the year information. The control codes could be used for anything.

When the year information was included in the IRIG standard at version 200-04(2004) the year information was included at positions P50 to P58 making the Spectracom format not comply with IRIG standard 200-04 because that's where we put the Time Sync status.

8183 Code word structure:

BCD: Word seconds digits begin at index count 1. Binary coded elements occur between position identifier elements P0 and P5 (7 for seconds, 7 for minutes, 6 for hours, and 10 for days) until the code word is complete. An index marker occurs between decimal digits in each group to provide separation for visual resolution. Least significant digit occurs first.

CF: IRIG formats reserve a set of elements known as Control Functions (CF) for the encoding of various control, identification, or other special purpose functions. IRIG B has 27 Control Functions located between elements 50 and 78. The NETCLOCK/GPS uses the Control Functions to encode year information and time sync status.

Element 55 is the time sync status bit. Element 55 is a Binary 1 when the front panel time sync lamp is green, and a Binary 0 when the lamp is red.

Year information consists of the last two digits of the current year (i.e. 97, 98, 99 etc.). Elements 60 through 63 contain the binary equivalent of year units. Elements 65 through 68 contain the binary equivalent of tens of years. In keeping with IRIG formats, the least significant bit occurs first. All unused Control Functions are filled with a space (Binary 0).

SBS: Word begins at index count 80. Seventeen Straight Binary Coded elements occur with a position identifier between the 9th and 10th binary coded elements. Least significant digit occurs first.

The fix for all this occurred with the SecureSync and its myriad of IRIG codes.

A) “Spectracom Format”

Year information

Partial email from Tom Richardson (11 July 2014) “ **CF:** IRIG formats reserve a set of elements known as Control Functions (CF) for the encoding of various control, identification, or other special purpose functions. IRIG B has 27 Control Functions located between elements 50 and 78. The NETCLOCK/GPS uses the Control Functions to encode year information and time sync status.”

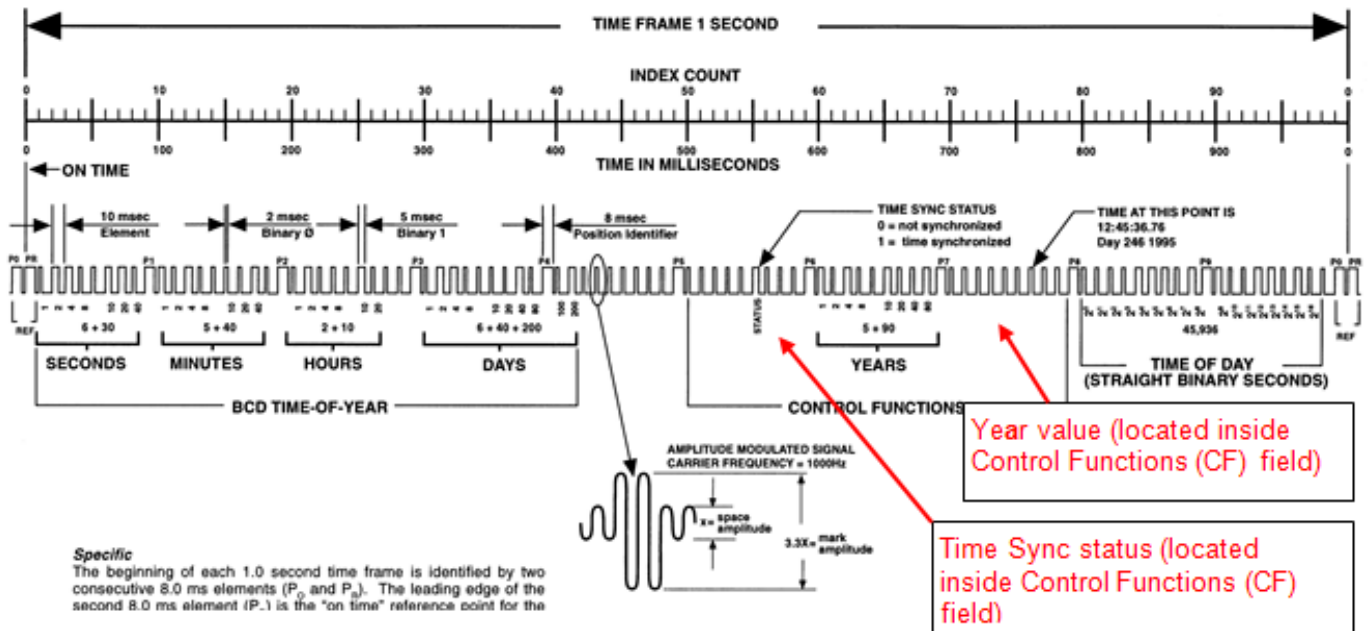
Time sync status

- Sync status of the time server is reported in the “Spectracom Format”

Partial email from Tom Richardson (11 July 2014) Element 55 is the time sync status bit. Element 55 is a Binary 1 when the front panel time sync lamp is green, and a Binary 0 when the lamp is red.

Below is the earlier “**Spectracom Format**” layout used in Model 9300 and earlier series NetClocks.

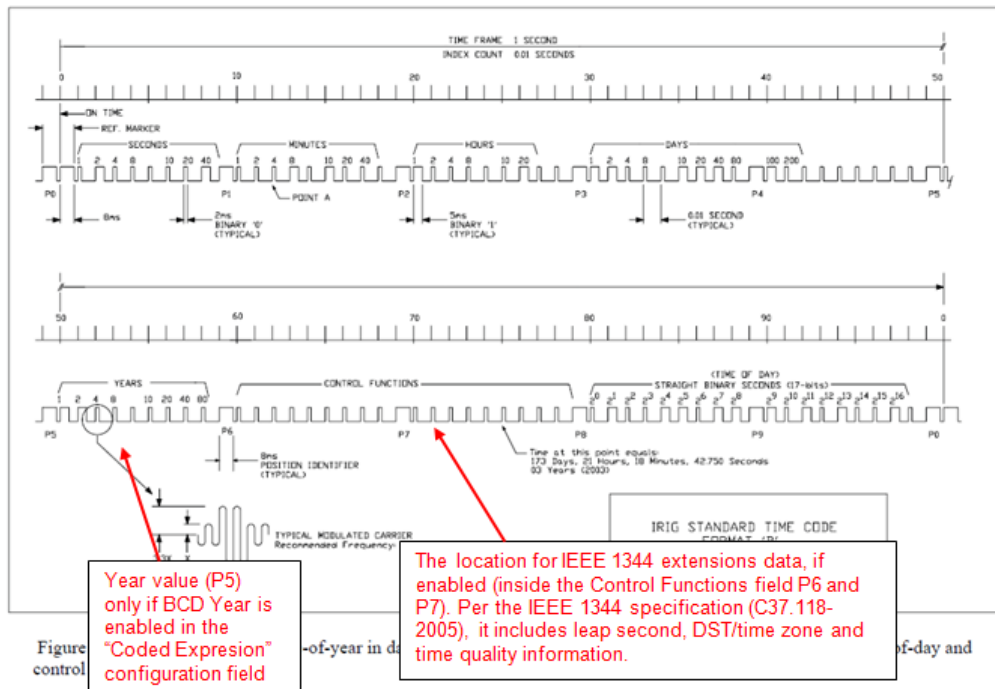
IRIG B TIME



B) RCC 200-04

- BCD year information was incorporated into IRIG with rev 200-04. We did not support this spec with the 93xx and 92xx products.
- This spec is available with SecureSyncs and TSync boards/

And here is the “RCC 200-04” format (available in SecureSyncs, Model 9483s and TSync-PCle):



Notice in the “Spectracom format, “Years” is located inside the “Control Functions” field, while in the RCC-2004 spec, the “Years” is located just before the “Control Functions”.

(Email from Dave Sohn 8/20/12)

Year information is not transmitted in the control fields for IEEE 1344. It is transferred in P5, and only if the unit is set with a coded expression that includes the year. With control fields enabled and using IEEE 1344 extensions, fields P6 and P7 are filled with information per the IEEE 1344 specification (C37.118-2005). It includes leap second, DST/time zone, and time quality information.

Email from Tom Richardson to Wade (11 July 14)

All the IRIG outputs included time information.

IRIG version 200-04 was an update to the IRIG standard to add year information.

This goes back a ways but referring to the 8183 manual, which the 9383 uses the same IRIG generator, we supported IRIG B and E version 200-98(1998) with Spectracom additions to the control codes for Time Sync Status at position P55 and Year information at P60 to P70. Because the year information was not included in version 200-98 this was a vendor specific implementation of the year information. The control codes could be used for anything.

When the year information was included in the IRIG standard at version 200-04(2004) the year information was included at positions P50 to P58 making the Spectracom format not comply with IRIG standard 200-04 because that's where we put the Time Sync status.

8183 Code word structure:

BCD: Word seconds digits begin at index count 1. Binary coded elements occur between position identifier elements P0 and P5 (7 for seconds, 7 for minutes, 6 for hours, and 10 for days) until the code word is complete. An index marker occurs between decimal digits in each group to provide separation for visual resolution. Least significant digit occurs first.

CF: IRIG formats reserve a set of elements known as Control Functions (CF) for the encoding of various control, identification, or other special purpose functions. IRIG B has 27 Control Functions located between elements 50 and 78. The NETCLOCK/GPS uses the Control Functions to encode year information and time sync status.

Element 55 is the time sync status bit. Element 55 is a Binary 1 when the front panel time sync lamp is green, and a Binary 0 when the lamp is red.

Year information consists of the last two digits of the current year (i.e. 97, 98, 99 etc.). Elements 60 through 63 contain the binary equivalent of year units. Elements 65 through 68 contain the binary equivalent of tens of years. In keeping with IRIG formats, the least significant bit occurs first. All unused Control Functions are filled with a space (Binary 0).

SBS: Word begins at index count 80. Seventeen Straight Binary Coded elements occur with a position identifier between the 9th and 10th binary coded elements. Least significant digit occurs first.

The fix for all this occurred with the SecureSync and its myriad of IRIG codes.

****Time sync status/Time Quality

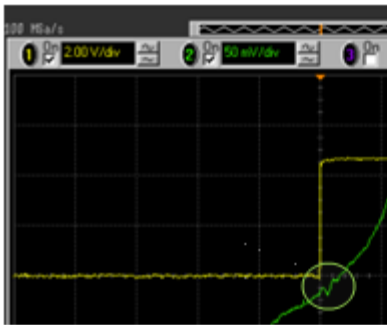
- Time Quality is reported in the IEEE-1344 extensions
- Time Sync status is reported in the “Spectracom Format”

Partial email from Tom Richardson (11 July 2014) Element 55 is the time sync status bit. Element 55 is a Binary 1 when the front panel time sync lamp is green, and a Binary 0 when the lamp is red.

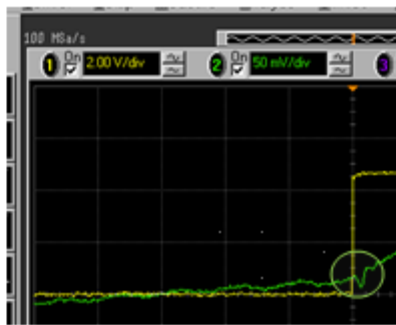
***IRIG PID marker for ON Time Point (OTP) / IRIG Accuracies

PID for On Time Point (OTP) for various IRIG AM signals

Note from Dave Sohn (referring to pictures below) Looking at the point where the slope of the signal changes in the image, you can see where we modulate the level of the IRIG signal, indicating the on-time point:



IRIG A



IRIG B



IRIG E

IRIG output accuracy (for products such as SecureSync and TSynC-PCIe):

Summary

Email from Dave LK (22 Sept 16) The accuracy spec for the SecureSync IRIG Output is dependent on whether you use IRIG AM or IRIG DCLS (TTL) output signals. Here are the Specs from the User Manual:

The IRIG outputs of the Spectracom Option Cards 1204-15, -1E, -22, and 1204-05, -27 deliver signals with the following 1PPS accuracy:

IRIG DCLS: Category Measured

IRIG A 30 ns

IRIG B 30 ns

IRIG G 30 ns

IRIG NASA 30 ns

IRIG E 30 ns

IRIG AM:

IRIG A 200 ns

IRIG B 800 ns

IRIG G 200 ns

IRIG NASA 800 ns

IRIG E 1.5 μ s

A) IRIG AM output

- We specify +/- 20 to 200 microseconds.

The IRIG output spec is to the "System Time" (which can be synced to GPS). The GPS spec for synchronization of the System Time to UTC can be added in to calculate the accuracy of the IRIG outputs to UTC time, if desired. The accuracy of the GPS receiver (and the "System Time" when synced to GPS) is +/- 15 ns of UTC time.

***IRIG input accuracy (for products such as TPRO/TSAT and TSynC-PCIe):

- **IRIG accuracy to UTC:** Consists of the synchronization to the IRIG source PLUS the stability/accuracy of the

IRIG source.

- **IRIG DCLS** input is much better than IRIG AM input because of the much faster rise-time of the DCLS signal. (the difference of one to just a few microseconds with IRIG DCLS versus 10s of microseconds with IRIG AM input). The faster the rise-time, the more accurate the synchronization,
- **IRIG B AM (1kHz carrier)** can provide sync accuracies in the tens of microseconds.

Our synchronization accuracy is dependent upon the accuracy of the incoming IRIG signal. Generally, DCLS is more accurate than AM, and faster carrier rates within AM are more accurate than slower rates. With a good IRIG source, accuracies can be achieved to the microsecond level.

Summary

Note: Table below is from the SecureSync user guide (Apr, 2017)

Signal Category	DCLS Measured Accuracy	AM Measured Accuracy
IRIG A	30 ns	200 ns
IRIG B	30 ns	800 ns
IRIG G	30 ns	200 ns
IRIG NASA	30 ns	800 ns
IRIG E	30 ns	1.5 us

As shown in the table above why are there variances in the IRIG AM input

Q What I am trying to understand is why the Amplitude Modulated signals vary in accuracy based on the different IRIG formats? And is this accuracy limited due to the specifics of the IRIG formats?

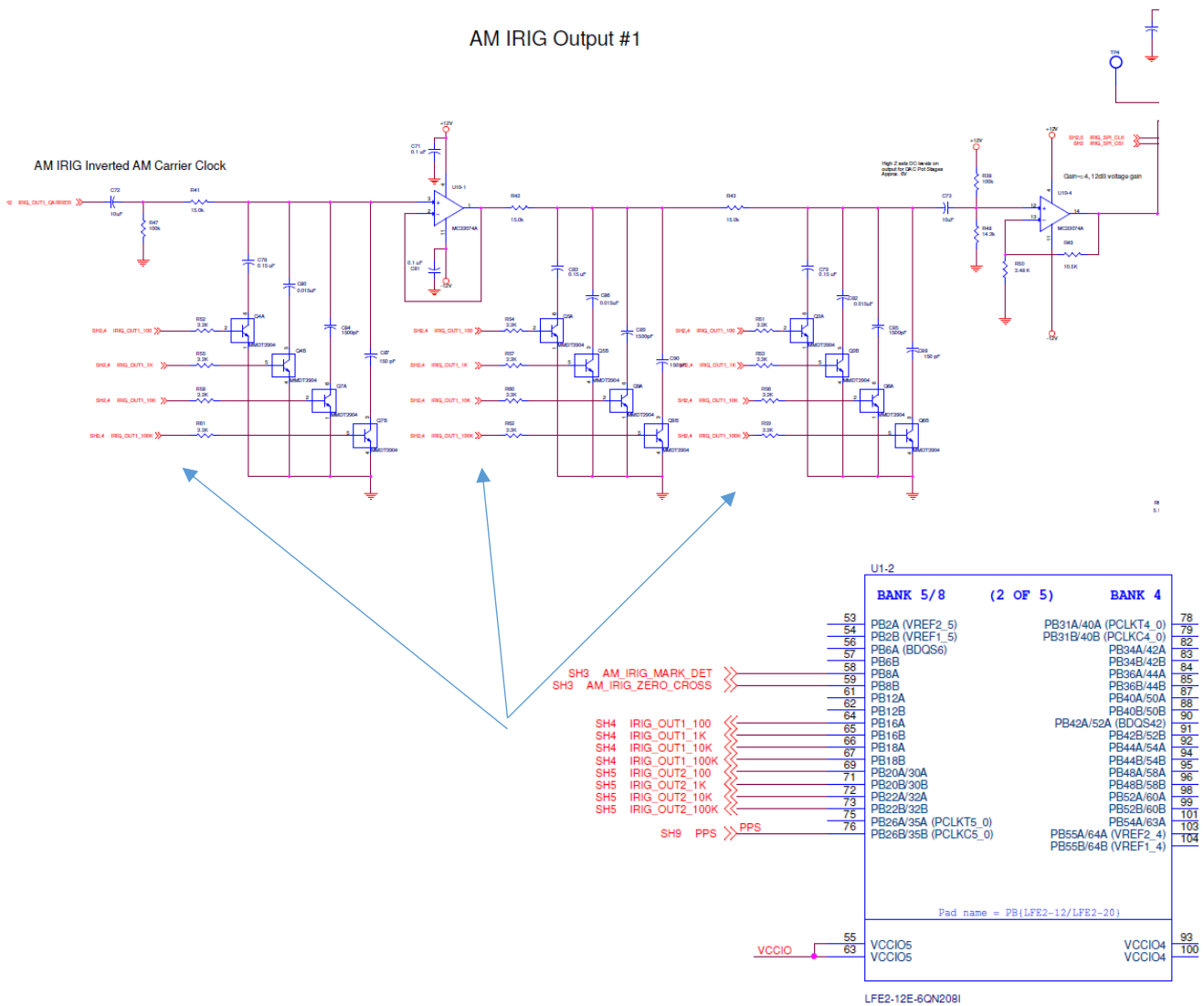
Need to confirm this info with Dave S (4/27/17 KW) Per Paul Myers, unlike IRIG DCLS, the IRIG AM circuit uses multiple digital pots that are configured based on which IRIG AM format (A, B, G etc) is selected, to best optimize the timing accuracy for each of the individual various formats. This change in pot configurations for each format results in slightly varying accuracies between each one.

See excerpts below for our understanding (internal use only- do not release these schematic excerpts):

Below schematic excerpts are for internal use only

From 1204-05 schematic: 1204-1051-0200

AM IRIG Output #1



Details of IRIG input/output accuracies

Email from Dave Sohn (26 Jan 2021) We can say what we can achieve generally through IRIG inputs, which is better than 1us for IRIG AM and 100ns for IRIG DCLS, but it will depend on the quality of the source of the IRIG (how stable and accurate it is).

A) IRIG DCLS input

- IRIG DCLS modulation can provide better accuracy than IRIG AM modulation, because IRIG DCLS has a much faster rise-time.
- The accuracy of DCLS or TTL is **+/- 100 nanoseconds** which is dependent or in addition to the accuracy of the source.

For example, if the accuracy of the source is 200 nanoseconds the DCLS or TTL would be 200 ±100 nanoseconds. Therefore, accuracy of the IRIG output would be 300 to 100 nanoseconds.

B) IRIG AM input

- The typical Spec for IRIG input to TSync/SecureSync is **+/- 20 to 200 microseconds** (from the IRIG generator-not to UTC)

This is not the accuracy of System Time to UTC (accuracy to UTC can only be spec'd with GPS input). This spec is only how close the System Time can be aligned to the IRIG source's output time. Our spec has to be added to the specs of the IRIG generator, assuming it's synced to an external reference, such as GPS. If the IRIG generator is not synced to an external reference, there is NO accuracy spec available for System Time sync to UTC time. The IRIG generator has to be traceable to UTC in order for a spec to UTC to be available.

For example, if the accuracy of the source is 200 nanoseconds the DCLS or TTL would be 200 nanoseconds, ± 200 microseconds. Therefore, accuracy of the IRIG output would be 20 to 200 microseconds (plus 200ns).

The Spec in the SecureSync manual ("**+/- 2 to 200 Microseconds**") encompasses all IRIG input formats (not just IRIG B, for instance). It is the "worst-case" range for all IRIG input signals. "Format dependent" is indicating whether the accuracy is closer to 2 microseconds or if it's closer to 200 microseconds depends on the IRIG carrier frequency being provided to the input and if it's an IRIG AM or IRIG DCLS modulated signal. No matter which IRIG format is provided to SecureSync, or what type of modulation is used, the System Time will be synced to within 200 microseconds of the IRIG generator's output time.

To calculate the accuracy of IRIG input to UTC:

- The IRIG generator needs to be synced to an external reference (such as GPS).
- You need to add the vendor's accuracy spec of its IRIG output to the IRIG input accuracy spec of:

DCLS input: +/- 100 nanoseconds

AM input: +/- 20 to 200 microseconds

We wound up spending extra time writing a time transfer algorithm for use between generic PCIe time cards and our own PCIe Network Analyzer card. This is pretty much completed so we will be testing with the Spectracom PCIe card in the next few days and into next week. We are hoping to get the absolute accuracy of packets time stamped by our Network Analyzer card close to 50 uSec or so. Obviously, with direct connection of the time card's 1PPS and 10 MHz to our board we would be able to get the accuracy closer to ~100 nSec.

One question has come up about using the Spectracom card in legacy or existing IRIG type timing networks. I have read the specs on the IRIG versions using the 1 kHz, 10 kHz, or even 100KHz carrier frequencies (and DCLS also), but have not been able to get a definitive answer on exactly what the absolute accuracy we could expect from an IRIG network. The specs talk about the resolution of the carrier being 1/frequency, but I also know that with suitable circuitry and phase locked loops you can determine the 'rising edge' of the sine wave of the nth cycle of the carrier that corresponds to the 1 PPS event. Obviously, jitter and noise of the circuits would compromise the detection, but is ~10 uSec or ~1 uSec typical absolute accuracies reasonable? What is the Spectracom specification for 1 PPS and 10 MHz output accuracy when the card is driven by an IRIG timing network?

****IRIG Cabling/max recommended cable distances

- There is no specific recommended maximum distance for an IRIG cable to be run, as many factors can affect the lengths of cable that can be run (such as types of cable used, noise sources located near the coax cable, etc).
- Typically, hundreds of feet of cable can be run from an IRIG source to one (or two) IRIG input devices with no problem at all. **Based on cable loss alone, 1000 feet of cable should be fine.**
- We recommend using **RG-58** coax cable
- Though it's used on the breakout cables, we **DO NOT** recommend using **RG-174** cable (due to high DC voltage drop through cabling)

For connecting devices to the IRIG output, we recommend using RG-58 or equivalent 50 ohm coax cable. The frequency of the IRIG signal is very low, so cable loss is not really a factor. Cable distances of 200-300 feet using RG-58 should not be a problem. RG-58 is readily available either locally or through companies such as Belden (<http://www.belden.com/>).

Luckily, IRIG is an extremely low frequency (typically either 100 Hz or 1000Hz), so the signal cable loss is extremely nominal, even when using a basic coax cable such as RG-58. RG-58 is a 50 ohm cable, which we recommend be used for the IRIG signal. However, noise and ground loops can be induced into very long cables, and these can affect the overall length of cable that can be run.

Note there is no specific recommended maximum distance for an IRIG cable to be run, as many factors can affect the lengths of cable that can be run (such as types of cable used, noise sources located near the coax cable, etc). Typically, hundreds of feet of cable can be run from an IRIG source to one (or two) IRIG input devices with no problem at all. Based on cable loss alone, 1000 feet of cable should be fine. As the input impedance of the receiving device(s) can affect the signal level if the same signal is fed to several devices in a row, when connecting the signal to more than a couple of devices, it is recommended to use an IRIG distribution amplifier that allows each of its outputs to provide the IRIG signal to each device. Splitting the IRIG signal to several devices without the use of an IRIG distribution amplifier could cause potential problems with the IRIG signal.

The primary factor of running long distance coax cable for IRIG is the input sensitivity of the device receiving the IRIG signal. The more sensitive the input, the longer the cable can be. If its sensitivity is too low (a larger signal is required for it to accept the IRIG signal) with a long distance between the IRIG generator and the receiving device (especially if it's over 1000 feet), fiber optic cabling is likely a better solution than standard coax (via either Fiber Optic output from the IRIG source or via Coax to Fiber- Fiber to Coax converters).

Note that if the receiving device can accept either IRIG DCLS or AM modulation, DCLS provides the most optimum timing accuracy (because it's faster rise-time than IRIG AM modulation provides results in a better 1PPS on-time point for the receiving device).

Note: The longer the cable, the larger the cable delays become (resulting in an offset between the IRIG Master and the IRIG Slave). Refer to the next section down ("IRIG Signal cable delays) for info on compensating for the inherent cable delays.

RG-174 coax cable (used in TSync breakout cables but not recommended to run from the breakout cable to equipment)

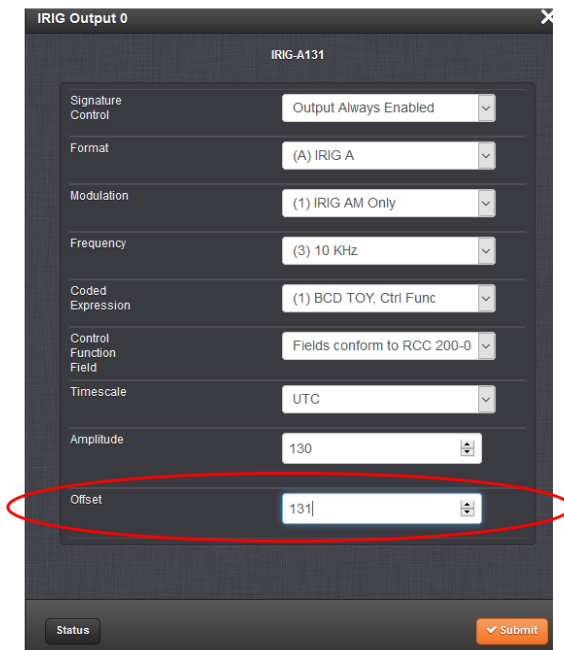
- Refer to Salesforce case 174338
- Though we use a very short length of it in breakouts- not recommended for distribution to equipment

Email from Dave Lorah (24 Sept 2018) We use the RG-174 for this cable but it is limited to a maximum length of 15 Meters. Your RG-174 cable is approximately four times this length and would have a lot of signal attenuation. This is due to the electrical resistance of the 26 AWG wire in the RG-174 vs the 20 AWG in the RG-58 cable.

Tam is going to move the IRIG Slave unit close to the IRIG Master and check if it syncs with a shorter cable. This will prove the configuration is correct and the two units are working properly.

***IRIG signal cable/processing delays

- Cabling between the IRIG output connector of the slave, and the inherent processing delays for the Slave to sync to the IRIG signal, can be compensated for in each IRIG output of a Spectracom IRIG source (such as SecureSync, NetClocks and TSync boards)
- To compensate for processing and/or cable delays, calculate the signal delay through the coax cable (based on type and length of the cable) and if the processing delay of the IRIG slave is known, add these two values together
- Enter the combined cable/processing delay value into the “**Offset**” field of the IRIG output configuration. (such as the **Interfaces -> IRIG Output 0** page of the SecureSyncs browser)



Cable delays for RG-58 at 1 kHz (such as IRIG B)

- Cable delay through RG-58 cable is about **1 to 1.5 ns/foot of cable** (or 3 to 5ns/meter).
- Multiply the total length of IRIG coax cable between the Master and Slave (in feet) **by 1.5** to calculate the approximate cable delay. Enter this value in the Offset field of the IRIG output. If the processing delays of the Slave is known, add this value to the cable delay and enter this total value instead,

****IRIG time-code over fiber for Secure Networks

- Refer to: <http://www.spectracomcorp.com/Desktopmodules/Bring2Mind/DMX/Download.aspx?EntryId=1606&PortalId=0>

****IRIG fiber converters (for long distance runs):

- Refer to: [!:Engineering\Fiber Optic](#)

Example AM and DCLS Fiber converters for IRIG:

Company name: LuxLink <http://www.luxlink.com/products/irig.htm>

Fiber to Coax converter

Q From Gilles: BAE System in UK is asking us to propose a solution to connect the output IRIG B over fiber from a SecureSync to the input of a TSync that will use the signal as external reference. Do some of you already propose a conversion box or any other solution to convert fiber output to IRIG compatible with TSync input?

A Reply from Lisa Perdue (6 Aug 2015) For conversion from Fiber back to TTL levels we have used this converter here in the past.

<http://www.sitech-bitdriver.com/products/ttl.htm>

The one we have is Model 2871-T/R because we have used it to transmit and receive but you can get a receive only version.

IRIG interleaving

Q. Regarding the fiber optic interface...do you have established interoperability with any other vendors – or is the fiber interface specified in one of the IRIG standards? We have a competitor (Schweitzer Engineering Labs, SEL) that interleaves IRIG-B signaling with RS-232 data on serial fiber, and I'm curious if this is similar to what you're doing (minus the serial data) or if there is a standardized method to put IRIG timing on fiber...

A. Reply from Tom Richardson It is just IRIG output on fiber. As far as I know the IRIG spec doesn't specify any media interface. Could be coax cable or microwave data link. You could ask Keith about any interoperability with other vendors. By interleaving he probably means multiplexing more than one signal on the fiber and then de-multiplexing at a receiver. We don't do that.

IRIG Surge Suppression:

The IRIG outputs of the Models 8183, 9183 and some NetClock/2's have transorbs on the output to help protect the NetClocks from surge damage. However, if additional external protection is desired, they can purchase our Model MP08455 PolyPhaser surge suppressor (this device is the WWVB antenna surge suppressor but will also work at the frequency of WWVB).

****IEEE-1344 extensions (IEEE C37.118-2005) and “Spectracom IEEE C37.118-2005”

- Refer to IEEE-1344 specs: [I:\Engineering\Specs and Standards\IEEE \(Institute of Electrical and Electronics Engineers\)](I:\Engineering\Specs and Standards\IEEE (Institute of Electrical and Electronics Engineers))
- The IRIG output of the earlier Model NetClocks (such as NetClock/2. And 8183 for examples) are not IEEE-1344 compliant (this spec is for power station synchronization).
- The actual IRIG spec that we designed to is located in: <I:\Engineering\Specs and Standards\IRIG>.
- SecureSyncs, TSync boards and NetClock Model 9483s can provide IEEE-1344 extensions (to include year info)

IRIG is spec'd in IEEE-1344 as well as AFNOR NF S87-500. IEEE-1344 has since been replaced by IEEE C37.118 (such as IEEE C37.118-2005) but it's still often called “IEEE-1344)

IEEE Standard for Synchrophasors for Power Systems
Institute of Electrical and Electronics Engineers
01-Jan-2006

IEEE-1344 Extensions

Year information was not specified in the IRIG standard prior to its 2004 revision. Before 2004, the IEEE adopted a standard (IEEE-1344) which included year data as part of the IRIG-B signal. This variation came to be known as “IEEE-1344 extensions.”

IEEE-1344 extensions use extra bits of the Control Functions (CF) portion of the IRIG-B time code. Within this portion of the time code, bits are designated for additional features, including:

- Calendar Year (now called BCDYEAR)
- Leap seconds, and leap seconds pending
- Daylight Saving Time (DST), and DST pending
- Local time offset
- Time quality
- Parity
- Position identifiers

To be able to use these extra bits of information, power system devices and other equipment receiving the time code must be able to decode them. Refer to individual product manuals to determine whether IEEE-1344 extensions are supported.

Since year information is now considered part of BCD (denoted as BCD~~YEAR~~), what was formerly considered B002 and B122 (with IEEE Extensions ON) would now be denoted as B006 and B126.

From Wikipedia: IEEE 1344 is a standard that defines parameters for [synchrophasors^{\[1\]}](#) for power systems.^[2] The standard added extension to the [IRIG-B time code](#) to cover year, time quality, daylight savings time, local time offset and leap second information.

IEEE-1344 Extensions (from: http://www.cyber-sciences.com/documents/TN-102_IRIG-B.pdf)

Year information was not specified in the IRIG standard prior to its 2004 revision. Before 2004, the IEEE adopted a standard (IEEE-1344) which included year data as part of the IRIG-B signal. This variation came to be known as “IEEE-1344 extensions.”

IEEE-1344 extensions use extra bits of the Control Functions (CF) portion of the IRIG-B time code. Within this portion of the time code, bits are designated for additional features, including:

- Calendar Year (now called BCDYEAR)
- Leap seconds, and leap seconds pending
- Daylight Saving Time (DST), and DST pending
- Local time offset
- Time quality
- Parity

- Positon identifiers

Control bit assignments

Table F.1—Control bit assignments

IRIG-B Pos ID	CTRL bits	Designation	Explanation
P 50	1	Year, BCD 1	Last 2 digits of year in BCD
P 51	2	Year, BCD 2	IBID
P 52	3	Year, BCD 4	IBID
P 53	4	Year, BCD 8	IBID
P 54	5	Not used	Unassigned
P 55	6	Year, BCD 10	Last 2 digits of year in BCD
P 56	7	Year, BCD 20	IBID
P 57	8	Year, BCD 40	IBID
P 58	9	Year, BCD 80	IBID
P 59	—	P6	Position identifier # 6
P 60	10	Leap Second Pending (LSP)	Becomes 1 s up to 59 s BEFORE leap second insert
P 61	11	Leap Second (LS)	0 = Add LS, 1 = Delete LS
P 62	12	Daylight Saving Pending (DSP)	Becomes 1 s up to 59 s before DST change
P 63	13	Daylight Savings Time (DST)	Becomes 1 during DST
P 64	14	Time Offset sign	Time offset sign—0 = +, 1 = -
P 65	15	Time Offset—binary 1	Offset from coded IRIG-B time to UTC time. IRIG coded time plus time offset (including sign) equals UTC time at all times (offset will change during DST).
P 66	16	Time Offset—binary 2	
P 67	17	Time Offset—binary 4	
P 68	18	Time Offset—binary 8	
P 69	—	P7	Position identifier # 7
P 70	19	Time Offset—0.5 h	0 = none, 1 = additional 0.5 h time offset
P 71	20	Time Quality	4-bit code representing approx. clock time error. 0000 = clock locked, maximum accuracy 1111 = clock failed, data unreliable
P 72	21	Time Quality	
P 73	22	Time Quality	
P 74	23	Time Quality	
P 75	24	PARITY	Parity on all preceding data bits
P 76	25	Not Used	Unassigned
P 77	26	Not Used	Unassigned
P 78	27	Not Used	Unassigned
P 79	—	P8	Position identifier # 8

Year (BCD year)

Leap Seconds

DST pending/DST correction

Local time offset

Time quality

Parity

Notes about the IEEE 1344 extensions:

1. The NetClocks (such as the Model 8183, 9183, 9283, 9383) do not support the IEE1344 extensions.
2. The1344 extensions are available with SecureSync and the TSync-PCIe boards.
3. The 1344 extension only apply to the IRIG B formatting (they don't apply to IRIG A, E, etc).

Email from Dave Lorah (15 June 16) Here is a list of the Spectracom IEEE C37.118-2005 Control Functions Control Field Elements from the manual. The Sync Status bit is at pos 55 and the year data from pos 60 to 68.
I hope this information helps. Please let me know if you need anything else.



“Spectracom IEEE C37.118-2005” (IEEE-1344 extensions plus leap second info)

- New Control Function added to distribute leap second info
- Version 5.2.1 Added **IRIG** control field format, “**Spectracom IEEE C37.118-2005**”, to extend **leap second notification** to a month.
- Intended for SecureSyncs syncing via IRIG input and outputting NTP (SecureSync acting like a Slave to another SecureSync). Without this new control field, the leap second won't be announced until just one minute before the leap second is inserted. This doesn't leave enough time for NTP on those IRIG units to read the leap second and announce it in time.
- Was primarily for Verizon, but others can benefit from this new capability

Manchester coding

- Below info is from the IRIG standard 200-04

Standard Manchester modulation or encoding is a return-to-zero type, where a rising edge in the middle of the clock window indicates a binary one (1) and a falling edge indicates a binary zero (0). This modification to the Manchester code shifts the data window so the data are at the edge of the clock window that is on time with the one-pulse-per-second clock synchronized to Coordinated Universal Time (UTC). Thus, the data edge is the on-time mark in the code. Because this code is easy to generate digitally, easy to modulate onto fiber or coaxial cable, simple to decode, and has a zero mean, and the code is easy to detect even at low voltage levels.

The basic Modified Manchester modulation, compared with the AM and level shift modulations are shown at Figure 4-2 and Figure 4-3. The Manchester encoding uses a square-wave as the encoding (data) clock, with the rising edge on time with UTC. The frequency of the encoding clock shall be ten times the index rate of the time code generated. As an example, the clock rate for IRIG B230 shall be 10 kHz.

The Modified Manchester coding technique has several advantages as noted below.

- No dc component
- Can be ac coupled
- Better signal-to-noise ratio
- Good spectral power density
- Easily decoded
- Better timing resolution
- The link integrity monitoring capability is intrinsic to bipolar pulse modulation.
- The coding technique is designed to operate over fiber-optic or coaxial lines for short distances.

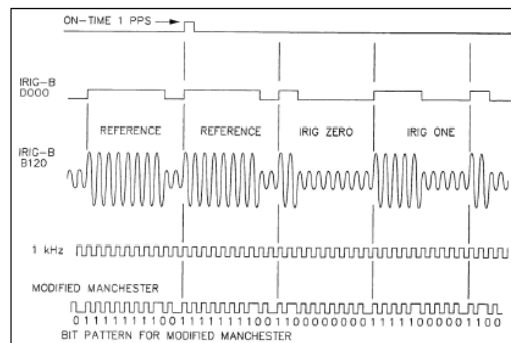


Figure 4-2. IRIG B coding comparisons: level shift, 1kHz am, and Modified Manchester.

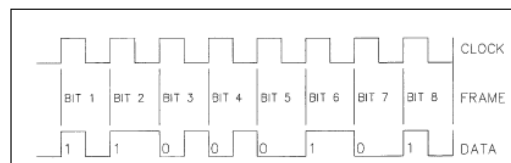


Figure 4-3. Modified Manchester coding.

***FAA IRIG

Description of FAA IRIG: Refer Addendum, A of the 8183A manual (<I:\Engineering\Archive\Released\069000 - 8183\Manual\CURRENT RELEASE\PDF>) as shown below

FAA IRIG CODE DESCRIPTION

A.0 INTRODUCTION

This Appendix contains a detailed description of the FAA modified IRIG B code. The FAA modifies the IRIG B code by including satellite lock status and time error flags in the Control Function Field. The error flags provide an inaccuracy estimate based on the time elapsed since loss of GPS lock. In addition, the Straight Binary Seconds (SBS) data was removed from the data stream. The SBS time is the number of seconds elapsed since midnight.

The NetClock/GTP can be configured to provide IRIG timing reflecting Universal Coordinated Time (UTC) or local time, with or without daylight saving time corrections. The *IRIG* command configures the IRIG time structure and is described in Section 4, *Software Commands*.

A.1 FAA IRIG B OUTPUT

The FAA IRIG B code contains the Binary Coded Decimal (BCD) time of year and a Control Function (CF) field containing satellite lock status and time error flags. With the exception of the position identifiers, all remaining code elements are set to a binary 0. Figure A-1 illustrates the FAA IRIG B data structure. The BCD time of year provides the day of the year, 001-366, and the time of day including seconds. The hour of the day is expressed in 24-hour format.

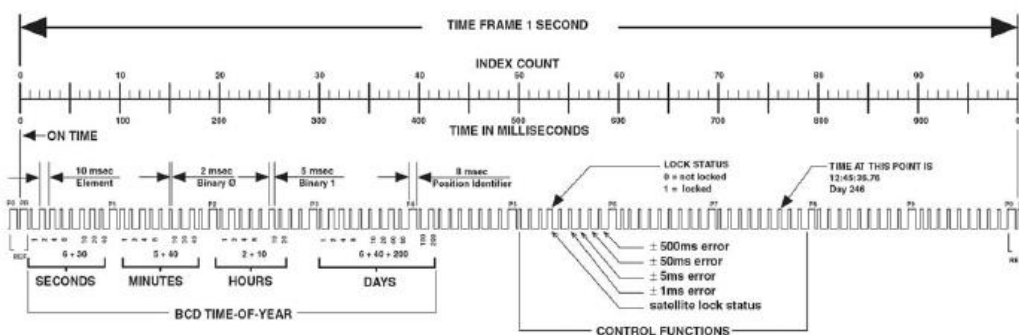
A.1.1 FAA IRIG B General Description

1. Time frame: 1.0 seconds.
2. Pulse rates:
 - A. Element rate: 100 per second.
 - B. Position identifier rate: 10 per second.
 - C. Reference marker rate: 1 per second.
3. Element identification: The "on time" reference point for all elements is the pulse leading edge.
 - A. Index marker (Binary 0 or uncoded element): 2 millisecond duration.
 - B. Code digit (Binary 1): 5 millisecond duration.

NetClock/GTP Instruction Manual

Page A-1

FAA MODIFIED IRIG B



Specific

The beginning of each 1.0 second time frame is identified by two consecutive 8.0 ms elements (P₀ and P₉). The leading edge of the second 8.0 ms element (P₉) is the "on time" reference point for the succeeding time code. 10 pps position identifiers P₀, P₁, ..., P₉ (8.0 ms duration) occur 10 ms before 10 pps "on time" and refer to the leading edge of the succeeding element.

The time code word and the control functions presented during the time frame are pulse width coded. The binary "zero" and index markers have a duration of 2.0 ms, and the binary "one" has a duration of 5.0 ms. The leading edge is the 100 pps "on time" reference point for all elements.

The binary coded decimal (BCD) time-of-year code word consists of 30 digits beginning at index count 1. The binary coded subword elements occur between position identifiers P₀ and P₉ (7 for seconds; 7 for minutes; 6 for hours; 10 for days) until the code word is complete. An index marker occurs between the decimal digits in each subword to provide separation for visual resolution. The least significant digit occurs first. The BCD code recycles yearly.

Twenty-seven control functions occur between position identifiers P₉ and P₀. FAA uses this field to communicate satellite lock status and time error and indicators. The first flag element is at 530 ms which indicates satellite lock. The +/- 1ms error flag occurs at 550 ms. The +/- 5 ms error flag occurs at 560 ms. The +/- 50 ms error flag occurs at 570ms. The +/- 500 ms error flag occurs at 580 ms.

The straight binary (SB) time-of-day code word normally found between position identifiers P₉ and P₀ is eliminated for FAA IRIG B. All elements between position identifiers P₉ and P₀ are set to Binary 0.

FIGURE A-1 FAA IRIG B TIME CODE

- C. Position Identifier: 8 millisecond duration.
- D. Reference marker, 1 per second. The reference marker appears as two consecutive position identifiers. The second position identifier marks the on-time point for the succeeding code word.
4. Resolution: 10 milliseconds.
5. Code word structure:
- BCD: Word seconds digits begin at index count 1. Binary coded elements occur between position identifier elements P₀ and P₅ (7 for seconds, 7 for minutes, 6 for hours, and 10 for days) until the code word is complete. An index marker occurs between decimal digits in each group to provide separation for visual resolution. Least significant digit occurs first.
- CF: IRIG formats reserve a set of elements known as Control Functions (CF) for the encoding of various control, identification, or other special purpose functions. IRIG B has 27 Control Functions located between elements 50 and 78. The FAA IRIG B code uses five of the Control Function elements to encode satellite lock status and time error flags. For a description of the status and error flag implementation, refer to Table A-1 and the paragraphs below.
- Element 53 (530 ms) is the time sync status bit. Element 53 is a Binary 1 when the receiver locked to GPS, and a Binary 0 when the receiver is not locked to GPS.
- Element 55 (550 ms) is the +/- 1.0 millisecond error flag. Element 55 is set to Binary 1 when the expected time error is within +/- 1.0 millisecond, and a Binary 0 during all other conditions of operation.
- Element 56 (560 ms) is the +/- 5.0 millisecond error flag. Element 56 is set to Binary 1 when the expected time error is within +/- 5.0 milliseconds, and a Binary 0 during all other conditions of operation.
- Element 57 (570 ms) is the +/- 50 millisecond error flag. Element 57 is set to Binary 1 when the expected time error is within +/- 50 milliseconds, and a Binary 0 during all other conditions of operation.
- Element 58 (580 ms) is the +/- 500 millisecond error flag. Element 58 is set to Binary 1 when the expected time error is within +/- 500 milliseconds, and a Binary 0 during all other conditions of operation.

Appendix A: FAA IRIG Code Description

Time Since Loss of Lock	Status/Error	Lock Indicator	±1 msec	±5 msec	±50 msec	±500 msec
N/A	Locked Error < 2us	1	0	0	0	0
< 00:16:40	Unlocked Error < 1 ms	0	1	0	0	0
00:16:41 to 01:23:39	Unlocked Error < 5 ms	0	0	1	0	0
01:23:40 to 13:53:19	Unlocked Error < 50 ms	0	0	0	1	0
13:53:20 to 5 days 18:53:19	Unlocked Error < 500 ms	0	0	0	0	1
>5 days 18:53:20	Unlocked Error Unknown	0	0	0	0	0
N/A	Power On	0	0	0	0	0

TABLE A-1 FAA TIME ERROR INDICATORS

****CTQ (Continuous Time Quality) (part of IEEE C37.118.1- 2011)

- Refer to Salesforce case 17145
- This appears to be the “Time quality” indicator included in the IEEE-1344 extensions.
- Refer to http://en.wikipedia.org/wiki/IEEE_1344

Email from Tom Richardson (12 Feb 15)

I can't say for certain.

Found I:\Engineering\Specs and Standards\IEEE (Institute of Electrical and Electronics Engineers)\IEEE 1344\ C37.118-2005.pdf

Since I don't have 2011 I can't say we comply. I see that they use P71 to P74 control bits to do the time quality in the 2005 standard and I don't see where we state that we do that. Where did you find the time quality info?

IRIG Input/Output (for Models 9383 and 9283 and 9183)

The NetClock's IRIG output connector can provide the following IRIG Formats

NetClock IRIG outputs

IRIG Code Format	Description of code
B000	IRIG B, TTL, BCD,CF and SBS
B120	IRIG B, AM, 1 kHz, BCD,CF and SBS
E000	IRIG E TTL, BCD,CF and SBS
E110	IRIG E AM, 100 Hz, BCD,CF and SBS
E120	IRIG E AM, 1 kHz, BCD,CF and SBS

Note: Believe they also support B122 and E122.

Note the NetClock's IRIG output does not provide the year in the same location in the control field as IRIG spec 200-04. The NetClock places the year in a different location in the control field. (Unlike TSync-PCIe and SecureSync, which can output either 200-04 or the "Spectracom Format" of the year value being in a different spot of the control field, the NetClocks can only output the "Spectracom Format"

Email from Mark McGregor to customer on 7/18/06

Q. I would just like to clarify which document should I use as a reference to describe the IRIG output of the 9183?

I received a PDF of the 200-95 document.

I received a PDF of the 200-04 document.

In Mark's e-mail, he mentions a 200-98 document.

A. In answer to your question, they all are applicable to the 9183 IRIG output.

The 9183 complies with the IRIG spec up to 200-98 (put out in 1998). For IRIG-B AM we put out B120 and for the TTL version output we put out B000. This is BCD Time Of Year (TOY), Straight Binary Seconds (SBS), and Control Functions (CF). We chose to use sub-frame 7 control function field to implement the two digit year code, as it was not specified up through the 200-98 IRIG spec. This would be labeled as sub-frame 6 in the timing diagrams of the IRIG spec., as the IRIG spec. calls the first sub-frame "0" instead of "1".

In the 200-04 IRIG spec., we still comply with the IRIG formats stated above. In the 200-04(put out in 2004) IRIG spec., the year information was added in sub-frame 6 (the IRIG spec. would call it sub-frame 5 or P5). IRIG that contains the year information per the IRIG 200-04 would be B124 or B127 for the AM, and B004 or B007 for the DC PWM TTL IRIG. The 9183 IRIG is still B120 for AM and B000 which is BCD Time Of Year(TOY), Straight Binary Seconds (SBS), and Control Functions (CF), no year encoded per the spec. 200-04. The year is in the 9183 IRIG, just put out as a control function in sub-frame 7.

For NetClock IRIG input (Option 06), refer to: [Option 6: IRIG input](#)

IRIG for TPRO-TSAT/ PCI, PCI-U, PCI-66U

PCI- Detects and outputs B122

PCI-U Detects and outputs B122

PCI-U-2 (PCI-33U) and PCI-66U

Input: Can accept IRIG-A (A132), IRIG-B (B122) and NASA36

Output: IRIG-B (B122) only

IRIG for TSynC-PCle

TSynC-PCle inputs

- The TSynC-PCle board supports IRIG inputs of the following coded expressions combinations for BCD_{TOY}, CF, SBS, and BCD_{YEAR} fields:
- 0 – BCD_{TOY}, CF, SBS
 - 1 – BCD_{TOY}, CF
 - 2 – BCD_{TOY}
 - 3 – BCD_{TOY}, SBS
 - 4 - BCD_{TOY}, BCD_{YEAR}, CF, SBS
 - 5 - BCD_{TOY}, BCD_{YEAR}, CF

The TSynC-PCle supports synchronization with the following analog and DCLS IRIG input formats:

A - DCLS	A - AM	B - DCLS	B - AM	G - DCLS	G - AM
A000	A130	B000	B120	NA	NA
A001	A131	B001	B121	G001	G141
A002	A132	B002	B122	G002	G142
A003	A133	B003	B123	NA	NA
A004	A134	B004	B124	NA	NA
NA	NA	NA	NA	G005	G145

Table 5-5-1 — IRIG Input Reference Formats

Available TSynC-PCle Outputs

The TSynC-PCle board allows the user to select the following Time Code Formats for IRIG output:

A - DCLS	A - AM	B - DCLS	B - AM	E - DCLS	E - AM	G - DCLS	G - AM
A000	A130	B000	B120	E000	E110	NA	NA
A001	A131	B001	B121	E001	E111	G001	G141
A002	A132	B002	B122	E002	E112	G002	G142
A003	A133	B003	B123	E003	E120	NA	NA
A004	A134	B004	B124	E004	E122	NA	NA
NA	NA	NA	NA	E005	E125	NA	G145

Table 5-5-3 — IRIG Output Reference Formats

The TSynC-PCle allows the user to select the IRIG B variant NASA36 as an IRIG output. It also supports user-selection of IEEE C37.118-2005 as an IRIG output. This is an IRIG B format with extensions. The TSynC-PCle board is compliant with IEEE 1344-1996 as IEEE C37.118-2005 supersedes this specification.

The board generates the non-standard IRIG formats that are generated by the Spectracom Netclock, including the non-standard BCD_{YEAR}. This provides for compatibility with existing Spectracom NetClock products.

IRIG B152

1/14/11 KW Email from Dave Sohn: None of our boards are currently capable of outputting IRIG B152 (IRIG B AM with 1MHz carrier frequency). The typical carrier frequency for IRIG B is 1kHz. In fact, the highest carrier rate we support at all is 100kHz for IRIG G.

This would be a SW and HW update to support this. In our Kramden IRIG output implementations (TSync, SecureSync), each carrier rate requires its own selectable filter to convert from a digital carrier to an analog carrier wave. Adding a new carrier rate would require adding an additional selectable filter to the board (PCB spin) and updating the SW and FPGA to support selection of this new filter. If this is a large opportunity it may be worthwhile, but I haven't heard of anyone using B152 prior to this.

****IRIG/ASCII Event Count Status messages (CS1, CS2, CS3, CS4 and CS5)

(CS-1, CS-2, CS-3, CS-4, CS-5)

Range Commander's Council (RCC) Inter-Range Instrumentation Group (IRIG) Standards. The Range Commanders

Council (RCC) publishes several IRIG Standards with various time code formats: <http://www.wsmr.army.mil/RCCsite/Pages/default.aspx>

CS1 through CS4

Purpose- (Per IRIG Standard 215-96)

Event count status formats to be used to transfer event count status over conventional asynchronous telecommunications circuits. These formats provide event count status information suitable for most computer, dumb terminal, line printer, and remote visual displays

We do not support Event Count Status (as of 9/20/10) (CS-1, CS-2, CS-3, CS-4 or "CS1, CS2, CS3, CS4")

Refer to IRIG standard 209-90 for CS1 through CS-4: <https://wsmrc2vger.wsmr.army.mil/rcc/manuals/209-90/209-90.pdf> for more information on Event Count Status.

Note: this document has been scanned. Find/Search in this document doesn't work.

CS5 IRIG Time code (Count-down timer message)

Refer to "IRIG Standard 215-96" for CS5 messages. <https://wsmrc2vger.wsmr.army.mil/rcc/manuals/215-96/index.html>


Email from Dave Sohn to Tony Diflorio (1/28/13) These time codes are not typically used to provide time, but rather to provide event countdown timers. What is the use case for an input like this?


Email from Keith to Tony Diflorio (1/29/13) Hi Tony,

FYI –These are unique ASCII formats- not IRIG formats. The Timing boards can't currently accept ASCII data. The closest solution would be SecureSyncs –not timing boards. Below is one of the CS5 ASCII messages from Standard 215-96

SecureSync doesn't currently support CS messages, either. It would be up to Dave S and Jim to decide if they want to design it in, with changes to incorporate it with a 1204-02 Option Card.

IRIG CS-511z

The IRIG CS-511z is for use at baud rates  300 (see figure 1). It is a Time-of-Year format with 1-second resolution and frame length. The accuracy of this format at the receiver end is primarily dependent on the characteristics (fixed and variable transmission delays) of the communications circuits between the transmitting and receiving equipment. The ASCII expression for this format is


<SOH>I<SP>DDD<SP>HH:MM:SS<SP>#<CR><LF>

where

<SOH> = start of header (01₁₆)

I = identification character -- space (20₁₆) is default, any alpha or numeric ASCII character

<SP> = space (20₁₆)

 = the event count sign

DDD = the event count day

HH = the event count hour of the day

<:> = colon (3A₁₆)

MM = the event count minute of the hour

SS = the event count second of the minute

= the event count status -- space (20₁₆) is default, H (48₁₆) if

holding

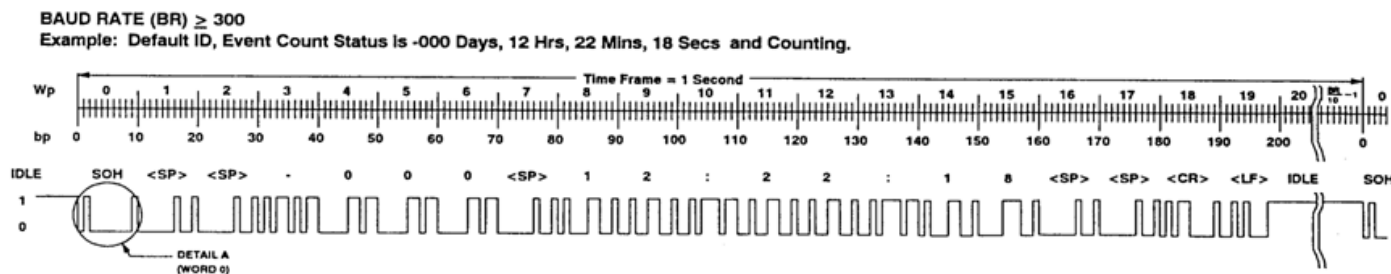
<CR> = carriage return (0D₁₆)

<LF> = line feed (0A₁₆)

The IRIG CS-511z uses the first 200 bits of the 1-second frame. The remaining bits are idle (logic level = 1) for the remainder of the frame. The frame length is 1 second, regardless of the baud rate.

The identification character is an ASCII 'space' character by default, although any alpha numeric ASCII character may be

used. The definition or function of the identification character is left to the user. Suggested uses might be identification of a net or network, an event, a test number, or a user number.



SMPTE time code

- Refer to “SMPTE” in the SecureSync customer assistance document.

**Stanag/HaveQuick input/output (for all products)

Refer to Spectracom Stanag/HaveQuick Tech Note:

<http://www.spectracomcorp.com/SearchResults/tabid/1551/Default.aspx/Default.aspx?q=stanag>

Havequick Message format

STANAG Principles

The main Time & Frequency STANAGs are:

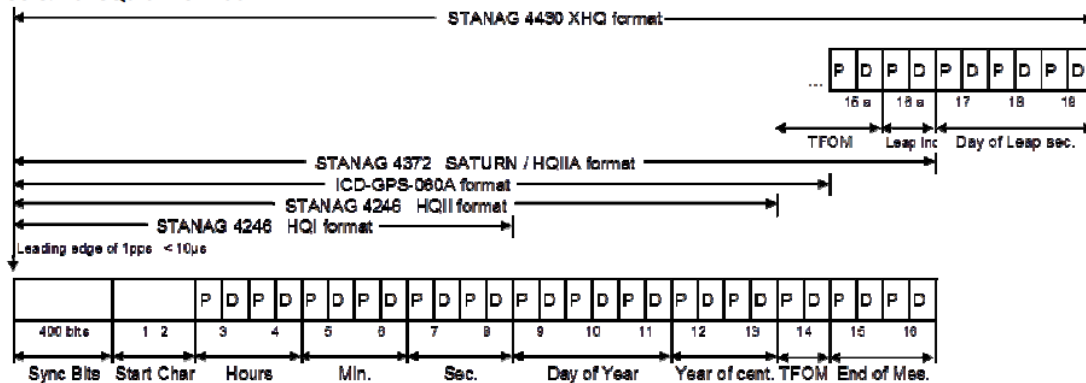
- **STANAG 4246** for HaveQuick UHF radio (second release)
- **STANAG 4372** for SATURN UHF radio,
- **ICD-GPS-060** timing interface for GPS User Equipment
- **STANAG 4430** interface for precise time and frequency transfer (generic)

Stanag/HaveQuick formats

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1																																
2																																
3																																
4																																
5																																
6																																
7																																
8																																
9																																
10																																
11																																
12																																
13																																
14																																
15																																
16																																
17																																
18																																
19																																
20																																
21																																
22																																
23																																
24																																
25																																
26																																
27																																
28																																
29																																
30																																
31																																

From our PDF document at the link above to our website

STANAG 4430 & HaveQuick Format



Time scale is UTC

Each character is one octet of Hamming code: 4 bits of parity preceding 4 bits of data except for specific Start character

Character	Meaning	Character	Meaning
1	Lead Ind. (00010001)	9	Day of Year 100's digit
2	Lead Ind. (11101001)	10	Day of Year 10's digit
3	Hours MSD	11	Day of Year 1's digit
4	Hours LSD	12	Year of century MSD
5	Minutes MSD	13	Year of century LSD
6	Minutes LSD	14	Time Figure of Merit, power of 10 ⁻¹⁰
7	Seconds MSD	15	End of Message
8	Second LSD	16	End of Message
15a	Time Figure of Merit, scale factor	17	Leap sec. Day of Year 100's digit
16a	Leap activity indicators	18	Leap sec. Day of Year 10's digit
		19	Leap sec. Day of Year 1's digit

Leap Second insertion

- From our PDF document, apparently the only Stanag/HaveQuick message to provide leap second pending notification is the Stanag 4430 XHQ format (provided by characters 17, 18 and 19 in the message).

Email Keith sent to Sylvain after discussing with Dave Sohn (5 Feb 2012) I just spoke to Dave Sohn for clarification about leap second processing when using Havequick input.

The processing of leap second insertion depends on whether SecureSync is receiving a Have quick or an extended have quick signal. Unlike the extended have quick signal, a havequick signal cannot alert to a pending leap second.

The extended havequick signal can provide the SecureSync with advanced notice (anytime/date of the current year for the leap second pending). If the SecureSync receives the notification of the pending leap second from the extended havequick source, SecureSync will latch the leap second in the Time Management page. Then, up to 30 days before the leap second occurs, NTP in the SecureSync will latch the Leap Indicator bits to inform the NTP clients that a leap second is scheduled to be inserted at the last second of the current month. It is then up to each NTP client on how it actually inserts the leap second (whither it be a one second jump, or more likely, it will insert it with a one second time slew).

If the SecureSync is not receiving an extended Have quick input (its instead receiving a standard Havequick signal), this input signal cannot provide advanced notification of a pending leap second. The Have quick signal is designed to insert a second of "60", at the very last second of the month of the pending leap second. The received "60" second's value will cause the SecureSync's System Time to jump one second. However, NTP will shortly thereafter start to slew itself to correct for the one second correction (NTP time won't jump one second). The NTP clients will continue to sync to the SecureSync's NTP output as its slewing to the new time, or any time thereafter. Then, the NTP clients will then likely slew their time to the new time from the SecureSync.

Second email Keith sent to Sylvain I was just looking at the Stanag/HaveQuick message formats. From the Stanag/HaveQuick document on the Spectracom website:

<http://www.spectracomcorp.com/SearchResults/tabid/1551/Default.aspx/Default.aspx?q=stanag> apparently the one specific Stanag/HaveQuick format that can provide advanced notification of a leap second pending is the STANAG 4430 XHQ message.

This particular message format has three extra characters at the end of the data stream, that the other Stanag formats don't contain. Characters 17, 18 and 19 provide the leap second pending information which allows SecureSync be aware that a leap second insertion

is pending.

So if your customer's HaveQuick source is providing the SecureSync with STANAG 4430 XHQ format messages, the SecureSync can be provided with advanced notification of a leap second pending. Otherwise, when using any other Stanag format for synchronization (and without any other types of inputs being available, such as GPS for instance), the SecureSync won't be able to detect that a leap second is pending. So the SecureSync and its outputs won't be able to provide any advanced notice to the devices its providing time to for their synchronization (such as the NTP time stamps won't be able to indicate a leap second pending), unless a user manually schedules the leap second to occur, via the **Setup- > Time Management** page of the browser.

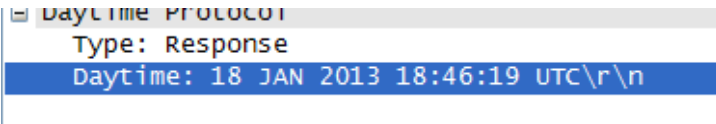
Daytime and Time protocols (for all products)

- We support both Daytime and Time protocols

Packet capture of daytime (TCP and UDP from NetClock and SecureSync)

- Refer to: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\DayTime- Time.protocol](#)

Daytime format (from the packet capture referenced above)



```
DayTime PROTOCOL
Type: Response
Daytime: 18 JAN 2013 18:46:19 UTC\r\n
```

DoW Mth DD HH:MM:SS [TZ] YYYY (Thu Aug 27 12:34:28 1998)

- **DoW:** Day of the week as a three-letter abbreviation for the English day of the week (i.e., Sun, Mon, Tue, Wed, Thu, Fri, Sat).
- **Mth:** Month as a three-letter abbreviation of the English month of the year (i.e., Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec).
- **DD:** Day of month as a two-digit day of the month.
- **HH:MM:SS:** The next eight values give the local time hour, minute and second separated with a colon (:).
- **TZ:** Optional three or four-letter abbreviation for the local time zone. (i.e., CDST, CEST). ClockWatch does not use this field. Use the difference in hours field on the server option form to correct for a time server in a different time zone.
- **YYYY:** The current four-digit year.

****Time protocol**

- The **time** protocol is defined in **RFC-868** (<http://tools.ietf.org/html/rfc868>)
- Per the RFC, there is a UDP version and a TCP version of the Time protocol.
- Time protocol uses **port 37**
- Time protocol responds with a Binary time stamp (not readable ASCII time stamp)
- The time stamp returned is the number of seconds since 00:00 (midnight) 1 January 1900GMT, such that the time 1 is 12:00:01 am on 1 January 1900 GMT; this base will serve until the year 2036M
- Make sure the Time Protocol is enabled in Services if its desired to use it (disabled by default)

****Daytime protocol**

- The **Daytime** protocol is defined in **RFC-867** (<http://tools.ietf.org/html/rfc867>)
 - Make sure the daytime Protocol is enabled in Services if its desired to use it (disabled by default)
 - Daytime uses network port **13**
 - Daytime responds with an ASCII time stamps
 - Per the RFC, there is a UDP version and a TCP version of Daytime.
 - We apparently support only the TCP version (not the UDP version)
- (18 Jan 2012) From a customer or Spectracom UK- I have making some probes and my conclusion is that your NetClock hasn't response of Daytime Protocol in UDP. I have probed with DayTime Protocol in TCP and we have response.

Timescale for Time/Daytime timestamps (such as UTC versus local time)

- There is no ability to apply a user-configured "**local clock**" to Time/Daytime time stamps, to have the timestamps outputted as local time.
- The Time/Daytime timestamps are outputted in the same timescale as the "**System timescale**" is configured as (**Management -> Time Management** page of the browser)
- In at least versions 5.7.1 and below, System timescale is limited to just **UTC**, **GPS** and **TAI** ("**Local**" is not an available System timescale)
- So **local** timescale output is not possible unless our Engineering team adds "local" timescale as a selection for the System timescale in a future update. Then the System will be in Local time, and Time/DayTime would simply follow along.

**Interface with daytime/time protocols

Email from Dave Sohn (10 Apr 2013) You can use any telnet utility that can be set to query the daytime port. I used windows telnet and teraterm during my testing.

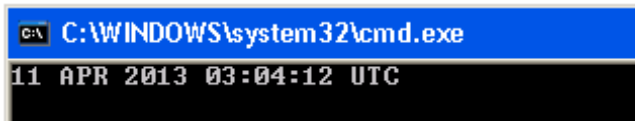
Notes

- Make sure Telnet port (**TCP port 13**) is open on any firewalls.
- Make sure DayTime protocol is enabled in the time server (**Management -> Network** settings page of the browser)
- Time protocol responds with a binary time stamp, so the methods below won't work with Time protocol- just with the Daytime protocol

A) Obtaining Daytime timestamp using Windows telnet (if telnet is enabled)

Daytime protocol: In a command prompt, enter: **telnet xxx.xxx.xxx.xxx 13** <enter> (where 13 is the daytime port number). One daytime UTC* time stamp will be returned

* Unless the System Timescale is configured as either GPS or TAI, in which case the timestamp will be in this timescale instead



B) Obtaining daytime timestamp using Tera Term (in telnet mode)

G) Setup -> TCP/IP

H) Host List: enter the IP address of your NTP server.

I) Uncheck "auto window close" (Keep "Telnet" selected). Click OK

J) File -> New Connection

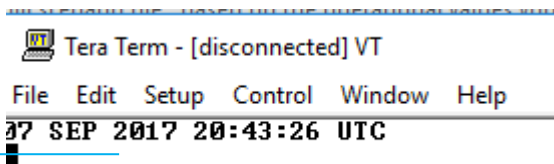
K) Service: Select Telnet

L) TCP port: Change to 13 (for Daytime time stamp) OR 37

M) Protocol: IPv4

N) Click OK. One UTC* time stamp will be returned.

* Unless the System Timescale is configured as either GPS or TAI, in which case the timestamp will be in this timescale instead



Chrony/chronyd (Crony) (replacement to NTP)

- Refer especially to: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/sect-understanding_chrony_and-its_configuration
- or other sites such as:

- <https://chrony.tuxfamily.org/> and http://docs.fedoraproject.org/en-US/Fedora/18/html/System_Administrators_Guide/chap-Configuring_NTP_Using_the_chrony_Suite.html
- Chrony is apparently replacing NTP (per http://docs.fedoraproject.org/en-US/Fedora/18/html/System_Administrators_Guide/chap-Configuring_NTP_Using_the_chrony_Suite.html) "chrony is a pair of programs for maintaining the accuracy of computer clocks. **chronyd** is a background daemon program that can be started at boot time.

chrony is a versatile implementation of the Network Time Protocol (NTP). It can synchronize the system clock with NTP servers, reference clocks (e.g. GPS receiver), and manual input using wristwatch and keyboard. It can also operate as an NTPv4 (RFC 5905) server and peer to provide a time service to other computers in the network.

It is designed to perform well in a wide range of conditions, including intermittent network connections, heavily congested networks, changing temperatures (ordinary computer clocks are sensitive to temperature), and systems that do not run continuously, or run on a virtual machine.

Typical accuracy between two machines synchronized over the Internet is within a few milliseconds; on a LAN, accuracy is typically in tens of microseconds. With hardware timestamping, or a hardware reference clock, sub-microsecond accuracy may be possible.

Two programs are included in chrony, chronyd is a daemon that can be started at boot time and chronyc is a command-line interface program which can be used to monitor chronyd's performance and to change various operating parameters whilst it is running.

License

- `chrony` is distributed under the GNU General Public License version 2.

Q Email Keith sent to Tim Tetreault (8 Oct 14) Jeremy Thomas has a TSync-PCIe customer desiring to sync a Fedora 16 machine using the timing board. Fedora 16 has a kernel version of 3.1.0.

The customer is saying NTP has been replaced by chronyd (Chrony suite).\ The following site: http://docs.fedoraproject.org/en-US/Fedora/18/html/System_Administrators_Guide/chap-Configuring_NTP_Using_the_chrony_Suite.html has info on Chrony. It appears Chrony takes the place of NTP.

From this site, I believe here is where the issue is:

Things `ntpd` can do that `chronyd` cannot do:

- `ntpd` fully supports NTP version 4 (*RFC5905*), including broadcast, multicast, manycast clients and servers, and the orphan mode. It also supports extra authentication schemes based on public-key cryptography (*RFC5906*). `chronyd` uses NTP version 3 (*RFC1305*), which is compatible with version 4.
- `ntpd` **includes drivers for many reference clocks whereas `chronyd` relies on other programs, for example `gpsd`, to access the data from the reference clocks.**

It looks like he could use a standard network time server with this machine. But will he be able to use a TSync board. Can he install `ntpd` in addition to Chrony?

Note: Link to "refclock_tsyncpci.c" file referenced in email below: [I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\Timing boards\TSync family\chrony-chronyd \(replacing NTP\)](I:\Customer Service\EQUIPMENT\SPECTRACOM\EQUIPMENT\Timing boards\TSync family\chrony-chronyd (replacing NTP))

A (reply from Keith, 9 Oct 14) I was talking with Tim T yesterday evening regarding your "Chrony" customer (Steve Klassen). I have some information for you to pass along to him, if you like.

To begin, in order for Chrony to be able to sync to an installed TSync-PCIe board, they will need to create a custom "reference clock driver" that tells Chrony how to use the timing board as an input reference. This is the same function we needed to create for NTP to use our timing board as a reference.

Attached you should find the source code from the TSync linux driver that is used to create the NTP reference clock driver. Your customer can use this code as an example of what needs to be done in Chrony to create the reference clock driver in order for the TSync board to be used as an internal time reference.

Compatibility of a Chrony client with a standard NTP time server

Email from Paul Myers (27 Feb 17) The SecureSync runs the NTP daemon standard implementation with the current release being 4.2.8p9 in Release 5.5.1

We do NOT run chrony on the SecureSync, however, a chrony client should be compatible. See the section 1.1 overview of manual which indicates it can support NTPv4 (RFC 5905)

<https://chrony.tuxfamily.org/comparison.html>

<https://chrony.tuxfamily.org/manual.html>

Time sources

	chrony	ntp	openntpd
NTP	Yes	Yes	Yes
Reference clocks	Yes	Yes	Yes
Manual input	Yes	No	No

Another example indicating how a Chrony client can sync to an NTP server is via Section 2: Installation of Chrony of the Chrony manual at” <https://chrony.tuxfamily.org/manual.html#Installation>

Now that the software is successfully installed, the next step is to set up a configuration file. The default location of the file is ‘/etc/chrony.conf’. Several examples of configuration with comments are included in the examples directory. Suppose you want to use public NTP servers from the pool.ntp.org project as your time reference. A minimal useful configuration file could be

```
pool pool.ntp.org iburst
makestep 1.0 3
rtcsync
```

NTP (for all products)

Good NTP documentation

- “NTP Architecture, Protocol and Algorithms”:
<https://www.eecis.udel.edu/~mills/database/brief/arch/arch.pdf>
- Good docs for definition of terms associated with NTP:
 - <http://support.ntp.org/bin/view/Support/NTPRelatedDefinitions>
 - “A Glossary of NTP-speak”: <https://docs.ntpsec.org/latest/ntpsspeak.html>

NTP versions/NTP version in gentoo package

Current version of NTP: <http://www.ntp.org/downloads.html>

- NTP version in linux Gentoo package: refer to <http://gentoobrowse.randomdan.homeip.net/package/net-misc/ntp>

NTP Best practices document (Written by Denis Reilly)

- Here is a link to the “IETF Best Practices draft for NTP”: <https://datatracker.ietf.org/doc/draft-ietf-ntp-bcp/>

RFC 8915: Network Time Security (NTS) for the Network Time Protocol (NTP)

- RFC for NTS officially Released ~Oct 2020
 - Refer to <https://tools.ietf.org/html/rfc8915>

“This memo specifies Network Time Security (NTS), a mechanism for using Transport Layer Security (TLS) and Authenticated Encryption with Associated Data (AEAD) to provide cryptographic security for the client-server mode of the Network Time Protocol (NTP).

NTS is structured as a suite of two loosely coupled sub-protocols. The first (NTS Key Establishment (NTS-KE)) handles initial authentication and key establishment over TLS. The second (NTS Extension Fields for NTPv4) handles encryption and authentication during NTP time synchronization via extension fields in the NTP packets, and holds all required state only on the client via opaque cookies.

Additional info

- Refer to sites such as: <https://blog.apnic.net/2019/11/08/network-time-security-new-ntp-authentication-mechanism/>
https://datatracker.ietf.org/doc/rfc8915/?include_text=1

Current Status (as of Nov 2020)

- Refer to Salesforce Case 252350

Q Email from Keith (13 Nov 2020) to Emmanuel/Apps I just received a call from Preston Cleary with Franchise Tax Board (California), inquiring about the new **RFC 8915: Network Time Security for the Network Time Protocol (NTS)** as it pertains to their SecureSyncs (1200s in his case).

I see the specs are now “official” (as of October), but couldn’t find any info on when its expected to be available in NTP. Once its available, will this just be integrated into SecureSyncs (1200 and 2400s) via a standard software upgrade to the NTP

package? Will it be available for all 1200/2400 customers, as a “feature update”, or will it be limited to just the 2400s/purchased update? Etc. I told Preston I would “ask around” to see about getting additional info to share with him.

A Reply from Emmanuel (16 Nov 2020) We’re working on it, as this has been identified as a key security consideration.

Our current plan is to introduce NTS on 2400 (it requires to migrate the NTP implementation from NTPd to Chrony) as part of the 1.5 release (expected Q3 2021).

Then we’ll do our best to port this implementation also on 1200 (this should be facilitated by the 1200/2400 platform convergence), and we will target to have it implemented on 1200 by end of next year.

****NTPSec (more secure NTPd)**

- Refer to: <https://www.ntpsec.org/>
- Intended replacement to NTPd)
- “NTPsec project - a secure, hardened, and improved implementation of Network Time Protocol derived from NTP Classic, Dave Mills’s original”

Q. Are you working with the folks respawning ntpd as ntpsec? <https://www.ntpsec.org>.

A. reply from Dave Sohn (22 Dec) to Tony Diflorio We are aware of the effort of ntpsec, and are monitoring their efforts within the working groups and community. We are not directly involved in those efforts. When they have something more viable we will probably look at it as a potential path for our NTP integration, but it is still early for now.

****NTP Vulnerabilities**

- Refer to <http://support.ntp.org/bin/view/Main/SecurityNotice>
- In this document, refer also to: [**CVE's/Potential Vulnerabilities \(All network appliances\)](#)

****W32Time (Windows Time Service)**

- Refer to: [Software\Windows 2000-2003\Synchronizing Windows computers.pdf](#)

A) (newer versions of Windows (Windows Server 2012/2008, Windows 10 and later)

good websites for info about w32time in newer versions of Windows

<https://docs.microsoft.com/en-us/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings#hkmsystemcurrentcontrolsetservicesw32timeconfig>

B) Earlier versions of Windows (such as 2003/2000/XP)

Default Minpoll/maxpoll intervals (Windows 2003 and higher. XP SP2 and higher)

- (Reference <http://www.scribd.com/doc/80624879/36/>)

Minpoll interval

- The default value for domain controllers is 6 (**1 min 4 sec**)
- The default value for domain members is 10 (**17 min 4 sec**)
- The default value for stand-alone clients and servers is 10 (**17 min 4 sec**)

MaxPoll interval

- The default value for domain controllers is 10 (17 min 4 sec)
- The default value for domain members is 15 (9 hr 6 min 8 sec)
- The default value for stand-alone clients and servers is 15 (**9 hr, 6 min 8 sec**)

Based on these two values (we don't recommend or support changing them to other values)

- Domain controllers will poll no less than every 17 minutes
- Workstations will poll no less than every 9 hours

Syncing Virtual Machines/VMs (such as VMware/ESX and ESXi, Hyper-V)

- VMs inherently have degraded timing accuracies
- Refer to sites such as:

https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1006427

https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1005092

<https://kb.vmware.com/s/article/1318>

Email from Ron Dries (8 Aug 2018) I found this article from VMware about time synchronization: <https://kb.vmware.com/s/article/1318>

I would still recommend they try to utilize the TSync Time Provider in server 2016 as Microsoft has made many improvements with time synchronization in Windows 10 and Windows Server 2016. Also I would recommend taking a look at the VMware recommendations for time synchronization.

Using TSync boards/TSync drivers in Virtual Machines/VMs/Virtual environments

- Refer also to "Using TSync in Virtual Machines/VMs/Virtual environments" in: <..\TimingBoardCustAssist.pdf>

TSync Time Provider for Windows

- However in Windows server 2016 the customer can take advantage of the TSync Time Provider included with the 64 bit version of the driver.
- This is described in the release notes: <https://spectracom.com/sites/default/files/document-files/TSync%20Release%20Notes%20for%203.2.1%20Windows%20Driver.pdf>
- Here is some information on time providers from Microsoft: <https://docs.microsoft.com/en-us/windows-server/networking/windows-time-service/accurate-time>

Q Sent to Ron Driers Regarding SF case **171013**, (for Northrop Grumman) I just want to confirm my intended response for this TSync-PCIe inquiry. I'm fairly certain I have the correct info to respond with, but just want to make sure before I send it. Below in red is the inquiry initially sent to Steve Visosky and forwarded to us:

Steve,

Willie gave me your contact information related to the TSync card we're using on a program (same one he asked about).

We have the card installed in an HPE server running VMWare ESXi, and then passed up to a virtual machine running Windows Server 2016.

We have installed the Tsync software, and the utility says it is synchronized. Also verified that the clock daemon service is running.

However, the actual clock on that VM appears to be several milliseconds (3-9ms) off from the IRIG time source that the Tsync card is connected to.

I'm hoping to get some guidance on how the TSync card and software work with Windows Server 2016, and if there are any documents/guides on configurations of the Tsync product to allow the Windows server to act as a time server (I have it configured per Microsoft guidance, but since the clock appears to be off from other sources, we're being generally marked as a false ticker).

My understanding is that Time synchronization in a virtual environment is inherently poor with lower accuracies/more jitter. And so, the time offsets being observed while syncing to the TSync board (3-4 milliseconds) doesn't sound the least bit unexpected.

With other servers also configured (in addition to the TSync board) it's highly likely those other servers have lower offsets (especially if they are only a couple/few hops away), inherently resulting in the TSync board being classified

a false ticker.

My recommendation, if they are looking for timing accuracies, is to use a true Windows (or Linux) machine and not a virtual machine to be an NTP server.

As for making Windows be treated as a true NTP server (beyond local NTP being able to sync just Windows clients), the only way I know of doing this is to install Meinberg's port of NTP for Windows. I don't like to advertise this program's availability, because it has their name all over it ☹!!

Are there any other ways (for Windows) besides Meinberg's NTP port??

A Reply from Ron Dries (7 Aug 2018) You are correct that the virtual environment can have a negative impact on the timing accuracy.

However in Windows server 2016 the customer can take advantage of the TSync Time Provider included with the 64 bit version of the driver.

This is described in the release notes: <https://spectracom.com/sites/default/files/document-files/TSync%20Release%20Notes%20for%203.2.1%20Windows%20Driver.pdf>

Here is some information on time providers from Microsoft: <https://docs.microsoft.com/en-us/windows-server/networking/windows-time-service/accurate-time>

Inherent issues with NTP Stability in VMs

- Not at all unexpected for VMs running ntpd to have NTP log entries(var/log) indicating errors of greater than 500PPM ("**frequency error -512 PPM exceeds tolerance 500 PPM**")

Recommended solutions:

1. Recommendation to use -q and -g switch when starting NTP

- Refer to <https://access.redhat.com/solutions/35640>

-g

Normally, ntpd exits if the offset exceeds the sanity limit, which is 1000 s by default. If the sanity limit is set to zero, no sanity checking is performed, and any offset is acceptable. This option overrides the limit and allows the time to be set to any value without restriction; however, this can happen only once. After that, ntpd will exit if the limit is exceeded.

-q

Exit the ntpd just after the first time the clock is set. This behavior mimics that of the ntpdate program, which is to be retired. The -g and -x options can be used with this option.

2. Recommendation to add "Tinker panic 0" to the TOP of the ntp.conf file of VM clients

- Refer to: https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1006427
- **Tinker panic 0** instructs NTP to not give up if it sees a large jump in time. This is important for coping with large time drifts and also resuming virtual machines from their suspended state.
 - **Note:** The `tinker panic 0` directive must be at the top of the `ntp.conf` file.

**Windows Hyper-V (ESXI hypervisor) and W32Time (Windows Time Service)

- Refer to Salesforce case **21763**
- “Hyper-V” (Hyper V) appears to be a virtual machine that only grabs time when it first opens and then drifts from there??? The time can be way off!
- Dave Lorah sent the standard Windows Time Service document along with the following

Here also is a link to an interesting article that may prove useful.

<http://mikefrobbins.com/2010/05/17/active-directory-and-server-time-synchronization-problems-with-hyper-v/>

***Report the time offset between a Windows PC and an NTP server

- Search for “stripchart” in knowledge base articles or link below:

https://na8.salesforce.com/articles/FAQ/Reporting-the-time-offset-between-a-Windows-PC-and-NTP-server?popup=false&navBack=H4slAAAAAAAAAuuVipVslSjy_N1M_Oyy_PSU1JT9UHcrxhHI_83FT74tTEouQM2-KS0syC5IzEohlHaVioD4UUVUCxbKBYQWJ6akhmSU6qUm0sAG3TarpfAAAA

full article pasted below:

Reporting the time offset between a Windows PC and NTP server

[Show Feed](#) [Follow](#) [Rate This Article](#) (Average Rating: No Rating) [Version 1](#) [Show Properties](#)

[Back to Knowledge Search](#)

Information

Question

How closely synced is my Windows PC to an NTP server?

Answer

Windows w32tm has a utility called “stripchart” which can provide periodic (such as every two seconds by default) reports of the time offset between a Windows PC and an NTP server on the network. This can be the NTP server that it normally syncs with, or any other NTP server on the network.

Below is an example of Windows stripchart comparing a Windows PC to an NTP server (with an IP address of 10.2.100.19).

```
H:\>w32tm /stripchart /computer:10.2.100.19
Tracking 10.2.100.19 [10.2.100.19].
The current time is 12/11/2013 5:32:23 PM (local time).
17:32:23 d:-00.0002167s o:-182.7822279s [E
]
17:32:25 d:-00.0001440s o:-182.7819402s [E
]
17:32:27 d:-00.0002245s o:-182.7812289s [E
]
17:32:29 d:-00.0001228s o:-182.7960008s [E
]
17:32:31 d:-00.0001730s o:-182.7949734s [E
]
^C
```

In this example above, there is currently a 182.79 second time difference (the “o” value) between this Windows PC and the selected NTP server. The time difference reports continue to occur every two seconds.

To use stripchart, open a Windows Command Prompt window on the PC you wish to compare to an NTP server. Type `w32tm /stripchart /computer:xxx.xxx.xxx.xxx` (where xxx.xxx.xxx.xxx is the IP address or hostname of the NTP server you wish to compare this PC against).

Below are switches that can also be used in the stripchart command, as desired:

<code>w32tm /stripchart</code> <code>/computer:<target></code> <code>[/period:<refresh>]</code> <code>[/dataonly]</code> <code>[/samples:<count>]</code> <code>[/packetinfo]</code> <code>[/protocol:<4 6>]</code>	Displays a strip chart of the offset between this computer and another computer. computer:<target> —The computer to measure the offset against. period:<refresh> —The time between samples, in seconds. The default value is 2 seconds. Dataonly —Display only the data, without graphics. samples:<count> —Collect <count> samples; then, stop. If a value is not specified, samples will be collected until the user types Ctrl-C is pressed. packetinfo —Print out NTP packet response message. lpprotocol —Specify the IP protocol to use. The default is to use whatever is available.
--	--

to stop the stripchart reports, press **Ctrl+C** (or close the command prompt window).

This information was obtained from the website: <http://technet.microsoft.com/en-us/library/w32tm.aspx>

Internal Comments

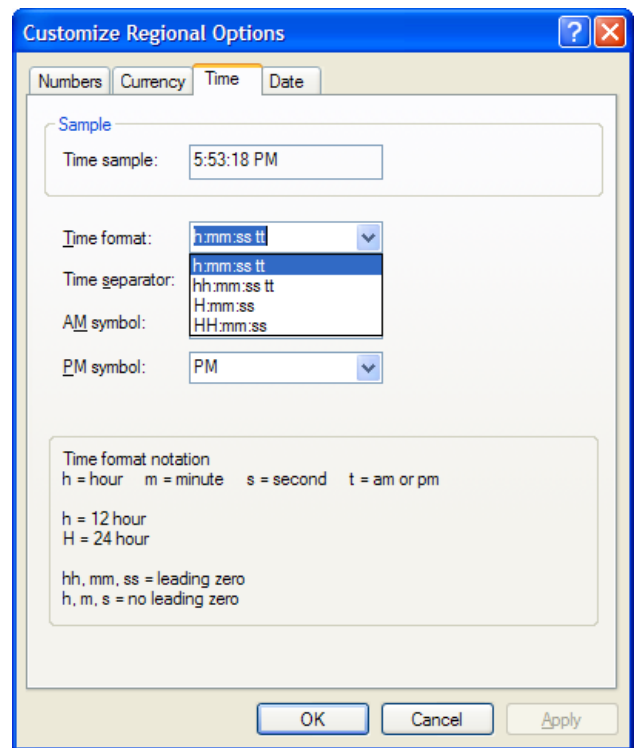
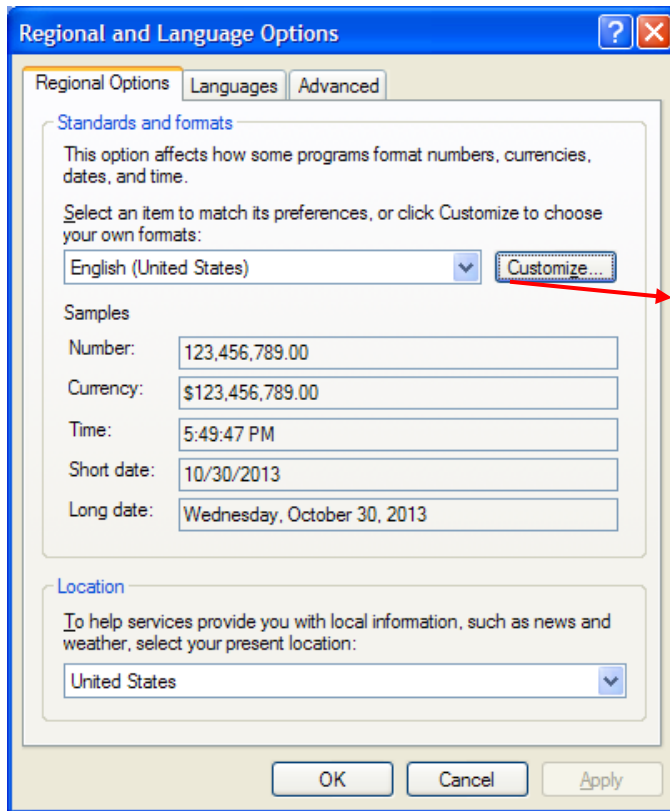
Related Attachment

Page | 549

****Change the desired Windows Time Format display from 12 hour to 24 hour**

To change the time display on a Windows PC from 12 hour to 24 hour mode:

1. Go to Control Panel to “Regional and Language options”.
2. Click on the “Customize” button and then click on the “Time” tab.



Desire to very accurately synchronize Windows

1) use a TSync series timing board installed in the PC

- Refer also to “Syncing Windows using a TSync Timing board” section of: [..\TimingBoardCustAssist.pdf](#)
- Refer to Salesforce case 12724 (Matt Windholtz)
- Limitation is we haven’t created a client that is intended to sync Windows very accurately (clock daemon can sync the Windows PC to a timing board, but accuracy is around 3-4 ms).

Email John Fischer sent to Matt Windholtz (16 Dec 2013)

My colleagues here have asked me to contact you regarding your precise timing requirements running under the Windows Server OS.

Since I had also worked with the folks at General Dynamics on this same project a few months ago, they thought it would be better for me to contact you directly.

As you know, our TimeKeeper software operates only under Linux and it appears it will be prohibitively expensive for this to be re-hosted to Windows.

I understand that for IA reasons, the OS must be Windows Server.

One alternative solution yet to be explored is whether Windows Server 2013 could be used. (We understand that the approved OS for this project is Server 2008). It is our belief that Server 2013 may have a sufficient timekeeping function built in which we could use for this application.

However, before we do an in-depth investigation on the suitability of Windows Server 2013, we first need to know if this would be a viable alternative for you. Is there a plan to eventually upgrade to Server 2013? Is it an IA approved OS?

I look forward to working with you on this project...

****Troubleshooting Linux box not syncing to NTP server (using CLI commands)**

*****errno error messages**

errno (such as “**errno = 22**” for example)

Refer to the following website for a list of errno numbers and what they mean: http://www-numi.fnal.gov/offline_software/srt_public_context/WebDocs/Errors/unix_system_errors.html

For example:“(**errno = 22**)” means “Invalid argument”

*****Using the ntpdate command**

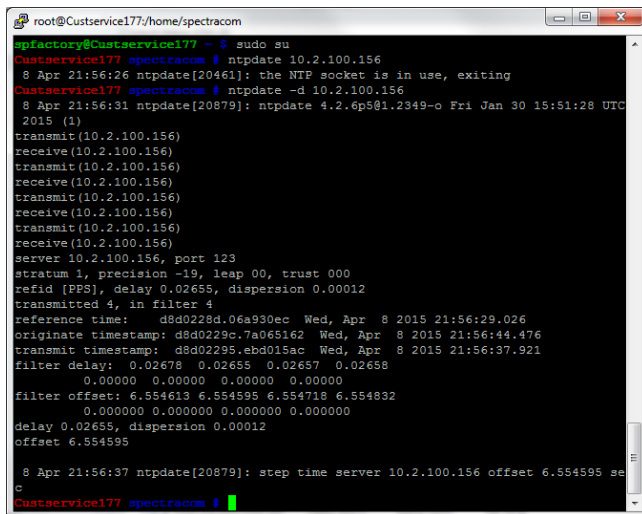
Refer to sites such as http://www-01.ibm.com/support/knowledgecenter/ssw_aix_61/com.ibm.aix.cmds4/ntpdate.htm

Note: Customers don't have permission to be able to use a SecureSync to perform this test. But they may on their linux machine.

On a linux box, use the ntpdate command in debug mode (**ntpdate -d xxx.xxx.xxx.xxx**) to verify info in NTP packet. Using

Reports info such as Stratum, delay, offset, refid, etc.

Internal use only: When using one of our SecureSyncs to perform this command, have to be logged in as root (not just spadmin or spfactory).



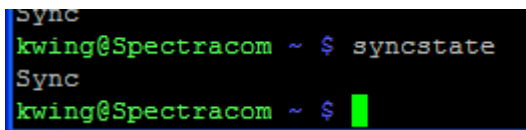
```
root@Custservice177:/home/spectracom
spfactory@Custservice177 ~ $ sudo su
Custservice177 spectracom # ntpdate 10.2.100.156
8 Apr 21:56:26 ntpdate[20461]: the NTP socket is in use, exiting
Custservice177 spectracom # ntpdate -d 10.2.100.156
8 Apr 21:56:31 ntpdate[20879]: ntpdate 4.2.6p5$1.2349-o Fri Jan 30 15:51:28 UTC
2015 (1)
transmit(10.2.100.156)
receive(10.2.100.156)
transmit(10.2.100.156)
receive(10.2.100.156)
transmit(10.2.100.156)
receive(10.2.100.156)
transmit(10.2.100.156)
receive(10.2.100.156)
transmit(10.2.100.156)
receive(10.2.100.156)
server 10.2.100.156, port 123
stratum 1, precision -19, leap 00, trust 000
refid [PPS], delay 0.02655, dispersion 0.00012
transmitted 4, in filter 4
reference time: d8d0228d.06a930ec Wed, Apr 8 2015 21:56:29.026
originate timestamp: d8d0229c.7a065162 Wed, Apr 8 2015 21:56:44.476
transmit timestamp: d8d02295.ebd015ac Wed, Apr 8 2015 21:56:37.921
filter delay: 0.02678 0.02655 0.02657 0.02658
0.00000 0.00000 0.00000 0.00000
filter offset: 6.554613 6.554595 6.554718 6.554832
0.000000 0.000000 0.000000 0.000000
delay 0.02655, dispersion 0.00012
offset 6.554595
8 Apr 21:56:37 ntpdate[20879]: step time server 10.2.100.156 offset 6.554595 se
c
Custservice177 spectracom #
```

1. Verify the sync state and Stratum level of the NTP server.

Telnet/SSH into CLI interface.

Perform a **syncstate** command

Reports Sync status as **Sync**, **Holdover** or **Free Run**)



```
kwling@Spectracom ~ $ syncstate
Sync
kwling@Spectracom ~ $
```

Perform a **status** command (note it takes about 5 seconds to respond).

(Reports selected references, NTP status, TFOM value)


```
kwing@Spectracom ~ $ status
REF:T=gps0 P=gps0
NTP:Strat=1 Sync=Y
OSC:OCXO (Trk/Lock)
TFOM=1 MaxTFOM=15
```

2. Review the NTP log of the NTP server.

```
kwing@Spectracom ~ $ cd log
kwing@Spectracom ~/log $ cat ntp.log
Mar 16:02:57 ntpd[16414]: 10.2.100.89 interface 10.2.100.176 -> (none)
Mar 16:02:58 ntpd[16414]: 10.2.100.89 interface 10.2.100.176 -> (none)
Mar 16:03:04 ntpd[16414]: 10.2.100.89 interface 10.2.100.176 -> (none)
Mar 16:03:09 ntpd[16414]: 10.2.100.89 interface 10.2.100.176 -> (none)
Mar 16:03:10 ntpd[16414]: 10.2.100.89 interface 10.2.100.176 -> (none)
Mar 16:03:17 ntpd[16414]: 10.2.100.89 interface 10.2.100.176 -> (none)
Mar 16:03:21 ntpd[16414]: 10.2.100.89 interface 10.2.100.176 -> (none)
Mar 16:03:26 ntpd[16414]: 10.2.100.89 interface 10.2.100.176 -> (none)
Mar 16:03:32 ntpd[16414]: 10.2.100.89 interface 10.2.100.176 -> (none)
```

3. Is the box running A) Timekeeper software or B) NTP software?

A) Linux box running Timekeeper?

Review the timekeeper logs (example entries from Morgan Stanley below)

Below shows our server losing time sync:

[velocity191.vhub.east.ms.com /var/user/changd17](https://velocity191.vhub.east.ms.com/var/user/changd17) \$ tail -f /var/log/timekeeper

1394058239.870878567: TimeKeeper alert at 1394058239.870858683: Time source change
NTP(10.251.26.105:127.127.22.0) -> NTP(10.251.26.105:10.251.10.15)

1394058253.630278811: TimeKeeper alert at 1394058253.630264464: Time source change
NTP(10.251.26.105:10.251.10.15) -> NTP(10.251.26.105:127.127.22.0)

1394058311.897257097: TimeKeeper alert at 1394058311.897242742: Time source change
NTP(10.251.26.105:127.127.22.0) -> NTP(10.251.26.105:10.251.10.15)

1394058326.916639051: TimeKeeper alert at 1394058326.916623421: Time source change
NTP(10.251.26.105:10.251.10.15) -> NTP(10.251.26.105:127.127.22.0)

1394061979.962625871: TimeKeeper alert at 1394061979.962610960: Time source change
NTP(10.251.26.105:127.127.22.0) -> NTP(10.251.26.105:10.251.10.15)

1394062109.758766591: TimeKeeper alert at 1394062109.758750993: Time source change
NTP(10.251.26.105:10.251.10.15) -> NTP(10.251.26.105:127.127.22.0)

1394062121.096135674: TimeKeeper alert at 1394062121.096120396: Time source change
NTP(10.251.26.105:127.127.22.0) -> NTP(10.251.26.105:10.251.10.15)

1394062134.985572750: TimeKeeper alert at 1394062134.985551815: Time source change
NTP(10.251.26.105:10.251.10.15) -> NTP(10.251.26.105:127.127.22.0)

B) Linux box running NTP?

1. With a CLI connection (telnet or SSH) into the SecureSync, try pinging your server. If it doesn't respond to a ping, there is a network issue likely occurring.

Note: use <CTRL> C to stop the ping command

```
kwing@Spectracom ~ $  
kwing@Spectracom ~ $ ping 10.2.100.71  
PING 10.2.100.71 (10.2.100.71) 56(84) bytes of data.  
From 10.2.100.73: icmp_seq=1 Destination Host Unreachable  
From 10.2.100.73: icmp_seq=2 Destination Host Unreachable  
From 10.2.100.73: icmp_seq=3 Destination Host Unreachable  
From 10.2.100.73: icmp_seq=4 Destination Host Unreachable  
From 10.2.100.73: icmp_seq=5 Destination Host Unreachable
```

2. Has there been any large changes applied to the linux box while NTP was running (greater than the panic level of 1000 seconds)? If there has, need to either manually bring the Linux box's time closer to the time sever, or restart NTP on the Linux box, using the "no limit on startup" switch ("-g").
3. Perform an `ntpq -p` or `ntpq -pn` command on the linux box (example of each shown below)

C) Note: use the "watch" command described below to have NTPQ update automatically

watch: refresh one or more displayed items such as tables

Note: CTRL C to exit

one item :

watch -n 0.1 ntpq -p (where 0.1 is the refresh rate in seconds)

```
spadmin@Spectracom ~ $ watch -n 0.1 ntpq -p
```

```
kwing@Spectracom ~ $ ntpq -p  
remote          refid          st t when poll reach  delay  offset  jitter  
-----  
*PCI_TSYNC(0)   .GPS.          0 1   4   16  377   0.000   0.043   0.002  
oPPS(0)         .PPS.          0 1   3   16  377   0.000  -0.004   0.007  
+10.2.100.93    .GPS.          1 u   2    8  377   0.290  -0.020   0.070  
kwing@Spectracom ~ $ ntpq -pn  
remote          refid          st t when poll reach  delay  offset  jitter  
-----  
*127.127.45.0   .GPS.          0 1  13   16  377   0.000   0.043   0.002  
o127.127.22.0   .PPS.          0 1  12   16  377   0.000   0.009   0.014  
+10.2.100.93    .GPS.          1 u   3    8  377   0.229   0.013   0.097  
kwing@Spectracom ~ $
```

- Make sure the IP Address /hostname of the time server is listed in the response
- Make sure reach value of the time server is "377". If Reach is less than "377", NTP on your server is not always getting time stamps from the SecureSync. A Reach value of "0" indicates the last 8 times the server polled the SecureSync for its time, it was not able to get a response back. We want the Reach to always be "377" except when NTP is first starting up.
- See if the NTP Tally Code at the beginning of each peer shows NTP has selected the time server (asterisk is the selected time reference and the "o" is the selected PPS for the atom clock driver).
- **Sync ("Tally Code"):** a symbol that indicates if the listed reference is available for selection as a reference.
 - Refer to (in this doc): [**NTP Status Symbols \(Tally Codes\)](#)

1) Perform an `ntpd -c sysinfo` command

- Refer to in this document, the following section for more info on this command: [Ntpdc -> Sysinfo command](#)


```

cat: /var/log/ntp.log: No such file or directory
kwing@Spectracom ~ $ ntpdc -c sysinfo
system peer:      PPS(0)
system peer mode: client
leap indicator:    00
stratum:          1
precision:        -19
root distance:     0.00000 s
root dispersion:   0.00046 s
reference ID:      [PPS]
reference time:    d6c318cc.a061ef85 Thu, Mar  6 2014 15:54:52.626
system flags:      auth monitor ntp kernel stats
jitter:            0.000000 s
stability:         0.000 ppm
broadcastdelay:    0.000000 s
authdelay:         0.000028 s
kwing@Spectracom ~ $

```

****NTP Stress Test / Stress test results**

For SecureSync, refer to: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP stress testing](#)

For NetClock 9200/9300 series, refer to: [EQUIPMENT\SPECTRACOM EQUIPMENT\9283-9288-9289-9383-9389-9388\NTP\NTP stress testing](#)

NetClock 9100/TTS series: TTSxxx and 9100 series time servers have never been NTP stress tested

Link to the NTP stress tool: [\\eng-server\public\Tool\NTPStressTool](#) (see important note below from Paul Myers - **do not** send this program to anyone, without an NDA agreement)

Email from Paul Myers to Dave Lorah (17 Jan 2013) Engineering does not send intellectual property outside of Spectracom without direct management authorization.

If Basingstoke is going to perform the testing and keep it within the Spectracom family this is not an issue. They need to be made aware of that.

Please have David Sohn or Bill Glase approve.

We have authorized its temporary use too Bell Alliant (?) I recall with an NDA in place placing terms and conditions on its use, and requirements that it NOT be distributed and all tests results shared with Spectracom. Will Hickey can provide you with information on the NDA used.

Sam Otto created a technical note for using the NTP Stress Tool to verify performance.

The tool has NOT been given to customers because we do NOT support it outside of Spectracom Rochester.

I can provide the location of the tool for reference. The executable is named NTPStress.exe. However it was built for Windows XP and may not run on all Windows Operating systems. Furthermore, we do NOT distribute the source code. The tool can be found here, I do NOT recall where customer service has Sam's Documentation you will also need.

**NTP packets

Reference, Originate, Receive and Transmit (T1, T2, T3, T4) timestamps

- **Reference timestamp:** Time/date NTP was last updated by the reference
- **Originate timestamp (T1):** Time/date of the NTP client
- **Receive timestamp (T2):** Time/date the packet was received by the NTP server
- **Transmit timestamp (T3):** Time/date the packet was sent by the NTP server
- **Destination timestamp (T4):** Time/date the packet was received by the NTP client

```

User Datagram Protocol, Src Port: ntp (123), Dst Port: ntp (123)
Network Time Protocol
  Flags: 0x24
    Peer Clock Stratum: primary reference (1)
    Peer Polling Interval: 10 (1024 sec)
    Peer Clock Precision: 0.000061 sec
    Root Delay: 0.0000 sec
    Root Dispersion: 28.3384 sec
    Reference ID: Global Position System
    Reference Timestamp: Mar 11, 2012 16:08:45.514776000 UTC
    Originate Timestamp: Apr  4, 2012 05:08:20.075289000 UTC
    Receive Timestamp: Apr  2, 2012 12:56:21.382108000 UTC
    Transmit Timestamp: Apr  2, 2012 12:56:21.383357000 UTC

```

NTP Stratum level

- Stratum (stratum): 8-bit integer representing the stratum:
- Stratum 16 is reported as Stratum 0 in the NTP time packet.

Value	Meaning
0	unspecified or invalid
1	primary server (e.g., equipped with a GPS receiver)
2-15	secondary server (via NTP)
16	unsynchronized
17-255	reserved

NTP time stamps reported in NTP packet

```

User Datagram Protocol, Src Port: ntp (123), Dst Port: ntp (123)
Network Time Protocol
  Flags: 0x24
    Peer Clock Stratum: primary reference (1)
    Peer Polling Interval: 10 (1024 sec)
    Peer Clock Precision: 0.000061 sec
    Root Delay: 0.0000 sec
    Root Dispersion: 28.3384 sec
    Reference ID: Global Position System
    Reference Timestamp: Mar 11, 2012 16:08:45.514776000 UTC
    Originate Timestamp: Apr  4, 2012 05:08:20.075289000 UTC
    Receive Timestamp: Apr  2, 2012 12:56:21.382108000 UTC
    Transmit Timestamp: Apr  2, 2012 12:56:21.383357000 UTC

```

The Kiss-of-Death Packet (Kiss of Death packet, KOD)

- Apparently, this is a special packet that the NTP server can send (when enabled) to an NTP client to let it know that the time request it sent to the NTP server was either:

- Denied access to NTP (access restriction is configured in the NTP server). Or,
- Was dropped due to NTP exceeding the number of clients it could respond to in that second (instead of NTP just dropping the packet without telling the client that it was dropping it).
- **Refer to:** <http://doc.ntp.org/4.1.2/acopt.htm> (excerpt below)

“Ordinarily, packets denied service are simply dropped with no further action except incrementing statistics counters. Sometimes a more proactive response is needed, such as a server message that explicitly requests the client to stop sending and leave a message for the system operator. A special packet format has been created for this purpose called the kiss-of-death packet. If the kod flag is set and either service is denied or the client limit is exceeded, the server returns the packet and sets the leap bits unsynchronized, stratum zero and the ASCII string "DENY" in the reference source identifier field. If the kod flag is not set, the server simply drops the packet.

A client or peer receiving a kiss-of-death packet performs a set of sanity checks to minimize security exposure. If this is the first packet received from the server, the client assumes an access denied condition at the server. It updates the stratum and reference identifier peer variables and sets the access denied (test 4) bit in the peer flash variable. If this bit is set, the client sends no packets to the server. If this is not the first packet, the client assumes a client limit condition at the server, but does not update the peer variables. In either case, a message is sent to the system log.”

NTP filters and algorithms

Refer to: <https://www.eecis.udel.edu/~mills/database/brief/arch/arch.pdf> and <http://www.eecis.udel.edu/~mills/ntp/html/prefer.html>

A) NTP Filters

1. Huff-n'-Puff (Huff-n-Puff) filter

- Refer to: <http://www.eecis.udel.edu/~mills/ntp/html/huffpuff.html>

In scenarios where a considerable amount of data are downloaded or uploaded using DSL or telephone modem lines, timekeeping quality can be seriously degraded. This occurs because the traffic volume, and thus the queuing delays, on the upload and download directions of transmission can be very different. In many cases the apparent time errors are so large as to exceed the step threshold and a step correction can occur during and after the data transfer.

The huff-n'-puff filter is designed to correct the apparent time offset in these cases.

Note: The default NTP Step threshold (which we use) is 128ms (For more detailed info on the step threshold, refer to [..\SecureSync CustAssist.pdf](#))

2. Clock Filter Algorithm:

- Refer to: <http://www.eecis.udel.edu/~mills/ntp/html/filter.html>
 - The clock filter algorithm processes the offset and delay samples produced by the on-wire protocol for each peer process separately.
 - It uses a sliding window of eight samples and picks out the sample with the least expected error.

Popcorn spike

Example ntp log entry from a SecureSync: `ntpd[4639]: 74.123.28.4 942d 8d popcorn 0.000040 s`

- Apparently can just be just a logging bug (<https://tools.cisco.com/quickview/bug/CSCug48022>)
- “**Popcorn**” is part of the **Clock Filter** algorithm

from <http://tools.ietf.org/html/draft-ietf-ntp-ntp4-algorithms-01>

“A 'popcorn spike' is a transient outlier, usually only a single sample, that is typical of congested Internet paths. The popcorn spike suppressor is designed to detect and remove them. Let θ_{prime} be the peer offset determined by the previous message and ψ the current peer jitter. If $|\theta - \theta_{\text{prime}}| > (K_s * \psi)$, where K_s is a tuning parameter that defaults to 3, the sample is a popcorn spike

B) NTP Algorithms

- These algorithms proceed in five phases:

1. Phase one:

Discovers the available *sources* and mobilizes an association for each source found.

“Discovery” via the “Automatic Server Discovery Schemes”

- Refer to www.eecis.udel.edu/~mills/ntp/html/discover.html

The automatic server discovery schemes provided in NTPv4. There are three automatic server discovery schemes: broadcast/multicast, many cast, and server pool

2. Phase two:

Uses the *Clock Select* algorithm to select the *candidates* from among the sources by excluding those sources showing one or more of the errors and to determine the *truechimers* from among the candidates, leaving behind the *falsechimers*

(From <http://what-when-how.com/computer-network-time-synchronization/select-algorithm-computer-network-time-synchronization/>) To provide reliable synchronization, NTP uses multiple redundant servers and multiple disjoint network paths whenever possible. When a number of associations are mobilized, it is not clear beforehand which are truechimers and which are falsechimers. Crucial to the success of this approach is a robust algorithm that finds and discards the falsechimers from the selectable server population.

Clock Select algorithm:

- Refer to: <http://www.eecis.udel.edu/~mills/ntp/html/select.html>
- Selects the best candidates for reference selection
- Determines which are **truechimers** and which are **falsechimers**.
- See the “**tos**” commands section further below for configurable tweaks

Intersection algorithm

- The intersection algorithm operates on the included population to select only those peers believed to represent the correct time.

Per Wikipedia (https://en.wikipedia.org/wiki/Intersection_algorithm): The intersection algorithm is an agreement algorithm used to select sources for estimating accurate time from a number of noisy time sources.

The intersection algorithm first scans all peers with a persistent association and includes only those that satisfy specified sanity checks. In addition to the checks required by the specification, the mitigation rules require either the local-clock peer or modem peer to be included only if marked as the prefer peer. The intersection

algorithm operates on the included population to select only those peers believed to represent the correct time. If one or more peers survive the operation, processing continues in the clustering algorithm. Otherwise, if there is a modem peer, it is declared the only survivor; otherwise, if there is a local-clock peer, it is declared the only survivor. Processing then continues in the clustering algorithm.

NTP Root Dispersion/Root Distance

- **root distance** is one-half the roundtrip root delay, plus the root dispersion, plus minor error contributions
- **root dispersion** (in milliseconds)- The root dispersion is the maximum (worst case) difference between the local system clock and the root of the NTP tree (stratum 1 clock)

<http://support.ntp.org/bin/view/Support/NTPRelatedDefinitions> This is a 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.

The **clock select algorithm** determines from a set of sources, which are correct (*truechimers*) and which are not (*falseickers*) according to a set of formal correctness assertions. The principles are based on the observation that the maximum error in determining the offset of a candidate cannot exceed one-half the roundtrip delay to the primary reference clock at the time of measurement. This must be increased by the maximum error that can accumulate since then. **The selection metric, called the *root distance*, is one-half the roundtrip root delay plus the root dispersion plus minor error contributions not considered here.**

First, a number of **sanity** checks is performed to sift the selectable candidate from among the source population. The sanity checks are summarized as follows:

1. A *stratum error* occurs if (1) the source had never been synchronized or (2) the stratum of the source is below the floor option or not below the ceiling option of the [tos](#) command. The default values for these options are 0 and 15, respectively. Note that 15 is a valid stratum, but a server operating at that stratum cannot synchronize clients.
2. A *distance error* occurs for a source if the root distance (also known as synchronization distance) of the source is not below the distance threshold *maxdist* option of the [tos](#) command. The default value for this option is 1.5 s for networks including only the Earth, but this should be increased to 2.5 s for networks including the Moon.
3. A *loop error* occurs if the source is synchronized to the client. This can occur if two peers are configured with each other in symmetric modes.
4. An *unreachable error* occurs if the source is unreachable or if the server or peer command for the source includes the *noselect* option.

3. Phase three:

???? (not mentioned)

4. Phase four:

- Uses the Clock Cluster algorithm to prune the statistical outliers from the truechimers, leaving the *survivor list* as result.

Clock Cluster Algorithm:

- Refer to: <http://www.eecis.udel.edu/~mills/ntp/html/cluster.html>
- See “**tos**” commands section further below for configurable tweaks

The clock cluster **algorithm processes the truechimers produced by the clock select algorithm to produce a list of survivors**. These survivors are used by the mitigation algorithms to discipline the system clock. The cluster algorithm operates in a series of rounds, where at each round the truechimer furthest from the offset centroid is pruned from the population. The rounds are continued until a specified termination condition is met.

5. Phase five:

Phase five uses a set of algorithms and mitigation rules to combine the survivor statistics and discipline the system clock. The mitigation rules select from among the survivors a *system peer* from which a set of system statistics can be inherited and passed along to dependent clients.

Mitigation Algorithms

- Refer to: <http://www.eecis.udel.edu/~mills/ntp/html/prefer.html>
- Consists of the **Combine Algorithm** and **Anti Clock-Hop Algorithm**
- Selects the System Peer (syspeer) for its sync and to generate the NTP statistics (Stratum level, delay, offset, jitter etc- all of the values reported in the **ntpq -p** response)

Once these five previous phases are complete:

Clock Discipline Algorithm

The clock offset developed from these algorithms can discipline the system clock, using the [clock discipline algorithm](#)

- Refer to: <http://www.eecis.udel.edu/~mills/ntp/html/discipline.html>

“tos” commands and other commands for tweaking NTP settings in clock selection and clock cluster algorithms

- Refer to: <https://www.eecis.udel.edu/~mills/ntp/html/miscopt.html#tos>

Available tos commands

- `tos [beacon beacon | ceiling ceiling | cohort {0 | 1} | floor floor | maxclock maxclock | maxdist maxdist | minclock minclock | mindist mindist | minsane minsane | orphan stratum | orphanwait delay]`

This command alters certain system variables used by the clock selection and clustering algorithms. The default values of these variables have been carefully optimized for a wide range of network speeds and reliability expectations. Very rarely is it necessary to change the default values; but, some folks can't resist twisting the knobs. It can be used to select the quality and quantity of peers used to synchronize the system clock and is most useful in dynamic server discovery schemes. The options are as follows:

beacon *beacon*

The manycast server sends packets at intervals of 64 s if less than maxclock servers are available. Otherwise, it sends packets at the *beacon* interval in seconds. The default is 3600 s. See the [Automatic Server Discovery](#) page for further details.

ceiling *ceiling*

Specify the maximum stratum (exclusive) for acceptable server packets. The default is 16. See the [Automatic Server Discovery](#) page for further details.

cohort { 0 | 1 }

Specify whether (1) or whether not (0) a server packet will be accepted for the same stratum as the client. The default is 0. See the [Automatic Server Discovery](#) page for further details.

floor *floor*

Specify the minimum stratum (inclusive) for acceptable server packets. The default is 1. See the [Automatic Server Discovery](#) page for further details.

maxclock *maxclock*

Specify the maximum number of servers retained by the server discovery schemes. The default is 10. See the [Automatic Server Discovery](#) page for further details.

maxdist *maxdistance*

Specify the synchronization distance threshold used by the clock selection algorithm. The default is 1.5 s. This determines both the minimum number of packets to set the system clock and the maximum roundtrip delay. It can be decreased to improve reliability or increased to synchronize clocks on the Moon or planets.

minclock *minclock*

Specify the number of servers used by the clustering algorithm as the minimum to include on the candidate list. The default is 3. This is also the number of servers to be averaged by the combining algorithm.

mindist *mindistance*

Specify the minimum distance used by the selection and anticlockhop algorithm. Larger values increase the tolerance for outliers; smaller values increase the selectivity. The default is .001 s. In some cases, such as reference clocks with high jitter and a PPS signal, it is useful to increase the value to insure the intersection interval is always nonempty.

minsane *minsane*

Specify the number of servers used by the selection algorithm as the minimum to set the system clock. The default is 1 for legacy purposes; however, for critical applications the value should be somewhat higher but less than minclock.

orphan *stratum*

Specify the orphan stratum with default 16. If less than 16 this is the stratum assumed by the root servers. See the [Orphan Mode](#) page for further details.

orphanwait *delay*

Specify the delay in seconds from the time all sources are lost until orphan parent mode is enabled with default 300 s (five minutes). During this period, the local clock driver and the modem driver are not selectable, unless marked with the prefer keyword. This allows time for one or more primary sources to become reachable and selectable before using backup sources, and avoids transient use of the backup sources at startup.

Other available commands

`broadcastdelay delay`

In broadcast and multicast modes, means are required to determine the network delay between the server and client. Ordinarily, this is done automatically by the initial calibration exchanges between the client and server. In some cases, the exchange might not be possible due to network or server access controls. The value of `delay` is by default zero, in which case the exchange is enabled. If `delay` is greater than zero, it becomes the roundtrip delay (s), as measured by the Unix `ping` program, and the exchange is disabled.

`driftfile driftfile`

This command specifies the complete path and name of the file used to record the frequency of the local clock oscillator. This is the same operation as the `-f` command line option. This command is mutually exclusive with the `freq` option of the `tinker` command.

If the file exists, it is read at startup in order to set the initial frequency and then updated once per hour or more with the current frequency computed by the daemon. If the file name is specified, but the file itself does not exist, the starts with an initial frequency of zero and creates the file when writing it for the first time. If this command is not given, the daemon will always start with an initial frequency of zero.

The file format consists of a single line containing a single floating point number, which records the frequency offset measured in parts-per-million (PPM). The file is updated by first writing the current drift value into a temporary file and then renaming this file to replace the old version.

`dscp dscp`

This command specifies the Differentiated Services Code Point (DSCP) value that is used in sent NTP packets. The default value is 46 for Expedited Forwarding (EF).

`enable [auth | bclient | calibrate | kernel | mode7 | monitor | ntp | stats]`

`disable [auth | bclient | calibrate | kernel | mode7 | monitor | ntp | stats]`

Provides a way to enable or disable various system options. Flags not mentioned are unaffected. Note that most of these flags can be modified remotely using [ntpq](#) utility program's `:config` and `config-from-file` commands.

`auth`

Enables the server to synchronize with unconfigured peers only if the peer has been correctly authenticated using either public key or private key cryptography. The default for this flag is enable.

`bclient`

Enables the server to listen for a message from a broadcast or multicast server, as in the `multicastclient` command with default address. The default for this flag is disable.

`calibrate`

Enables the calibrate feature for reference clocks. The default for this flag is disable.

`kernel`

Enables the kernel time discipline, if available. The default for this flag is enable if support is available, otherwise disable.

`mode7`

Enables processing of NTP mode 7 implementation-specific requests which are used by the deprecated `ntpd` program. The default for this flag is disable. This flag is excluded from runtime configuration using `ntpq`. The `ntpq` program provides the same capabilities as `ntpd` using standard mode 6 requests.

`monitor`

Enables the monitoring facility. See the [ntpq program](#) and the `monstats` and `mrulist` commands, as well as the [Access Control Options](#) for details. The monitoring facility is also enabled by the presence of [limited](#) in any `restrict` commands. The default for this flag is enable.

`ntp`

Enables time and frequency discipline. In effect, this switch opens and closes the feedback loop, which is useful for testing. The default for this flag is enable.

`stats`

Enables the statistics facility. See the [Monitoring Options](#) page for further information. The default for this flag is enabled. This flag is excluded from runtime configuration using `ntpq`.

`includefile includefile`

This command allows additional configuration commands to be included from a separate file. Include files may be nested to a depth of five; upon reaching the end of any include file, command processing resumes in the previous configuration file. This option is useful for sites that run `ntpd` on multiple hosts, with (mostly) common options (e.g., a restriction list).

`interface [listen | ignore | drop] [all | ipv4 | ipv6 | wildcard | name | address[/prefixlen]]`

This command controls which network addresses `ntpd` opens, and whether input is dropped without processing. The first parameter determines the action for addresses which match the second parameter. That parameter specifies a class of addresses, or a specific interface name, or an address. In the address case, `prefixlen` determines how many bits must match for this rule to apply. `ignore` prevents opening matching addresses, `drop` causes `ntpd` to open the address and drop all received packets without examination. Multiple `interface` commands can be used. The last rule which matches a particular address determines the action for it. `interface` commands are disabled if any `-I`, `--interface`, `-L`, or `--novirtualips` command-line options are used. If none of those options are used and no `interface` actions are specified in the configuration file, all available network addresses are opened. The `nic` command is an alias for `interface`.

`leapfile leapfile`

This command loads the IERS leapseconds file and initializes the leapsecond values for the next leapsecond time, expiration time and TAI offset. The file can be obtained directly from the IERS at <https://hpiers.obspm.fr/iers/bul/bulc/ntp/leap-seconds.list> or <ftp://hpiers.obspm.fr/iers/bul/bulc/ntp/leap-seconds.list>.

The `leapfile` is scanned when `ntpd` processes the `leapfile` directive or when `ntpd` detects that `leapfile` has changed. `ntpd` checks once a day to see if the `leapfile` has changed.

While not strictly a security function, the Autokey protocol provides means to securely retrieve the current or updated leapsecond values from a server.

`leapsmearinterval seconds`

This EXPERIMENTAL option is only available if `ntpd` was built with the `--enable-leap-smear` option to the `configure` script. It specifies the interval over which a leap second correction will be applied. Recommended values for this option are between 7200 (2 hours) and 86400 (24 hours). **DO NOT USE THIS OPTION ON PUBLIC-ACCESS SERVERS!** See <http://bugs.ntp.org/2855> for more information.

`logconfig configkeyword`

This command controls the amount and type of output written to the system `syslog` facility or the alternate logfile `log` file. All `configkeyword` keywords can be prefixed with `=`, `+` and `-`, where `=` sets the `syslogmask`, `+` adds and `-` removes messages. `syslog` messages can be controlled in four classes (`clock`, `peer`, `sys` and `sync`). Within these classes four types of messages can be controlled: informational messages (`info`), event messages (`events`), statistics messages (`statistics`) and status messages (`status`).

Configuration keywords are formed by concatenating the message class with the event class. The `all` prefix can be used instead of a message class. A message class may also be followed by the `all` keyword to enable/disable all messages of the respective message class. By default, `logconfig` output is set to `allsync`.

Thus, a minimal log configuration could look like this:

`logconfig=syncstatus +sysevents`

This would just list the synchronizations state of `ntpd` and the major system events. For a simple reference server, the following minimum message configuration could be useful:

```
logconfig=synccall +clockall
```

This configuration will list all clock information and synchronization information. All other events and messages about peers, system events and so on is suppressed.

```
logfile logfile
```

This command specifies the location of an alternate log file to be used instead of the default system `syslog` facility. This is the same operation as the `-l` command line option.

```
mru [maxdepth count | maxmem kilobytes | mindepth count | maxage seconds | initialloc count |
```

```
initmem kilobytes | incalloc count | incmem kilobytes]
```

Controls size limits of the monitoring facility Most Recently Used ([MRU](#)) list of client addresses, which is also used by the [rate control facility](#).

```
maxdepth count
```

```
maxmem kilobytes
```

Equivalent upper limits on the size of the MRU list, in terms of entries or kilobytes. The actual limit will be up to `incalloc` entries or `incmem` kilobytes larger. As with all of the `mru` options offered in units of entries or kilobytes, if both `maxdepth` and `maxmem` are used, the last one used controls. The default is 1024 kilobytes.

```
mindepth count
```

Lower limit on the MRU list size. When the MRU list has fewer than `mindepth` entries, existing entries are never removed to make room for newer ones, regardless of their age. The default is 600 entries.

```
maxage seconds
```

Once the MRU list has `mindepth` entries and an additional client address is to be added to the list, if the oldest entry was updated more than `maxage` seconds ago, that entry is removed and its storage reused. If the oldest entry was updated more recently, the MRU list is grown, subject to `maxdepth`/`maxmem`. The default is 64 seconds.

```
initialloc count
```

```
initmem kilobytes
```

Initial memory allocation at the time the monitoring facility is first enabled, in terms of entries or kilobytes. The default is 4 kilobytes.

```
incalloc count
```

```
incmem kilobytes
```

Size of additional memory allocations when growing the MRU list, in entries or kilobytes. The default is 4 kilobytes.

```
nonvolatile threshold
```

Specify the `threshold` in seconds to write the frequency file, with default of 1e-7 (0.1 PPM). The frequency file is inspected each hour. If the difference between the current frequency and the last value written exceeds the threshold, the file is written and the `threshold` becomes the new threshold value. If the threshold is not exceeded, it is reduced by half. This is intended to reduce the frequency of unnecessary file writes for embedded systems with nonvolatile memory.

```
phone dial ...
```

This command is used in conjunction with the ACTS modem driver (type 18). The arguments consist of a maximum of 10 telephone numbers used to dial USNO, NIST or European time services. The Hayes command ATDT is normally prepended to the number, which can contain other modem control codes as well.

```
reset [allpeers] [auth] [ctl] [io] [mem] [sys] [timer]
```

Reset one or more groups of counters maintained by `ntpd` and exposed by `ntpq` and `ntpdcc`.

```
rlimit [memlock Nmegabytes | stacksize N4kPages | filenum Nfiledescriptors]
```


This command alters certain process storage allocation limits, and is only available on some operating systems. Options are as follows:

`memlock Nmegabytes`

Specify the number of megabytes of memory that should be allocated and locked. Probably only available under Linux, this option may be useful when dropping root (the `-i` option). The default is 32 megabytes on non-Linux machines, and -1 under Linux. -1 means "do not lock the process into memory". 0 means "lock whatever memory the process wants into memory".

`stacksize N4kPages`

Specifies the maximum size of the process stack on systems with the `mlockall()` function. Defaults to 50 4k pages (200 4k pages in OpenBSD).

`filenum Nfiledescriptors`

Specifies the maximum number of file descriptors ntp may have open at the same time. Defaults to system default.

`saveconfigdir directory_path`

Specify the directory in which to write configuration snapshots requested with ntpq's [saveconfig](#) command. If `saveconfigdir` does not appear in the configuration file, saveconfig requests are rejected by ntpd.

`setvar variable [default]`

This command adds an additional system variable. These variables can be used to distribute additional information such as the access policy. If the variable of the form `name = value` is followed by the `default` keyword, the variable will be listed as part of the default system variables (ntp `rv` command). These additional variables serve informational purposes only. They are not related to the protocol other than they can be listed. The known protocol variables will always override any variables defined via the `setvar` mechanism. There are three special variables that contain the names of all variable of the same group. The `sys_var_list` holds the names of all system variables. The `peer_var_list` holds the names of all peer variables and the `clock_var_list` holds the names of the reference clock variables.

`tinker [allan allan | dispersion dispersion | freq freq | huffpuff huffpuff | panic panic | step step | stepout stepout]`

This command alters certain system variables used by the clock discipline algorithm. The default values of these variables have been carefully optimized for a wide range of network speeds and reliability expectations. Very rarely is it necessary to change the default values; but, some folks can't resist twisting the knobs. Options are as follows:

`Allan allan`

Specifies the Allan intercept, which is a parameter of the PLL/FLL clock discipline algorithm, in seconds with default 1500 s.

`dispersion dispersion`

Specifies the dispersion increase rate in parts-per-million (PPM) with default 15 PPM.

`freq freq`

Specifies the frequency offset in parts-per-million (PPM). This option is mutually exclusive with the `driftfile` command.

`huffpuff huffpuff`

Specifies the huff-n'-puff filter span, which determines the most recent interval the algorithm will search for a minimum delay. The lower limit is 900 s (15 min), but a more reasonable value is 7200 (2 hours). See the [Huff-n'-Puff Filter](#) page for further information.

`panic panic`

pecifies the panic threshold in seconds with default 1000 s. If set to zero, the panic sanity check is disabled and a clock offset of any value will be accepted.

step step

Specifies the step threshold in seconds. The default without this command is 0.128 s. If set to zero, step adjustments will never occur. Note: The kernel time discipline is disabled if the step threshold is set to zero or greater than 0.5 s. Further details are on the [Clock State Machine](#) page.

stepout stepout

Specifies the stepout threshold in seconds. The default without this command is 300 s. Since this option also affects the training and startup intervals, it should not be set less than the default. Further details are on the [Clock State Machine](#) page.

“Time Reset” when NTP starts up

The following information is from <http://doc.ntp.org/4.1.1/debug.htm>.

In summary of the following info: Each time SecureSync boot-up, its on-time point is arbitrary. When NTP starts running:

- At least four valid polls from the majority of all configured time references are required before NTP can sync.
- If the time error is greater than the panic threshold (1000 seconds) NTP will stop syncing.
- If the time error is less than the step threshold (128 ms) when NTP syncs, NTP will simply slew its time and therefore, no “Time Reset” will occur (the NTP log won’t contain a “Time Reset” entry).
- If the time error is less than 1000 seconds, but greater than the step threshold (128 ms) NTP starts a 900 second counter (stepout threshold). During this “wait”, its apparently verifying the information it’s receiving is valid. At the end of 900 seconds (exactly 15 minutes) if the data was valid, NTP performs a “Time Reset” to the correct time (the NTP log will contain a “Time Reset” entry)
- To change the default duration of step threshold (shorter or longer) use the NTP Expert mode to add a “tinker stepout” line to the ntp.conf file. Example: Add “Tinker stepout 1800” to the ntp.conf file for a 30 minute wait before the time is corrected.

When first started, the daemon normally polls the servers listed in the configuration file at 64-s intervals. In order to allow a sufficient number of samples for the NTP algorithms to reliably discriminate between correctly operating servers and possible intruders, at least four valid messages from the majority of servers and peers listed in the configuration file is required before the daemon can set the local clock. However, if the difference between the client time and server time is greater than the panic threshold, which defaults to 1000 s, the daemon will send a message to the system log and shut down without setting the clock. It is necessary to set the local clock to within the panic threshold first, either manually by eyeball and wristwatch and the Unix [date](#) command, or by the [ntpdate](#) or [ntpd -q](#) commands. The panic threshold can be changed by the [tinker panic](#) command described on the [Miscellaneous Options](#) page. The panic threshold can be disabled entirely by the [-g](#) command line option described on the [ntpd - Network Time Protocol \(NTP\) daemon](#) page.

If the difference between local time and server time is less than the panic threshold but greater than the step threshold, which defaults to 128 ms, the daemon will perform a step adjustment; otherwise, it will gradually slew the clock to the nominal time. The step threshold can be changed by the [tinker step](#) command described on the [Miscellaneous Options](#) page. The step threshold can be disabled entirely by the [-x](#) command line option described on the [ntpd - Network Time Protocol \(NTP\) daemon](#) page. In this case the clock will never be stepped; however, users should understand the implications for doing this in a distributed data network where all processing must be tightly synchronized. See the [NTP Timescale and Leap Seconds](#) page for further information. If a step adjustment is made, the clock discipline algorithm will start all over again, requiring another round of at least four messages as before. This is necessary so that all servers and peers operate on the same set of time values.

The clock discipline algorithm is designed to avoid large noise spikes that might occur on a congested network or access line. If an offset sample exceeds the step threshold, it is ignored, and a timer started. If a later sample is below the step threshold, the counter is reset. However, if the counter is greater than the stepout interval, which defaults to 900 s, the next sample will step or slew the time as directed. The stepout threshold can be changed by the [tinker stepout](#) command described on the [Miscellaneous Options](#) page.

Sync status at start-up (LI bits and Stratum value)

There are two values that NTP uses to report to its NTP clients whether or not its time stamps are valid and useable. These are its reported NTP Stratum level and its two Leap Indicator bits (LI bits). The LI bits are used to report the NTP sync status and whether a leap second is pending. The Ref ID is an operation indicator but isn’t meant to indicate whether or not the time data should be used. Step indicates that a larger than 10 minute time difference between the kernel time and the reference times exists, so NTP is making a large correction to the time (this value will not necessarily be reported at start-up). Ref ID of GPS indicates the reference is synced to GPS, etc.

When NTP first starts up, the Stratum is reported as 0 (not a valid NTP stratum level, which tells the NTP clients to ignore

the time stamps). Also, both of the LI bits are set, for a LI value of “3”. This tells the NTP clients that NTP is not in sync and the rest of the packet should be ignored.

When NTP is ready to have its clients be able to synchronize to it (based on it being able to provide valid time) the LI bits will become a 0, 1 or 2 (depending on leap second state) and the Stratum will be reported as Stratum 1.

- When the Web browser shows NTP is at Stratum 16, the NTP packets are actually outputting “Stratum 0” (which indicates “invalid packet”).

Two emails from Paul Myers (7/5/12)

If you refer to RFC 5905, Stratum 0 indicates INVALID or UNSYNCHRONIZED. The NTP Client will NOT use such a packet. When we go to Stratum 16 it is to ensure that NO one can sync to us.

Stratum 0 is a BAD thing in a NTP packet. This is ONLY an issue if NTP clients are badly written and ignore Stratum and/or LI bits.

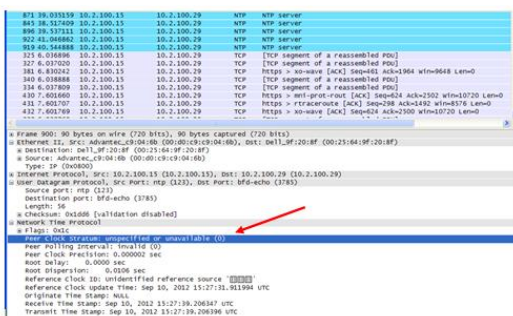
The Local Clock is fudged to make us go to 16 so we cannot be an NTP reference to any other NTP client/server.

<http://www.ietf.org/rfc/rfc5905.txt>

It is customary to map the **stratum value 0 in received packets to MAXSTRAT (16)** in the peer variable stratum and to map p.stratum values of MAXSTRAT or greater to 0 in transmitted packets. This allows reference clocks, which normally appear at stratum 0, to be conveniently mitigated using the same clock selection algorithms used for external sources (see Appendix A.5.5.1 for example).

NTP at Stratum 16

The NTP server's Stratum level is reported in the NTP packet's “**Peer Clock Stratum**” field. When NTP is Stratum 16, the NTP servers report this to the NTP clients by indicating in this field that the Stratum is currently “0”. Specifically, it reports “**unspecified or unavailable (0)**” as shown in the screenshot below (taken from a Model 9483 while NTP was running at Stratum 16).



Since “0” is not a valid NTP Stratum level (valid range is 1 through 15), NTP Clients **SHOULD** ignore the NTP server, when it indicates its Stratum “0”

Note: Apparently, the VxWorks NTP client still accepts the time when we reported the Stratum as “0”. Refer to the record for TOYO in Salesforce that discusses this issue with VxWorks.

****NTP operational modes/states (.INIT, Step, etc)**

Client: Indicates a Client/Server relation used when communicating with another reference that is configured as a "Server".

.INIT: Indicates the NTP mode of the reference has not yet been identified (see additional info further below).

.STEP: Indicates an initial time correction has been applied.

Symmetric Active (1): 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 (2): This type of association is ordinarily created upon arrival of a message from a peer operating in the symmetric active mode and persists only as long as the peer is reachable and operating at a stratum level less than or equal to the host; otherwise, the association is dissolved. However, the association will always persist until at least one message has been sent in reply. By operating in this mode the host announces its willingness to synchronize and be synchronized by the peer.

per: <https://www.eecis.udel.edu/~mills/ntp/html/assoc.html#symact>

Symmetric Active/Passive Mode

Symmetric active/passive mode is intended for configurations where a clique of low-stratum peers operate as mutual backups for each other. Each peer operates with one or more primary reference sources, such as a reference clock, or a set of secondary (stratum, 2) servers known to be reliable and authentic. Should one of the peers lose all reference sources or simply cease operation, the other peers will automatically reconfigure so that time and related values can flow from the surviving peers to all hosts in the subnet. In some contexts, this would be described as a "push-pull" operation, in that the peer either pulls or pushes the time and related values depending on the particular configuration.

A **symmetric active** peer sends a **symmetric active** (mode 1) message to a designated peer. If a matching configured symmetric active association is found, the designated peer returns a symmetric active message. If no matching association is found, the designated peer mobilizes a ephemeral symmetric passive association and returns a symmetric passive (mode 2) message. Since an intruder can impersonate a symmetric active peer and cause a spurious symmetric passive association to be mobilized, symmetric passive mode should always be cryptographically validated.

A peer is configured in symmetric active mode using the `peer` command and specifying the other peer DNS name or IPv4 or IPv6 address. The `burst` and `iburst` options should not be used in symmetric modes, as this can upset the intended symmetry of the protocol and result in spurious duplicate or dropped messages.

As symmetric modes are most often used as root servers for moderate to large subnets where rapid response is required, it is generally best to set the minimum and maximum poll intervals of each root server to the same value using the `minpoll` and `maxpoll` options.

Per: <https://www.eecis.udel.edu/~mills/ntp/html/assoc.html#symact>

With symmetric modes the most stable behavior results when both peers are configured in symmetric active mode with matching poll intervals of 6 (64 s).

.INIT refID being reported by an NTP reference

A) INIT

- should only remain “.init” until after about the initial NTP packet return from the SecureSync
- Indicates the NTP mode of the reference has not yet been identified (see additional info further below).
- “.init” is **494e4954** (in hex)
- Indicates NTP is trying to reach the reference for the first time, but can't initiate communications with this reference.
- Most likely causes:
 - The default gateway is not configured or not configured correctly, or
 - There is a network issue with port 123, or
 - NTP symmetric key is being enforced, but not correctly configured in all devices (preventing auth from being successful)

To troubleshoot “.init” refID not changing shortly after NTP has started

- is the “.init” SecureSync able to sync any other NTP clients
- Does the “.init” SecureSync respond to pings (If no response, likely network issue or problem with the “.init” SecureSync)
- perform a **traceroute -p 123 xxx.xxx.xxx** CLI call to the init SecureSync
- verify it's a valid NTP server that is known to be up and running.
- Check if **NTP Symmetric key authentication** is being enforced in either SecureSync
- To determine if a SecureSync requires successful symmetric key authentication, on the left side of the **Management** -> NTP Setup page of the browser, click the “**Access Restrictions**” button. In the pop-up window, see if there is a “1” in the first row (for “IP4”), for the “Auth Only” column (as shown below)



Type	IP Version	IP	IP Mask	Auth Only	Enable Query	
Allow	IPv4	default		1		<div>Change</div> <div>Delete</div>
Allow	IPv6	default				<div>Change</div> <div>Delete</div>

email Keith sent about “.init and symmetric authentication: (18 Dec 2018) I was just talking with one of our Apps Engineers about NTP's refid value of “.init”. In addition to this being the initial refid for a peer/server when NTP first starts-up (until it starts getting NTP responses back from the particular peer/server), I wasn't sure if NTP would continue reporting “.init” if there was a larger time error than its expecting

He said he didn't believe so, especially if the Reach value for this same NTP sever is remaining “0” as well. And the testing I've been performing shows this doesn't appear to be the case- time error doesn't affect “.init” and doesn't stop the reach from incrementing. These two values in ntpq -p just need to see a time stamp returned.

But I just thought of another factor (besides a firewall in between blocking port 123) which I suspect could very well also affect both items— NTP symmetric key authentication, (one SecureSync requiring it, while its peer/server SecureSync/NTP either not configured to use it, or not correctly configured with an identical keystore/digest, or a key not marked as trusted. Symmetric key is a function of NTP often required for switches to sync to an NTP server, especially Cisco switches.

After first verifying normal/expected NTP peering operation (Reach incrementing and “.init” changing mere moments later) with no symmetric keying configured, I then ran a simple test to see if NTP symmetric key, if not correctly configured in both SecureSyncs, will prevent “.init” from changing/Reach from incrementing for a peer.

I had “B” peered to “A” and told “A” to require symmetric key (even though “B” has no keys configured). This provided a case where successful authentication isn't possible. As I suspected, just like if there was a network issue between the two SecureSyncs – such as port 123 being closed, the Reach value stayed 0 and the refid stayed init for the peer which was not able to successfully authenticate.

Based on this observation that it definitely affects init and Reach, I now suspect the issue you are observing is that there is a symmetric key configuration mis-match between the “.init” server and the other SecureSync(s).

If the server that you were running ntpq -p command on has been configured to require authentication (not the factory default state), and its

To determine if a SecureSync requires successful symmetric key authentication, on the left side of the **Management** -> NTP Setup page of the browser, click the “**Access Restrictions**” button. In the pop-up window, see if there is a “1” in the first row (for “IP4”), for the “Auth **Only**” column (as shown below)

If this field is blank, this SecureSync doesn't require successful authentication in order to exchange NTP packets with other NTP clients/other SecureSyncs. But if there is a "1" in the field (as shown above) symmetric key is being enforced and so it will only exchange NTP packets with other devices which are configured with an identical keystore.

1	1	WDS	153492618	<input type="checkbox"/> delete <input checked="" type="checkbox"/> clone
11111111	key ID	device	key value	

the keystring on both NTP devices have to be IDENTICAL

if the Keys table for the SecureSync requiring auth has at least one key in it and its marked as Trusted, but the other NTP server has no keys listed, none of the keystings are identical and/or a key with a matching string isn't marked as trusted, this is the problem. You will need to either create a new key having the trusted box selected and a matching keystring, or edit an existing incorrect key to make it a trusted/matching key.

B) .DROP

If the antenna or other reference is not connected, do not list each other as peers. Instead, list the one that is synced as a NTP server in the “Servers” table of the other unit that is not synced to a reference. Then restart NTP.

Example below:

MILFORD (Antenna attached)

NTP Reference Status:												
Sync	Host	Ref ID	Stratum	Mode	Type	Auth Status	Last (Sec)	Poll Interval (Sec)	Reach	Delay (mS)	Offset (mS)	Jitter (mS)
*	Spectracom	GPS	0	Client	local	none	65	64	377	0.000	0.063	0.002
	172.23.75.10	Ⓜ	16	Symmetric Active	unicast	none	12	128	0	0.000	0.000	4000.000

Jefferson (No Antenna)

NTP Reference Status:												
Sync	Host	Ref ID	Stratum	Mode	Type	Auth Status	Last (Sec)	Poll Interval (Sec)	Reach	Delay (mS)	Offset (mS)	Jitter (mS)
	Spectracom	LCL	0	Client	local	none	0	16	0	0.000	0.000	4000.000
	172.23.75.10	DROP	16	Symmetric Active	unicast	none	0	16	0	0.000	0.000	4000.000

C) .USER

- “.user” is “55534552” in hex
- System Time has been manually set using the user reference.

D) .STEP

- A step time change in system time has occurred, but the association has not yet resynchronized.
- Time change of less than the panic threshold of 1000 seconds (16 min 40 sec) occurred.

E) .DENY

- NTP access was denied by the NTP server

F) .BCST

- NTP broadcast time server

G) **.PPS (atom clock driver/ System PPS)

- Refer to sites such as <http://www.eecis.udel.edu/~mills/ntp/html/drivers/driver22.html>
- “.PPS” is “50505300” in hex
- As long as the “Enable Stratum 1PPS” checkbox (newer browser) or “Timing System 1PPS Reference” field is “Enabled” (classic interface) in the NTP Servers tab, NTP can select the System PPS reference, if it wishes to (it’s not guaranteed that it will). When Enabled, the Status -> NTP page of the browser will list System PPS as an NTP reference for NTP selected. But if it’s an “X”, NTP won’t be able to select it as a reference.
- If the “Enable Stratum 1PPS” checkbox (newer browser) or “Timing System 1PPS Reference” field is “Disabled” (classic interface) in the NTP Servers tab, the Status -> NTP page won’t list system PPS as a possible reference for NTP input. So it can’t be selected.
- It can take several minutes for NTP to select System PPS, if it desires to select it.

Note: When NTP servers or peers have been configured, the “**Enable Stratum 1PPS**” checkbox (newer browser) or “**Timing System 1PPS Reference**” field” (classic interface) should be disabled.

Newer web browser (versions 5.1.2 and above)

Once NTP has synced to GPS inside the SecureSync (and assuming the “**Enable Stratum 1 1PPS**” checkbox is Enabled in the **Management -> NTP Setup** page of the browser, **Stratum 1** tab, after pressing the “gear” icon to the right of “NTP Services” as shown below), we enable another NTP input reference that uses the 1PPS generated by the GPS signal.

This “PPS” reference helps stabilize/optimize the NTP functionality, if NTP decides to select it as its input. This input is known as NTP’s PPS clock driver and can be selected by NTP shortly after NTP syncs to GPS. If NTP selects it as its reference, NTP changes the Ref ID to “.PPS” to indicate this PPS clock driver had been enabled.



**NTP Leap Seconds

- The two LI (Leap Indicator) bits in the NTP packet signify when a leap second is pending (they also normally indicate NTP not in sync).
- NTPv3 specs (RFC 1305) say the LI bits will be set and Leap second will occur at the end of that particular day (LI bits change 24 hours prior)
- NTPv4 specs say the LI bits will be set and Leap second will occur at the end of that particular month (LI bits change 30 days prior)

LI, Leap Indicator (2 bits)

This code warns of an impending leap second to be inserted/deleted in the last minute of the current day.

LI bits	Description
0	No warning.
1	Last minute has 61 seconds.
2	Last minute has 59 seconds.
3	Alarm condition (clock not synchronized)

- NTPv4 specs (RFC 5905) say the LI bits will be set and Leap second will occur at the end of that particular month. <http://datatracker.ietf.org/doc/rfc5905/>

LI Leap Indicator (leap): 2-bit integer warning of an impending leap second to be inserted or deleted in the last minute of the current month with values defined in Figure 9.

-----+-----
Value Meaning
-----+-----
0 no warning
1 last minute of the day has 61 seconds
2 last minute of the day has 59 seconds
3 unknown (clock unsynchronized)
-----+-----

(2/15/12 KW) All Models 9300 series and below as well as some SecureSyncs/9400 series support the NTPv3 spec. We are in the process of likely changing the software in NetClocks and SecureSync to support the NTPv4 specs (leap second inserted “end of month” instead of “end of day”).

Unexpected NetClock 9300 series time jumps due to leap second

- Abnormal/unexpected time jumps occurred on Model 9388s on Jun 31st.
- Refer to ICAP Salesforce case 7050 for more info)

Email from Paul Myers to Dave Lorah (9 Jan 2013) All units have the leap second in the GPS config file scheduled for 7/1/2012 appropriately.

This leads me to believe the peer ntp packets setup the Linux kernel via NTP or NTP

leapsecondstatus=16, 16, 7, 1, 2012

I believe the NTP packet containing an LI leap indicator was received AFTER the leap second adjustment and scheduled another one.

Our code did not use NTP as a leap second source so we did not log it.

However, the linux kernel did and it happened later.

I would have assumed it would have happened at the beginning of the next month.

<http://lists.ntp.org/pipermail/questions/2012-August/033666.html>

The fast NTP poll rate of 64 seconds probably facilitated this. We will have to test NTP leap second and then test the kernel for scheduled leap second adjustments. Maybe we can clear the NTP and kernel after a leapsecond event?

Email from Paul Myers to Dave Lorah (9Jan 2013)

We should tell them:

root cause was NTP propagating Leap second too fast over end of day. Due to fast poll rate.

We have made leap second changes in code

NTP

NTP Selection algorithm selects among Stratum 1 servers and GPS based on complex algorithm.

I can provide the book and you can scan the page and email it.

I need to come up with a smooth answer....

Update to 3.6.0 and optionally 3.6.1 later

Peer ONLY locally with the adjacent server if they must peer at all!!!!

NTP peering max poll rates should be longer – no benefit to fast polls

Min 6, Max 10 or

Min 4, Max 10

NTP Bug (sys_leap is sticky)”: False leap second keeps being asserted- NTP flag doesn’t clear after a leap second has been inserted (earlier NTP versions v4.2.6 and below. Fixed in v4.2.7)

- Refer to [https://groups.google.com/forum/#!topic/comp.protocols.time.ntp/nHZOEvNTpVo\[1-25\]](https://groups.google.com/forum/#!topic/comp.protocols.time.ntp/nHZOEvNTpVo[1-25])
 - “One is a bug in ntpd 4.2.6 that it can get stuck with the incorrect leap status and only restart can fix it”
 - Refer to NTP bug 2246 (“**sys_leap is sticky**”) http://bugs.ntp.org/show_bug.cgi?id=2246
 - “Leapseconds. If a leap is pending, decrement the time remaining. If less than one day remains, set the leap bits. When no time remains, clear the leap bits and increment the TAI.”
- “The line marked A) only resets sys_leap if leapsec decrements from 1 to 0. However, leapsec is set to 0 elsewhere as a result of the voting process:
- From a 9383 config file that keeps asserting leap seconds (note the first number is current TAI offset and the second is future TAI offset): **leapsecondstatus=16, 17, 7, 1, 2015**
- Stopping/Restarting NTP or rebooting **all** of the time servers on the network (or at least the ones that have a different value for current and future TAI offsets) before the end of the month reportedly should fix it

NTP flags leap second insertion even with just one upstream NTP server indicating leap second is pending (versions prior to version 4.2.6-)

- Refer to [https://groups.google.com/forum/#!topic/comp.protocols.time.ntp/nHZOEvNTpVo\[1-25\]](https://groups.google.com/forum/#!topic/comp.protocols.time.ntp/nHZOEvNTpVo[1-25])
 - “The other is in pre 4.2.6 versions that they accept the leap at any time when any of its sources is announcing the leap”
 - “The current firmware version, 6.18.004, ships with NTP 4.2.8p3 which doesn't accept a leap second announcement from a single upstream server.”

NTP Peering

Reference identifier showing “.DROP”

The Reference identifier shows the word “**DROP**” in a Peer status. This appears to be due two units being peered, but when NTP starts up, only one of the two is in sync while the other is not in sync. If they both don't start at the same stratum, peering does not seem to work.

If the antenna or other reference is not connected, do not list each other as peers. Instead, list the one that is synced as a NTP server in the “Servers” table of the other unit that is not synced to a reference. Then restart NTP. Example below:

MILFORD (Antenna attached)



JEFFERSON (No Antenna)

NTP Reference Status:												
Sync	Host	Ref ID	Stratum	Mode	Type	Auth Status	Last (Sec)	Poll Interval (Sec)	Reach	Delay (mS)	Offset (mS)	Jitter (mS)
	Spectracom	LCL	0	Client	local	none	0	16	0	0.000	0.000	4000.000
	172.23.75.10	.DROP.	16	Symmetric Active	unicast	none	0	16	0	0.000	0.000	4000.000

***NTP log entries associated with NTP peering

1) Unexpected origin timestamp xxxxx.xxxxx does not match aorg 00000.00000 from xx

Example log entries (from a SecureSync)

```
Jul 12 15:04:28 ndcntp201 ntpd[2035]: receive: Unexpected origin timestamp 0xdb2a06ab.321416e8 from 172.18.33.227
xmt 0xdb2f857c.349efd85
Jul 12 15:22:34 ndcntp201 ntpd[2035]: receive: Unexpected origin timestamp 0xdb2a06ab.321416e8 from 172.18.33.227
xmt 0xdb2f89ba.349ec968
Jul 12 15:40:11 ndcntp201 ntpd[2035]: receive: Unexpected origin timestamp 0xdb2a06ab.321416e8 from 172.18.33.227
xmt 0xdb2f8ddb.34a0dfa1
```



In Summary of the info further below:

- (**SecureSync/NetClock 9400 Versions 5.4.4 and below**): Actual NTP operation issue with loss of peer responsiveness prior to NTPv4.2.8p7
 - (**SecureSync/NetClock 9400 (Versions 5.4.5 to at least 5.8.4, and likely even higher)**): Errant NTP logging issue only – not an indication of operational NTP issue (these log entries are carryover from the issue in earlier NTP versions, and can simply be ignored/disregarded)
 - (**all NetClock 9300/9200 series**): all software versions are at NTPv4.2.0 (prior to v4.2.8p7) so this entry being asserted is highly likely indicative of an actual issue in NTP, and not likely just an errant NTP log entry/
- Refer to Salesforce Cases such as 185388 (for a SecureSync)
- This is a bug in NTP- Reportedly fixed in NTP v4.2.8p7 (SecureSync versions 5.4.4 and below are susceptible. We are expecting to update to 4.2.8p7 in v5.4.5) For more info on this NTP bug, refer to: http://bugs.ntp.org/show_bug.cgi?id=2952
- in earlier NTP versions it appears to cause intermittent loss of communications (NTP timestamps between

peers), intermittent loss of time stamps from a peer and so the Peer(s) Reach value goes to 0.

- Refer to sites such as: <https://www.suse.com/support/kb/doc?id=7017645> (except pasted below)

Situation

Having peer servers configured as part of the NTP configuration, the following messages are logged in "/var/log/ntp":

ntpd[xxxx] receive: Unexpected origin timestamp xxxxx.xxxxx does not match aorg 00000.00000 from xx (Where xx at the end of the message is the IP address of the configured peer server). Eventually this results in communication failure between the configured servers.

Resolution

Update NTP to version 4.2.8p7 or above (SecureSync versions 5.4.4 and below are susceptible. We are expecting to update to 4.2.8p8 in v5.4.5)

Cause

This was caused by changes made to bogus packet detection of NTP. Although the messages are still logged with the current latest NTP version, communication is not lost anymore, and the messages can be ignored.

NTP start-up / NTP auto restart for >10 minute time jump

NTP in SecureSync as well as Model 9200/930/9400 use a switch that allows NTP at startup to accept the reference's info, no matter how far off the information is (time/date errors). However this switch allows only one "time jump" to occur. If the time is off by more than 10 minutes more than once and if it only has one reference to select from, NTP will stop polling the reference until NTP has been restarted.

SecureSync/9400s with version 4.8.2 and above installed have an NTP monitor that will restart NTP if it's enabled but not running. As of at least 4/4/12, the Model 9300/9200 NetClocks will not automatically restart NTP if this issue occurs.

According to Mark Goodlein (/25/12) NTP is monitored using a daemon that looks at NTP every 5 seconds to ensure its running (if NTP is enabled). In certain cases, it speeds up to every two seconds, but it won't exceed every 5 seconds.

Email from Paul Myers (4/4/12):

NTP is started with the line:

loadproc /usr/sbin/ntpd -g -c /etc/ntp/ntp.conf

Note the -g only allows one correction. Further time jumps still crash it.

<http://www.eecis.udel.edu/~mills/ntp/html/ntpd.html>

-g

Normally, ntpd exits with a message to the system log if the offset exceeds the panic threshold, which is 1000 s (16.7 minutes) by default. This option allows the time to be set to any value without restriction; however, this can happen only once. If the threshold is exceeded after that, ntpd will exit with a message to the system log. This option can be used with the -q and -x options. See the tinker command for other options.

****NTP performance/algorithms for reference selection

- <http://www.eecis.udel.edu/~mills/ntp/html/stats.html>
- <http://www.eecis.udel.edu/~mills/ntp/html/cluster.html>

Email from Dave Lorah (20 Jan 15) The SecureSync runs NTP software which governs the network time messaging and synchronization. NTP processes each peer and decides which are the best.

There is some good information on the NTP website describing the Clock Cluster Algorithm and other that decide good references

(truechimers) from lesser references (outliers). For questions on NTP operation we refer customers to the NTP website.

Here are links to this info:

<http://www.eecis.udel.edu/~mills/ntp/html/stats.html>

<http://www.eecis.udel.edu/~mills/ntp/html/cluster.html>

***Clock Status / NTP Precision value

NTP Precision

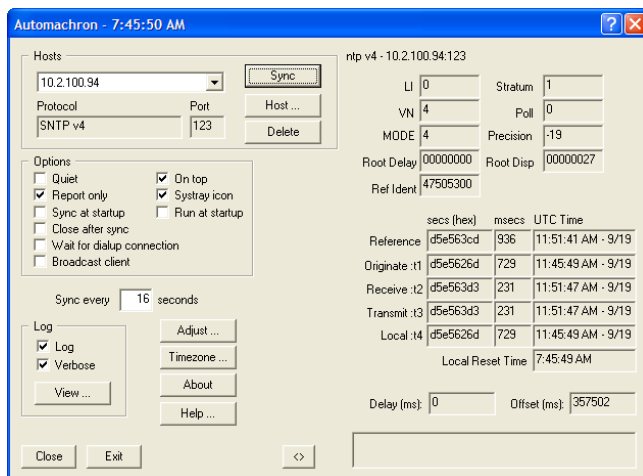
From <http://www.ntp.org/ntpfaq/NTP-s-sw-clocks-quality.htm>

In NTP precision is determined automatically, and it is measured as a power of two. For example when `ntpq -c rl` prints `precision=-16`, the precision is about 15 microseconds (2^{-16} s).

If you like formal definitions, consider this one: "Precision is the random uncertainty of a measured value, expressed by the standard deviation or by a multiple of the standard deviation."

Q What clock precision does it advertise through the SNTP protocol? (See RFC 4330: Precision is an eight-bit signed integer used as an exponent of two, where the resulting value is the precision of the system clock in seconds. This field is significant only in server messages, where the values range from -6 for mains-frequency clocks to -20 for microsecond clocks found in some workstations)

A From Keith (19 Sept 2013) I ran Automachrom against both a Model 9483 and a Model 9383, and every time I grabbed the data from both units, this value was a "-19".



What I didn't know is if this value changes under different scenarios (such as not synced or synced to itself). So I went to a 9483 on the Internet that isn't synced to anything. Precision was consistently "-20". I then synced it to itself and it stayed a constant "-20".

So the precision appears to be around "-19" and "-20".

****NTP Status graphs**

The graphs displayed in the NTP section have dynamic vertical scales. The bottom scale is the number of seconds since UTC midnight. The graph shows about 22 hours across. The vertical scales vary depending upon the actual error values so pay close attention to the labeling. Above a certain value, a decimal notation is used (such as 0.01 seconds). Once the error value decreases, the values change to scientific notation (such as 2e-06).

The scientific breakdown is as follows:

0000.000000001= 1ns or 1e-09
0000.000001000 = 1microsecond or 1e-06
0000.000010000 = 10 microseconds or 1e-05
0000.000100000 = 100 microseconds or 1e-04
0000.001000000 = 1 millisecond or 1e-03
0000.010000000= 10 millisecond or 1e-02
0000.100000000= 100 millisecond or 1e-01
0001.000000000 = 1 second or 1e+00
0010.000000000 = 10 Seconds or 1e+01
0100.000000000 = 100 Seconds or 1e+02
1000.000000000 = 1000 Seconds or 1e+03

Or 0000.000020000 = 20 microseconds or 2e-05

FTP of Statistics will result in a text file full of the NTP info. See <http://www.eecis.udel.edu/~mills/ntp/html/monopt.html#types> of a description of this data.

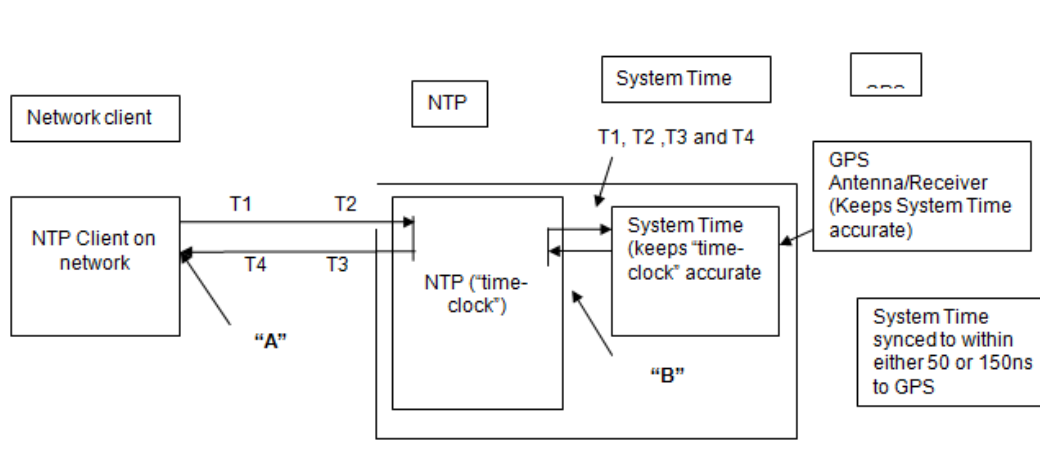
Block diagram/system description of an NTP server / NTP operation (tailored for SecureSync)

The best way to think of the NTP server is to think of it as an employee punch-in/out "time-clock". Its primary role is to timestamp when the NTP packets are received from the NTP client and when they go back out to the client. In order for the "time-clock" to be able to provide the "employer" with accurate times of when their "employees" arrive and depart, the "time-clock" needs to be kept synced to some external reference.

In the case of the Spectracom NTP server, the "time-clock" (NTP) inside of the NTP server is being kept accurate, by syncing NTP to GPS. So, the NTP indications you see on the NTP/Status page is displaying how accurately aligned the "time-clock" is to its external reference.

When the NTP clients ask for the time, they are essentially "employees" that need their packets time-stamped. The NTP server receives the time stamp and provides a timestamp for when it arrived. It then passes it right back to the NTP client with another time stamp for when it's to go back out (the NTP server doesn't hold the packet for any reason. It just time stamps it and sends it back out to the NTP client that requested the time). So, when the "employee" (NTP client) receives the NTP packet back, it knows what time the "time-clock" received it and what time it sent it back out. Based on the NTP client's time stamps and the NTP server's time stamps, NTP can calculate how long it took for the packets to transit between the client and the NTP server, in order to compensate for this delay. It also can determine how much time offset is between the "employee's watch" (NTP clients current time) and the real-time "time-clock" (NTP server).

The NTP packet exchange between the NTP client and NTP server results in a total of four time-stamps, commonly referred to as T1, T2, T3 and T4. Below is a depiction of these four time-stamps:



In the picture above is also a letter "A" and a letter "B". "A" and "B" represent where NTP calculations of delay, offset and jitter are being performed. "A" shows that the NTP client is performing its own calculations for the packet delays between itself and the NTP Server (The NTP server is not performing any calculations for this path delay. It's just letting the client know what time the NTP server received the NTP packet and what time it sent it back to the NTP client. NTP that is running in the client then performs all of the necessary calculations (path delay, jitter and offset) and compensates for these measured delays.

Letter "B" represents the NTP "time-clock" measurements that are also being simultaneously performed in order to keep NTP ("time-clock") in the NTP server accurately aligned to its "System Time" (which is held very accurately synced to GPS). The "B" NTP measurements are what are displayed in the NTP/Status page of the NTP server's web browser. Since all of the measurements for "A" are performed in the NTP client and not in the NTP server at all, the NTP server has no idea what these calculations end-up being. So, it can't display any of these calculations in the server's web browser. However, the NTP server is also performing its own calculations of path delay, offset and jitter, so it can display these values (These are the <1ms values you referred to in your earlier email).

The NTP path delay is the result of NTP measuring the time difference between T1 and T2. Since NTP can only calculate path delay in one direction only, it assumes the path delay is the same between T3 and T4 as it is between T1 and T2. If they aren't the same (due to either network hops in between or packet collisions that may occur during heavy network loading), the NTP's calculations of the path delay will not be as accurate. This results in higher path delay measurements and therefore higher jitter and offset values.

The difference between letters "A" and "B" is that the "A" packets have to deal with the network environment (such as changes in routing because of network hops, packet collisions, etc) while "B" is a "direct-connect" of NTP to its reference (System Time). This is why the NTP Status page of the web browser is able to show the path delay, jitter and offset values of NTP as typically much less than 1ms. It also shows why the calculated path delay values will be much higher in the NTP client.

The path delay, offset and jitter measurements in the NTP client ("A") are going to be based on many factors, such as how well the path delays can be measured (this is where having many network hops and packet collisions due to network loading come into play) and how soon after the departure/arrival of the T1 and t4 time stamps at the NTP client can be time stamped by the NTP client (this is where PC loading comes into play- if the PC is too busy, it may delay in placing its T1/t4 time stamps on the packet after it arrives, thereby throwing off the accuracy of the path delay measurements).

NTP Manycast mode

- Supported with NTP Expert mode in SecureSync and 9483 (not supported in earlier products).
- Refer to :\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert Mode-Broadcast and Multicast

Manycast Scheme

Manycast is an automatic server discovery and configuration paradigm new to NTPv4. It is intended as a means for a client to troll the nearby network neighborhood to find cooperating servers, validate them using cryptographic means and evaluate their time values with respect to other servers that might be lurking in the vicinity. It uses the grab-n'-drop paradigm with the additional feature that active means are used to grab additional servers should the number of associations fall below the maxclock option of the tos command.

The manycast paradigm is not the anycast paradigm described in RFC-1546, which is designed to find a single server from a clique of servers providing the same service. The manycast paradigm is designed to find a plurality of redundant servers satisfying defined optimality criteria.

A manycast client is configured using the manycastclient configuration command, which is similar to the server configuration command. It sends ordinary client mode messages, but with a broadcast address rather than a unicast address and sends only if less than maxclock associations remain and then only at the minimum feasible rate and minimum feasible time-to-live (TTL) hops. The polling strategy is designed to reduce as much as possible the volume of broadcast messages and the effects of implosion due to near-simultaneous arrival of manycast server messages. There can be as many manycast client associations as different addresses, each one serving as a template for future unicast client/server associations.

A manycast server is configured using the manycastserver command, which listens on the specified broadcast address for manycast client messages. If a manycast server is in scope of the current TTL and is itself synchronized to a valid source and operating at a stratum level equal to or lower than the manycast client, it replies with an ordinary unicast server message.

The manycast client receiving this message mobilizes a preemptable client association according to the matching manycast client template. This requires the server to be cryptographically authenticated and the server stratum to be less than or equal to the client stratum.

It is possible and frequently useful to configure a host as both manycast client and manycast server. A number of hosts configured this way and sharing a common multicast group address will automatically organize themselves in an optimum configuration based on stratum and synchronization distance.

The use of cryptographic authentication is always a good idea in any server discovery scheme. Both symmetric key and public key cryptography can be used in the same scenarios as described above for the broadcast/multicast scheme.

**Accuracy of NTP in Holdover (Oscillator free-run specs)

(Note – this Engineering document has not been maintained and is outdated (instead refer to table from SecureSync manual below)

<I:\Engineering\Products\ProductPerformanceSpecs5.xls>

Oscillator typical Holdover accuracies

Oscillator Type	Typical Error Rates after 4 hrs	Typical Error Rates after 24 hrs	after 7 days (nominal)	after 30 days (nominal)
Low Phase noise Rb (Rubidium)	0.2 microseconds (nominal)	1 microseconds (nominal)	7 microseconds	31 microseconds
Rb (Rubidium)	0.2 microseconds (nominal)	1 microseconds (nominal)	7 microseconds	31 microseconds
High performance OCXO	0.5 microseconds (nominal)	10 microseconds (nominal)	70 microseconds	310 microseconds
Standard OCXO	1 microseconds (nominal)	25 microseconds (nominal)	175 microseconds	775 microseconds
TXCO	12 microseconds (nominal)	450 microseconds (nominal)	3150 microseconds (3.1 milliseconds)	13,950 microseconds (13.950 milliseconds)

Table 2-9: Estimated Oscillator Error Rates during Holdover

Falseticker vs Truechimer / NTP sanity check (time change of greater than 1000 seconds occurs while NTP is running)

- `ntpq -> associations` will report the NTP server is “insane” if the sanity check fails.

“Falseticker” vs “Truechimer” (opposites of each other)

Q. What is a Falseticker

A GREAT question. falseticker is a specific word associated with NTP. Below is the definition, per <https://docs.ntpsec.org/latest/ntpsspeak.html> Note that "Mills-speak" at the beginning of the definition below is referring to Dr. David Mills, who created NTP...

falseticker

“Mills-speak for a timeserver identified as not reliable by statistical filtering. Usually this does not imply a problem with the timeserver itself but rather with highly variable and asymmetric network delays between server and client, but firmware bugs in GPS receivers have produced falsetickers.”

Email from Dave Sohn (11/21/12) NTP should generally operate with three or more servers defined, such that issues on any given server will not cause problems downstream. If a SecureSync is configured with three or more servers, and a single server started reporting very inaccurate time, that server would be disqualified as a “false-ticker” until it recovered and started reporting correct time again.

In a SecureSync with a single server entry, the server with very inaccurate time would still be disqualified as a “false-ticker” and not synchronized against. However, if the condition persists NTP will eventually shutdown as it has no servers present to operate. NTP will then restart, and the unit would now synchronize with the falsely reporting server. That mechanism is in place to allow the SecureSync to resynchronize using NTP if its time has been set beyond the normal bounds for NTP to recover. These sorts of issues are the reason why the recommendation is to include at least three different sources for the NTP time.

NTP has two input references, and both are being rejected

Email from Dave Sohn: If there are only two references for NTP and they don't agree with each other or the system itself, it is possible for them both to be declared falsetickers.

Q. What is a Truechimer

Truechimer is a specific word associated with NTP. below is the definition, per <https://docs.ntpsec.org/latest/ntpsspeak.html> Note that "Mills-speak" at the beginning of the definition below is referring to Dr. David Mills, who created NTP...

truechimer

Mills-speak for a timeserver that provides time believed good, that is with low jitter with respect to UTC. As with a falseticker, this is usually less a property of the server itself than it is of favorable network topology.

Time after initial boot-up for NTP to sync as Stratum 1 (such as in a mobile environment)

TSync-PCIe boards

Email KW sent to Aeroflex regarding mobile mode versus stationary mode (12/9/10)

To begin, there are two main types of GPS receivers. There are GPS receivers that emphasize their positional accuracies, but don't care too much about timing accuracies. These types of receivers are typically used in consumer equipment, because you don't need to know exactly what the time is while you are driving down the road. The other main type of GPS receivers are known as timing receivers. Timing receivers still need to calculate their location in order to provide very accurate timing on its outputs. However, it doesn't need to put extensive processing towards calculating its position in order to provide very accurate timing. Since the main purpose of the TSync-PCIe board (as well as our other products) is to provide very accurate timing, these are the type of GPS receivers we use in our equipment.

Timing GPS receivers put their emphasis on accurately calculating time and PPS output. In order to do this, they like to calculate their location, lock it in and then use this position to calculate distances and of the satellites its tracking. This allows them to get the best estimate of the time and PPS. In stationary mode, the position is calculated and then locked in. In mobile mode, the position can't be locked in because the receiver is likely to be moving and the position to be updating on a constant basis. So, the ability to provide very accurate timing outputs is inherently slightly degraded while in the mobile mode.

Another important concept to understand is that the GPS satellites do not operate in UTC time scale (you can think of UTC as GMT time, though they aren't exactly the same thing). GPS has their own time scale they use, which does not directly correlate to the UTC time scale that we often use to know what time it is. There is a known offset value between these two time scales. And this offset is not a fixed value. Each time a leap second occurs in the UTC time scale, this offset between GPS time and UTC increases by a value of one. Luckily GPS transmits this value in part of a continuous 12.5 minute message. In order for the TSync board to know what this current offset value is, so that we can convert GPS time to UTC time, we have to receive it from the GPS message. If the value was assumed as one value, but a leap second occurred since the last time it was received, the timing board calculations for time would be one second off and a time jump would have to occur.

In order to prevent the one second time jump from potentially occurring after the TSync-PCIe board has declared sync, the TSync-PCIe boards do not declare Sync status until it has read this particular bit (known as the "UT1 correction") in the loop of data that is constantly broadcasted by each and every GPS satellite.

In order to declare Sync status, the position has to be known, the 1PPS has to be stabilized and this UT1 correction factor value needs to be known (so the current GPS time to UTC conversion can be accurately calculated each second). Once these requirements have been met, the internal oscillator can start to be disciplined to the incoming PPS data and the Sync status can be achieved. As I mentioned, the board can't declare sync until it also knows the UT1 correction value. The value is included in a continuous 12.5 minute loop (my previous email said 12.5 minutes- I meant to say 12.5 minutes). Once the bit has been read, it's then known. The "variable" in how long it takes to sync is dependent upon where the message is at when the GPS receiver is starting to obtain this loop from one of the satellites. If it happens to start obtaining it just before the data is transmitted, it has it right away. However, if it just missed this bit, it has to wait almost 12.5 minutes for it to finish the loop, start over again and get back to the location of where this information is provided in the transmitted message.

In order to calculate position and stabilize the PPS (other requirements to declare sync), the receiver has to be continuously tracking at least four satellites. This is the minimum number of satellites needed to calculate a 3-D fix. If the view of the sky is completely unblocked, there should be no less than four satellites in view at all times, no matter where you are. However, if any view of the sky is partially blocked, the number of satellites in view may be affected. It may have trouble continuously tracking all four minimum satellites.

In standard (default) mode, in addition to needing to read the UT1 correction bit, it needs to initially obtain the whole 12.5 minute message in its entirety before the board declares sync. This is during the GPS survey which is needed to lock in position. The GPS survey process takes about 34 minutes to complete. Once the survey has initially completed, the data is stored, so as long as the

board is not relocated, the survey doesn't need to occur again after each power-up, unless the board is relocated. So the first sync after initial install, while in standard mode, can take about 35 minutes or so after power-up. However, when the board is configured for mobile mode (mode is set to continuous and the dynamics code has also been changed from stationary to land, sea or air) the survey is not performed, because the data would be distorted as the position was changed. In mobile mode, the board should always declare sync much faster. But because of the above described variable on where the message is at when the GPS receiver starts decoding it, the sync interval cannot be pre-determined. But, if the receiver is able to track four satellites right away, it should always be able to sync within 12.5 minutes plus a couple of minutes for the board's oscillator to stabilize using the stable 1PPS input from the GPS receiver. If it happens to get the UT1 from the message within a minute or two of it decoding the message, the board will sync up in just a few minutes. But if it just missed the bit, it may be another 12-13 minutes before it gets the bit for the first time and then sync will occur within a couple of minutes from there!

That's the basics of GPS sync operation. Now for the specific answers to your questions.

The old email explains 12.5 of the 30 minutes, though it never made much sense to me since consumer hardware doesn't take that long to initialize but they aren't trying for perfect times. On the other demo system yesterday I also saw a sync delay of at least 15 minutes and probably more like 20.

I hope the information above explains the differences that you are seeing in the time it takes to sync. In mobile mode, it really depends on where the Ephemeris data message is when the message is started to be decoded by the GPS receiver.

Acquisition Time (cold start)

- <46 sec (50%), <50 sec (90%)

This is the expected time for the GPS receiver to start tracking satellites once the receiver is powered up (assuming the GPS antenna is attached, and the antenna has a clear view of the sky). The spec says that 50% of the start-ups, it should be tracking satellites in less than 46 seconds. But in 90% of the start-ups, it should be tracking satellites in less than 50 seconds.

- Q. However, we are seeing it take somewhere from 8 to 30 **minutes** from the power on time before the green LED goes on. There seems to be a very big discrepancy. What is happening? How long should we count on waiting before we get a GPS fix?
- A. As described above, just tracking satellites does not meet the requirement for sync. So this time has little to do with time to sync, other than the faster the receiver can start tracking satellites, the faster the requirements can start to be met. If it took 5 minutes for the receiver to start tracking, it would add 5 additional minutes to the time it takes for it to declare sync. The time to sync is also shortened while completely in mobile mode, because the GPS survey does not get performed while in mobile mode. As described in Section 4 of the attached document, both the receiver mode and the dynamics mode have to be changed to be in mobile mode. Changing the receiver mode but keeping the dynamics code as stationary likely confuses the receiver and will likely affect its operation.

We received the card and it is working. We found that we needed to change the Dynamics mode from 3 to 0. However, it does bring up questions that I do not find the answers for in the manual:

- 1) What effect does the Dynamics mode have? i.e. what is the difference in receiver effect for
 - a. GL_DYN_LAND
 - b. GL_DYN_SEA
 - c. GL_DYN_AIR

The three mobile mode dynamics codes (land, sea and air) seem to have very little outward appearance on the performance of the GPS receiver. They do not affect any "rules" outside of the GPS receiver. Our belief, based on information received from the vendor of the GPS receivers, is that these codes likely set up constraints in algorithms inside the GPS receivers. They likely change the limitations of factors based on anticipated movement of the receiver (such as expected altitudes, speed, and other movements of the GPS receiver). By limiting what is expected to be experienced while the receiver is in motion, it can probably fine tune its performance even better. For example, it wouldn't expect to see 30,000 feet of elevation in land and sea mode, by it will in air mode. The same concept would apply with velocity.

- 2) What is the difference in the dynamics mode algorithm selection:

GL_MODE_1SAT (Single Satellite mode –not recommended for use)

GL_MODE_STND ("Standard" for Stationary mode. Factory default)

GL_MODE_CONT (“Continuous” for Mobile mode. Must also change the Dynamics mode to land, sea or air)
GL_MODE_TIME (N/A for TSynC-PCle. For use with SecureSync SAASM GPS receiver)
GL_MODE_STBY (N/A for TSynC-PCle. For use with SecureSync SAASM GPS receiver)
GL_MODE_SELF (N/A for TSynC-PCle. For use with SecureSync SAASM GPS receiver)

Regarding the receiver modes, only the first three apply to the TSynC-PCle boards. 1SAT is for “Single Satellite Mode”. This mode is a worst-case mode that should only be used when stationary and it’s impossible to track at least four satellites, but Sync is still allowed to occur. With less than four satellites tracked, position cannot be accurately calculated. An error in position can result in significant time errors (one of our customers was using this mode in a different product. The product was synced to only one satellite but had about a 20 minute time error because after months of operation, it never tracked four satellites and so the position was completely unknown).

GL_MODE_STND is for stationary position where the platform is not moving and it’s desired to provide optimum timing. In this mode, the 34 minute GPS survey will be performed to lock in an accurate position so timing capabilities can be optimized/

GL_MODE_CONT is for mobile mode. The receiver knows it will be moving, so it does not perform the GPS survey. Because the position cannot be locked in with a GPS survey, the timing outputs are slightly degraded while in this mode. This mode still requires four satellites, so the position can be continuously updated.

The last three modes (**GL_MODE_TIME**, **GL_MODE_STBY** and **GL_MODE_SELF**) are not applicable to the TSynC-PCle board. This same driver is also used in our SecureSync NTP server appliance. These last three modes are used with the specialized SAASM GPS receivers that can be used in the SecureSync appliances (SAASM receivers are used by our government and military applications).

SecureSync/NetClock 9400 series

Note: Software version 4.5.N reduces the time it takes to reach Stratum 1 after System Sync (no matter what reference is used to sync SecureSync

Email from Dave Sohn (7/17/11) regarding this new version: “Total time from startup to NTP Stratum 1 sync is about five minutes”. (includes about 3 minutes to get GPS sync)

Q. In Stationary mode, how long does the SecureSync take to do the GPS survey, then sync to it and output valid NTP time packet (with Stratum 1)?

A) New location

In a new location (and with the GPS receiver configured for stationary mode) the GPS survey needs to first be performed to lock its current position. The GPS survey starts after the GPS receiver is tracking at least four satellites (usually within just a couple minutes after power-up). The GPS survey takes about 34 minutes (2000 seconds) to complete, if the GPS receiver continues to track at least four satellites. The System Time declares Sync (as indicated by the front panel Sync light going solid green) within a minute or two of completing the GPS survey.

Once the GPS survey has been completed and Time Sync has been declared, it takes NTP about 15 minutes or so to sync to Stratum 1 (note that the time it takes for NTP to sync to Stratum 1 is not a set amount of time. It will vary each time NTP needs to resync, but will typically be around 13-15 minutes, after Time Sync occurs).

B) Same location

If the GPS receiver is configured for stationary mode, the GPS survey was already completed and SecureSync is still in the same location as it was in when the GPS survey was first completed, the GPS survey process does not need to occur, but it takes up to 12.5 minutes after power-up to achieve Time Sync. Then NTP will sync about 15 minutes thereafter. In order for SecureSync to re-declare time sync, the GPS receiver has to first be tracking four satellites again and it also has to read a particular value from the GPS satellites. This value is known as the UT1 correction factor, which indicates the time difference between GPS time and UTC time. We need to obtain this important value from GPS before we can go into sync.

This particular value is transmitted by the GPS satellites in a message that repeats every 12.5 minutes. Depending

on where the satellite message is in the 12.5 minute time span in relation to when the GPS receiver starts acquiring this transmitted signal will determine how long it takes for the GPS receiver to obtain this value. If the value happens to be transmitted just after it starts to receive this message, it will have it almost right away. However, if it just missed it, it will have to wait up to 12.5 minutes for this value to be repeated again. Then, once it receives this value, SecureSync can then declare time sync. This value needs to be obtained before time sync occurs in order to verify a leap second has not occurred while SecureSync was powered-down.

Q. In stationary mode, if the reference input is IRIG-B, how long does it take before it can output valid NTP time packet (stratum 1)?

A "Stationary mode and mobile mode" only apply to the GPS receiver input reference. Neither of these modes apply at all to IRIG input. With IRIG input applied and being the selected input reference, SecureSync will achieve Time Sync in just a couple of seconds. Then, NTP will be synced and Stratum 1 within about 15 minutes or so from there.

Q. If we use stationary mode when the aircraft is parked on the ground to sync with the GPS and get stratum 1 status, then when it is in flight and we need to recycle the power of the SecureSync, how can we switch to the mobile mode on the air to get it resync with the GPS again in motion? Can we do it from the front panel control or have to login to switch it? and how?

A If SecureSync is installed in a mobile platform (such as a plane), we only recommend configuring the GPS receiver for mobile mode once, and then leaving it configured for this mode. We do not recommend switching back and forth between mobile and stationary modes.

Mobile mode can only be activated via the web browser.

If the SecureSync happens to be power-cycled in flight, and GPS is the input reference, as described above, time Sync will occur within about 13 minutes and NTP will be resynced about 15 minutes thereafter. With IRIG input, it will resync almost immediately after power cycle and NTP will be synced in about 15 minutes.

Q. In the Mobile mode, how long does it take to sync to the GPS and get to stratum 1 status?

A Mobile mode is similar to stationary mode, after the GPS survey has already been completed (as described in Number 1B). Mobile mode eliminates the 34 minutes-2000 seconds it takes to perform a GPS survey, each time the GPS receiver is in a new location. However, just like when the SecureSync is powered-up in the same location, after a GPS survey has already been completed, the GPS receiver still needs to start tracking at least four satellites and needs to obtain the UT1 correction factor, before Time sync can be achieved. After the GPS receiver is tracking at least four satellites, it can take up to 12.5 minutes for it to obtain this important value. The actual time it will take to get this value, once its tracking four satellites, will be based on where the message is when the GPS receiver starts obtaining this message. It may only be seconds, or it could be as much as 12.5 minutes. Then, NTP sync can start to occur. NTP will be in sync about 13-15 minutes later.

In Summary, after power-up has completed, the GPS receiver should be tracking at least 4 satellites within just a couple of minutes. Up to about 13 minutes later, SecureSync is in sync. Then, about 15 minutes later, NTP will be in sync. Being in Mobile mode reduces the overall time for NTP to sync as Stratum 1 from around 45 minutes (as it is when the receiver is in stationary mode and at a new location-GPS survey not yet completed), to a varying value of anywhere between like 15 minutes best-case to around 30 minutes or so, worst-case.

As you can see from the details above, many variables determine when NTP will be at Stratum 1 after each power-up. There is no set time that this can occur. This time will vary each time SecureSync is powered-up and will vary widely based on the configuration of the GPS receiver (stationary versus mobile modes) or whether IRIG or GPS is the input reference, and will also vary widely (up to 12.5 minutes) depending on where the UT1 correction value is in the message, based on when the GPS receiver starts obtaining the satellite message

NetClock 9300 and 9200 series

****NTP transmission modes- Anycast, Broadcast and Multicast modes**

NTP AnyCast mode

<http://en.wikipedia.org/wiki/Anycast>

NTP Broadcast/Multicast modes

The Model 9100/9200/9300 support Broadcast mode. They do not support the multicast mode, even though we refer to broadcast mode as multicast. NTP broadcast mode send NTP data in one direction to all of the PCs on the network via the network's broadcast address.

True "multicast mode" consists of a range of reserved IP addresses used by various devices. From: <http://www.iana.org/assignments/multicast-addresses/> and (http://en.wikipedia.org/wiki/Multicast_address), the multicast addresses are in the range 224.0.0.0 through 239.255.255.255. The range of addresses between 224.0.0.0 and 224.0.0.255, inclusive, is reserved for the use of routing protocols and other low-level topology discovery or maintenance protocols, such as gateway discovery and group membership reporting. Multicast routers should not forward any multicast datagram with destination addresses in this range, regardless of its TTL. In order to support this mode, we would need an address assigned to Spectracom and the customer would need to be able to enable this address inside the time server.

NTP Multicast mode (SecureSync supports in Expert Mode)

Regarding the NTP multicast mode, on the website page of: <http://doc.ntp.org/4.1.2/confopt.htm>, I found the following information about NTP multicast mode:

Broadcast/Multicast Modes

From: <http://www.eecis.udel.edu/~mills/ntp/html/assoc.html#broad>.

NTP broadcast and multicast modes are intended for configurations involving one or a few servers and a possibly very large client population. Broadcast mode can be used with Ethernet, FDDI and WiFi spans interconnected by hubs or switches. Ordinarily, broadcast packets do not extend beyond a level-3 router. Where service is intended beyond a level-3 router, multicast mode can be used. Additional information is on the [Automatic NTP Configuration Options](#) page.

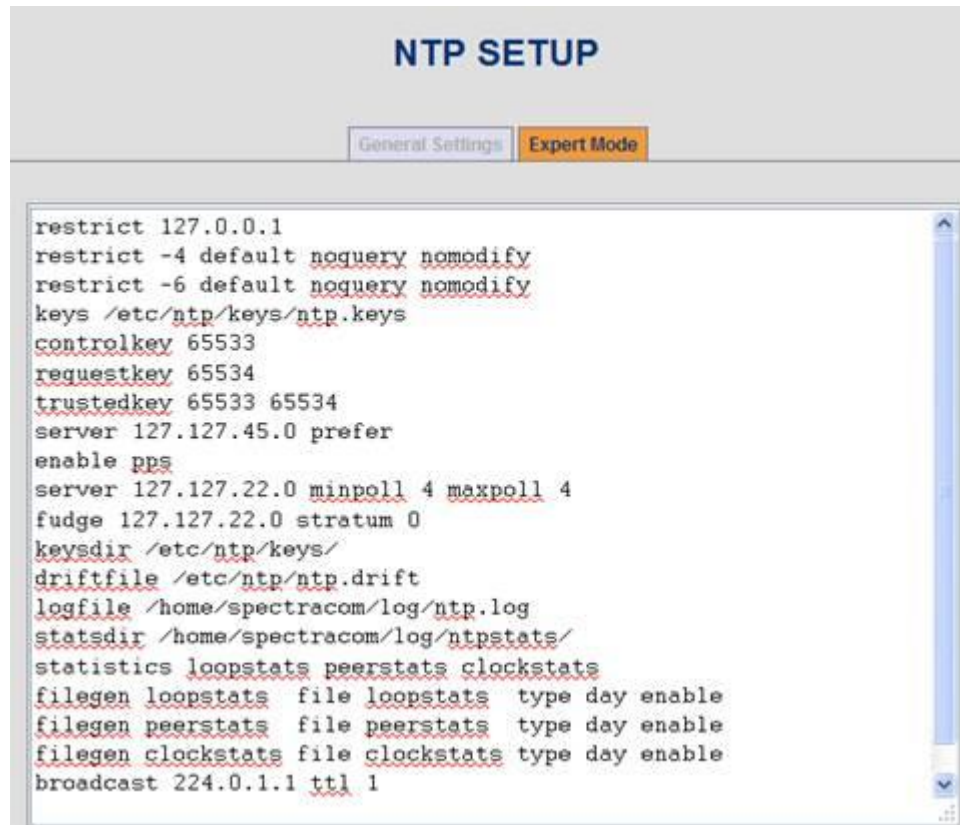
A server is configured to send broadcast or multicast messages using the broadcast command and specifying the subnet address for broadcast or the multicast group address for multicast.

NTP has a dedicated NTP multicast address. It is 224.0.1.1 (port 123). Apparently, this can be changed, if desired, depending on how the Expert Mode is configured. The command to enable multicast mode in Expert Mode is "broadcast".

To configure SecureSync to multicast NTP packets, append the following line to the end of the Expert Mode window (as shown in the screenshot below):

broadcast 224.0.1.1 ttl 1 (where "224.0.1.1" is the multicast address, and where "ttl 1" is the "time to live" of 1 which keeps the packets on the immediate subnet only).

NTP needs to be disabled and re-enabled after editing the Expert Mode field.



Multicast Transmit interval:

The default interval for multicast packets is once every 64 seconds, unless otherwise specified. The minimum value is once every 8 seconds (when “minpoll 3” is tacked onto the end of the broadcast command).

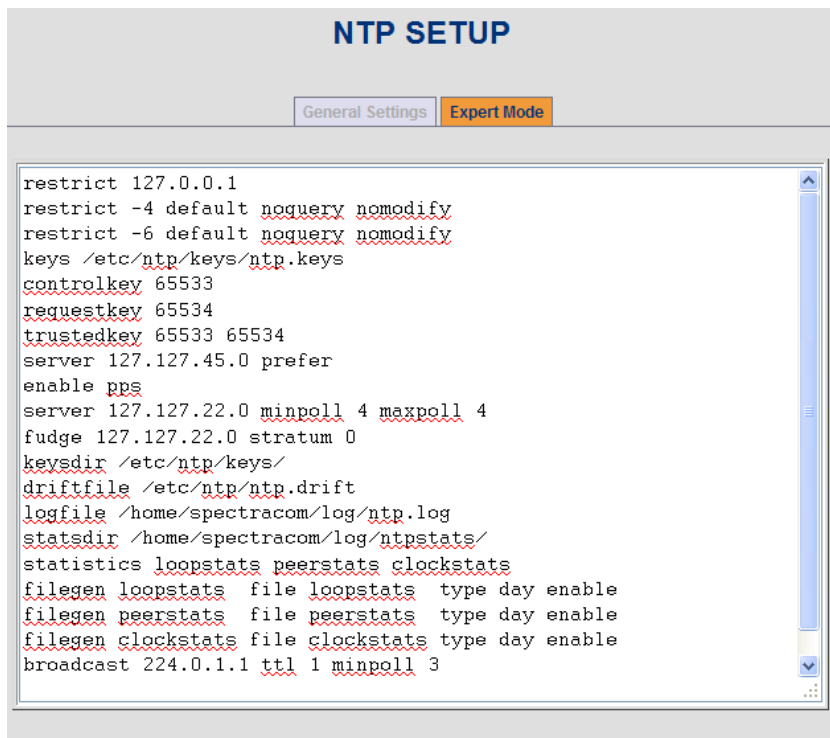
From: <http://www.eecis.udel.edu/~mills/ntp/html/confopt.html#command>

minpoll *minpoll*

maxpoll *maxpoll*

These options specify the minimum and maximum poll intervals for NTP messages, in seconds as a power of two. The maximum poll interval defaults to 10 (1024 s), but can be increased by the `maxpoll` option to an upper limit of 17 (36 hr). The minimum poll interval defaults to 6 (64 s), but can be decreased by the `minpoll` option to a lower limit of 3 (8 s). Additional information about this option is on the [Poll Program](#) page.

To configure the packets to be transmitted every 8 seconds (instead of every 64) append, the following to the end of the broadcast line (as shown in the screenshot): `minpoll 3`



Troubleshooting NTP broadcast mode

If NTP clients don't seem to be syncing to the broadcast packets:

- G) Make sure the NTP client supports broadcast mode (this is not common)
- H) Are there are firewalls blocking port 123.
- I) Run a wireshark capture on same subnet as the NTP server (example NTP broadcast packet below):

525	12.585466	10.2.100.20	10.2.255.255	NTP	NTP broadcast
441	10.269676	10.2.100.44	10.2.100.29	syslog	LOCAL7 NOTICE: spectracom: [system] 1

- J) Are there any switches/routers in between? If there are, they may not pass the broadcast packets
- K) Verify the NTP stratum level of the NTP server is not Stratum 16.
- L) Does the NTP client require MD5 authentication? If it does, Symmetric keys need to be added to the NTP server (the same passphrases that are entered into the NTP client) and one of the keys has to be defined in the NTP broadcast configuration of the NTP server (selects which MD5 key hash to transmit with the NTP packets).

Spectracom NTP server on the Internet (outside of firewall)

IP address= 63.138.60.57 HTTP is disabled, so to get into the browser, type [HTTPS://63.138.60.587](https://63.138.60.587) or [HTTPS://time.spectracomcorp.com](https://time.spectracomcorp.com)

List of available Internet NTP time servers (such as NIST and USNO).

Refer to either the Model 938x or SecureSync NTP Peering documents in [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT](#). These two documents have links and additional info on Internet NTP servers for Stratum 2 sync.

ntpd[714]: too many recvbufs allocated (40)

(From <https://lists.ntp.org/pipermail/hackers/2003-September/000311.html>)

This error message means that more packets are arriving than ntpd has receive buffers for, faster than they are

Page | 589

processed. One way for this to occur is if lots of multicast or broadcast NTP packets are being received by your Ethernet interface. (Is it possible that multicast packets are getting propagated further than intended?) In xntpd 3-5.93e, the number of buffers is (30), and the condition can generate lots and lots of log messages, but the program does not hang in a loop. I suppose many things changed between 3-5.93e and 4.0.99i.

My email to John Burkell on 2/03/11):

This particular NTP log entry is one of the many entries that are sent from the NTP software module running in the Spectracom NTP server. As NTP is not a Spectracom-created software module), we don't have a lot of specific information on this particular entry. However, this entry is typically associated with having one or more NTP time servers the network which have the NTP broadcast mode activated.

The Model 9389's have the ability to simultaneously send NTP packets to individual NTP clients in a unicast mode as well as for the NTP packets to also be broadcasted at a user-specified interval. These packets are sent to the entire network, via the broadcast address. As the NTP broadcast mode is not as accurate as the NTP unicast mode, almost all NTP clients support only the NTP unicast mode. When a user enables the broadcast mode in the NTP server(s) on the network, it causes additional and unnecessary bandwidth to be used, because the NTP clients are all receiving the broadcasted NTP packets, but the clients are completely ignoring them. When the NTP clients desire to receive an NTP time stamp from the NTP server, they will request one and then the NTP server sends it back to just that client via the unicast mode. For this reason, we almost never recommend enabling the NTP broadcast mode (unless you have some abnormal device on the network that requires NTP broadcast data- I have only heard of one device that supported this mode of NT (It was an analog clock hand movement motor which synced using NTP).

It looks like you likely have NTP broadcast unnecessarily enabled in your Model 9389 NTP server(s). If you navigate to the NTP/Status page of the browser you will see an "NTP Reference Status" table on this page. If NTP broadcast has been enabled (by factory default, this mode is disabled) the table will contain at least two horizontal entries associated with the Model 9389. The "Ref ID" column in one horizontal line is typically "GPS" and the other entry is "BCST" (Broadcast) when the broadcast mode has been enabled (as shown below):

NTP Reference Status:

Sync	Host	Ref ID	Stratum	Mode	Type	Auth Status	Last (Sec)	Poll Interval (Sec)	Reach	Delay (mS)	Offset (mS)	Jitter (mS)
	10.2.255.255	BCST.	16	Broadcast	unicast	none	0	16	0	0.000	0.000	4000.000
*	Spectracom	.GPS.	0	Client	local	none	19	64	377	0.000	0.076	0.003

To disable the NTP broadcast mode since it's not needed to be enabled (Note that the NTP unicast mode that is desired/supported by most NTP clients will still operate normally after the broadcast mode has been disabled), navigate to the NTP/General page of the browser. First, at the top of this page, disable the NTP service by selecting "Disabled" and hit Submit. Then, uncheck the "NTP Broadcast every..." check-box and then hit Submit. Then, restart NTP by selecting "Enabled" and press Submit.

After disabling NTP broadcast, the horizontal "BCST" entry in the "NTP Reference Status table" (NTP/Status page) will no longer be present and the "too many rcvbufs allocated (40)" entries will likely no longer be present in the NTP log.

**NTP software:

Reference: <http://www.eecis.udel.edu/~mills/ntp/html/autokey.html> and <http://www.cis.udel.edu/~mills/proto.html>

For more information on Autokey, refer to: \\Roc.spectracom.us\ICS\Engineering\Projects\Lafayette\200 Engineering Documents\Working Papers\WP-033_NTP_Autokey.doc

For SecureSync Autokey Application Note, refer to: [EQUIPMENT\SPECTRACOM](#)

Note: Refer to Mantis cases for any new info on NTP autokey

NTP main versions

Example “main” NTP versions: 4.2.**8**p14, 4.2.**8**p15

- NTP “main” versions (the number before the “p”) ending in **odd numbers** (such as **4.2.7**) are **development** releases.
 - NTP “main” versions (the number before the “p”) versions ending in **even numbers** (such as **4.2.8**) are **stable** releases.
-

PKI (Public Key Infrastructure/Public Key cryptography) for NTP security

Refer to sites such as <http://www.ntp.org/ntpfaq/NTP-s-algo-crypt.htm> and the “NTP Security Model” PowerPoint presentation at: <https://www.eecis.udel.edu/~mills/database/brief/autokey/autokey.ppt>

NTP Security Model

- NTP operates in a mixed, multi-level security environment including symmetric key cryptography, public key cryptography and unsecured.
- NTP timestamps and related data are considered public values and never encrypted.
- Time synchronization is maintained on a master-slave basis where synchronization flows from trusted servers to dependent clients possibly via intermediate servers operating at successively higher stratum levels.
- A client is authentic if it can reliably verify the credentials of at least one server and that server messages have not been modified in transit.
- A client is **proventic** if by induction each server on at least one path to a trusted server is authentic.

****NTP Authentication/NTP Symmetric key (MD5 Authentication)

SHA1 authentication instead of MD5 authentication

- (7/15/13 KW) SHA1 will likely be available for SecureSyncs/9400s in the future. Refer to NTP in the SecureSync section of this document for more info.
- (7/15/13 KW) SHA1 will not likely ever be available for 9300 series, unless we decide to upgrade NTP to a newer version. the current version of NTP does not support SHA1 authentication

- **Refer to:** <http://doc.ntp.org/4.2.4/authopt.html>

FYI- the Symmetric key should be able to be any of the following printable characters (21 through 7F, Hex) with the exception of a space and a “#” sign (these two characters are not allowed). They key length can be up to 20 characters long.

I believe I may have an explanation for you on why the symmetric keying isn’t working, after applying the version 5.1.2 update! It’s based on the answer to the following question...

Are you using any non- alphanumeric keys in the key strings? If you are, can you test the connection using just alphanumeric keys. For my test, I used the keystring of simply “string” and symmetric key worked just fine.

I’m going to look into this further, but I suspect the newer version of NTP that is running in the versions 5.0.0 and above updates may support different non- alphanumeric characters than the earlier version. If the connection works fine with just alphanumeric characters, this will confirm that symmetric key is still working for you in the newer version.

Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
32	20	040	 	Space	64	40	100	@	@	96	60	140	`	`
33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
36	24	044	$	\$	68	44	104	D	D	100	64	144	d	d
37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
40	28	050	((72	48	110	H	H	104	68	150	h	h
41	29	051))	73	49	111	I	I	105	69	151	i	i
42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
59	3B	073	;	;	91	5B	133	[[123	7B	173	{	{
60	3C	074	<	<	92	5C	134	\	\	124	7C	174	|	
61	3D	075	=	=	93	5D	135]]	125	7D	175	}	}
62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
63	3F	077	?	?	95	5F	137	_	_	127	7F	177		DEL

Source: www.LookupTables.com

Ntp.conf file associated with NTP keys/NTP authentication

- Excerpt below is from Dave Sohn (25 Aug 2021) associated with JIRA SSS-1186

The following declarations control MAC authentication:

controlkey key

Specifies the key identifier to use with the ntpq(1) utility, which uses the standard protocol defined in RFC 5905. The *key* argument is the key identifier for a trusted key, where the value can be in the range 1 to 65,535, inclusive.

keys keyfile

Specifies the complete path and location of the key file containing the keys and key identifiers used by ntpd(8), and ntpq(1) when operating with symmetric-key cryptography. This is the same operation as the -k command line option.

trustedkey key...

Specifies the key identifiers which are trusted for the purposes of authenticating peers with symmetric key cryptography, as well as keys used by the ntpq(1) program. Multiple keys on the same line should be separated by spaces. Key ranges can be specified as (first ... last). The spaces around the ... are necessary. Multiple trustedkey lines are supported and trusted keys can also be specified on the command line.

The MAC authentication procedures require that both the local and remote servers share the same key and key identifier for this purpose, although different keys can be used with different servers. The *key* arguments are 32-bit unsigned integers with values from 1 to 65,535.

***FIPS compliancy (FIPS 140-2) for all Spectracom NTP servers

Federal Information Processing Standard (FIPS)

FIPS 140-2: SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>

- FIPS for NTP is associated with NTP authentication (exchanging of shared keys)
- Refer to sites such as https://www.ibm.com/support/knowledgecenter/ko/SSB2MG_4.6.2/com.ibm.ips.doc/tasks/configuring_ntp.htm

Purpose and levels of FIPS 140-2

Note: Information below is from: http://en.wikipedia.org/wiki/FIPS_140-2

N) (<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>)

A) Purpose of FIPS 140-2

The [National Institute of Standards and Technology](#) (NIST) issued the [FIPS 140](#) Publication Series to coordinate the requirements and standards for cryptography modules that include both hardware and software components. Federal agencies and departments can validate that the module in use is covered by an existing [FIPS 140-1](#) or FIPS 140-2 certificate that specifies the exact module name, hardware, software, firmware, and/or applet version numbers. The cryptographic modules are produced by the [private sector](#) or [open source](#) communities for use by the U.S. government and other regulated industries (such as financial and health-care institutions) that collect, store, transfer, share and disseminate [sensitive but unclassified](#) (SBU) information. A commercial cryptographic module is also commonly referred to as a [Hardware Security Module](#). FIPS 140-2 defines four levels of security, simply named "Level 1" to "Level 4". It does not specify in detail what level of security is required by any particular application.

B) Levels of FIPS 140-2

Level 1

Security Level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module (e.g., at least one Approved algorithm or Approved security function shall be used). No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components. An example of a Security Level 1 cryptographic module is a personal computer (PC) encryption board.

Level 2

Security Level 2 improves upon the physical security mechanisms of a Security Level 1 cryptographic module by requiring features that show evidence of tampering, including tamper-evident coatings or seals that must be broken to attain physical access to the plaintext cryptographic keys and [critical security parameters](#) (CSPs) within the module, or pick-resistant locks on covers or doors to protect against unauthorized physical access.

Level 3

In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroizes all plaintext CSPs when the removable covers/doors of the cryptographic module are opened.

Level 4

- Security Level 4 provides the highest level of security.

At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate zeroization of all plaintext CSPs.

Security Level 4 cryptographic modules are useful for operation in physically unprotected environments. Security Level 4 also protects a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the normal operating ranges may be used by an attacker to thwart a cryptographic module's defenses. A cryptographic module is required to either include special

environmental protection features designed to detect fluctuations and zeroize CSPs, or to undergo rigorous environmental failure testing to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module.

FIPS requirements for NTP (NTP authentication)

Per: https://www.stigviewer.com/stig/infrastructure_router/2017-03-08/finding/V-14671

Review the network element configuration and verify that it is authenticating NTP messages received from the NTP server or peer using either PKI or a FIPS-approved message authentication code algorithm. **FIPS-approved algorithms for authentication are the cipher-based message authentication code (CMAC) and the keyed-hash message authentication code (HMAC). AES and 3DES are NIST-approved CMAC algorithms. The following are NIST-approved HMAC algorithms: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256.**

A) Examples of FIPS-compliant hashing algorithms

1. **PKI (Public Key Cryptography) such as NTP autokey**
2. **Cipher-based message authentication code (CMAC) such as AES and 3DES**
 - AES and 3DES are NIST-approved CMAC algorithms.
3. **Keyed Hash Message Authentication Code (HMAC) such as SHA-1, SHA-2 and SHA3**
 - Refer to sites such as : <https://en.wikipedia.org/wiki/HMAC> and <https://www.oit.va.gov/Services/TRM/StandardPage.aspx?tid=5296>

The Keyed-Hash Message Authentication Code (HMAC), as described in Federal Information Processing Standards (FIPS) PUB 198-1, describes a HMAC mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative approved cryptographic hash function, in combination with a shared secret key.

- **NIST-approved HMAC algorithms include the following:** "SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256"

Hash algorithms for HMAC are Approved if they are listed in **FIPS 180-4** (or earlier versions). SHA-1, SHA-256 and SHA-512 are all FIPS Approved secure hash algorithms and the HMAC function based on them are thus FIPS Approved HMAC functions. Using a ...

FIPS 180-4: Secure Hash Standard (SHS): <https://csrc.nist.gov/publications/detail/fips/180/4/final>

B) Examples of NOT FIPS compliant hash algorithms

1. **MD5 authentication**
 - MD5 is not considered FIPS compliant (must use either SHA or SHA1)
 - per: <http://doc.ntp.org/4.2.6/authopt.html>

By default, the message digest algorithm is MD5 selected by the key type M in the keys file. However, if the OpenSSL library is installed, any message digest algorithm supported by that library can be used. The key type is selected as the algorithm name given in the OpenSSL documentation. The key type is associated with the key and can be different for different keys. The server and client must share the same key, key ID and key type and both must be trusted. **Note that if conformance to FIPS 140-2 is required, the message digest algorithm must conform to the Secure Hash Standard (SHS), which requires an algorithm from the Secure Hash Algorithm (SHA) family, and the digital signature encryption algorithm, if used, must conform to the Digital Signature Standard (DSS), which requires the Digital Signature Algorithm (DSA)**

Compliance of Spectracom products to FIPS 140-2

- **Refer to Knowledge Base Article (KBB) about FIPS 140**
https://orolia.my.salesforce.com/kA0C0000000LGXQ?srPos=0&srKp=ka0&lang=en_US (**Note:** internal link only, customers can't reach it. But KBB is also pasted below):

Q Is the time server FIPS 140-compliant?

A The time servers are compatible with FIPS 140-2 compliant systems, but the certification does not apply to these devices because the time server does not store or process user data (the FIPS 140-2 is a specific third-party certification that qualifies a cryptographic module to handle data).

A) FIPS compliance to Spectracom Products, in general (Feb 2011):

Q. I was asked by our customer at the US Patent Office if the 9289 was FIPS compliant. I found no indication we have ever advertised the 9289 as being FIPS. Do any of you know if we do or do not say we are FIPS Compliant as far as the NTP MD5 Authentication goes?

A. Email response from Bill Glase (2/28/11) We are compatible with FIPS 140-2 compliant systems, but the certification does not apply to our device because [SecureSync] does not store or process user data (the FIPS 140-2 is a specific third-party certification that qualifies a cryptographic module to handle data).

By the way, MD5 (as used in the NTPv4 standard) is NOT a FIPS certified algorithm - so if the network time data were required to be FIPS certified for some particular system, it would require a custom protocol on both the client and server side.

B) Specific to SecureSyncs (Dec 2018)

- For more details, refer to "FIPS-140" in: <..\SecureSync CustAssist.pdf>

Q **From Dave L to Apps Engineering team:** I am not able to locate any information or documentation anywhere on this subject. Do you know if we are compliant and/or have any documentation we can send to customers?

A (per Mike Sutton) I have confirmed with engineering and we do NOT claim compliance with FIPS 140-2.

C) Specific to 9300s

- For more details, refer to "FIPS-140" in: <..\NetClockEpsilon.pdf>
- refer to Salesforce case 1439

D) Specific to 9200s

- For more details, refer to "FIPS-140" in: <..\NetClockEpsilon.pdf>
- refer to Salesforce case 2561

****NTP Autokey:

Refer to: <http://doc.ntp.org/4.2.4/authopt.html>

- Automatically handles Symmetric Key usage.
- With Autokey, NTP certificates are exchanged between the stratum levels (known as “certificate chain) before every NTP time stamp exchange occurs. The Stratum 1 reference generates the trusted certificate for the entire chain.
- Packet integrity is checked by MD5 and trusted source is checked with RSA keys.

Q. (Regarding NetClock-not SecureSync) We are experiencing difficulties to full understand the autokey feature. Could you support us in this, maybe with a how-to document, or giving us a working configuration example?

A The engineer that implemented this feature is no longer here. The feature does work but is not commonly utilized. I am forwarding your email to our Engineering department to review and we will get back to you on the use of this NTP feature.

NTP Autokey support in SecureSync (as of March 2013)

- Per Paul Myers- Our NTP Supports security which includes Symmetric Keys and a single configuration of the AUTOKEY ‘IFF protocol’.
- Per Paul Myers -Our AUTOKEY implementation is the most basic and supports IFF Group and Client Keys. We only support RSA keys and MD5 hash.
- NTP Autokey supporting IFF with MD5 digest and RSA keys/certificates implemented and tested.
- The ability to support Groups using a single IFF Group/Client key or Exported Keys to a Group member or a Client only is supported.
- The same group key gets distributed to all devices desired to be part of the Autokey group.

Known limitations/issues with NTP Autokey in SecureSync

- With the NTP update to v4.2.6 starting in Archive version 5.0.0, the generated trusted group key appears to not be downward compatible with earlier versions of NTP running on the clients. Customers may need to upgrade NTP in their clients to be compatible with this group key.
- With the NTP update to v4.2.6 starting in Archive version 5.0.0, NTP no longer supports both a client and group key. Only the group key can be generated. The client key is no longer supported.
- IPv6 with Autokey does not work (at least Archive versions 4.8.9 and below)

Per Paul Myers--Our AUTOKEY implementation is the most basic and supports IFF Group and Client Keys. We only support RSA keys and MD5 hash.

Update for SecureSyncs with v5.0.0 or higher installed (new version of NTP). This may no longer be the case:

From: <http://doc.ntp.org/4.2.0/release.html?advanced=on>

New Features

1. **Support for the IPv6 addressing family is included in this distribution.** If the Basic Socket Interface Extensions for IPv6 (RFC-2553) is detected, support for the IPv6 address family is generated in addition to the default support for the IPv4 address family. **Combination IPv6 and IPv4 configurations have been successfully tested in all protocol modes supported by NTP and using both symmetric and public key (Autokey) cryptography. However, users should note that IPv6 support is new and we have not had a lot of experience with it in various operational scenarios and local infrastructure environments. As always, feedback is welcome.**

- NO SUPPORT of any Identity scheme other than IFF (Mantis case 1130)

- NO Group names or use of other digests or Key Types (DSA) is supported (Mantis case 1130)

Known limitations/issues with NTP Autokey in Model 9300 and 9200 series (as of at least v3.6.1 anyways)

- Supports Group key generation but not Client key generation.

NTP RFCs (Request for Comments)

RFC 4330

RFC 4330 replaces RFCs 2030 and 1769.

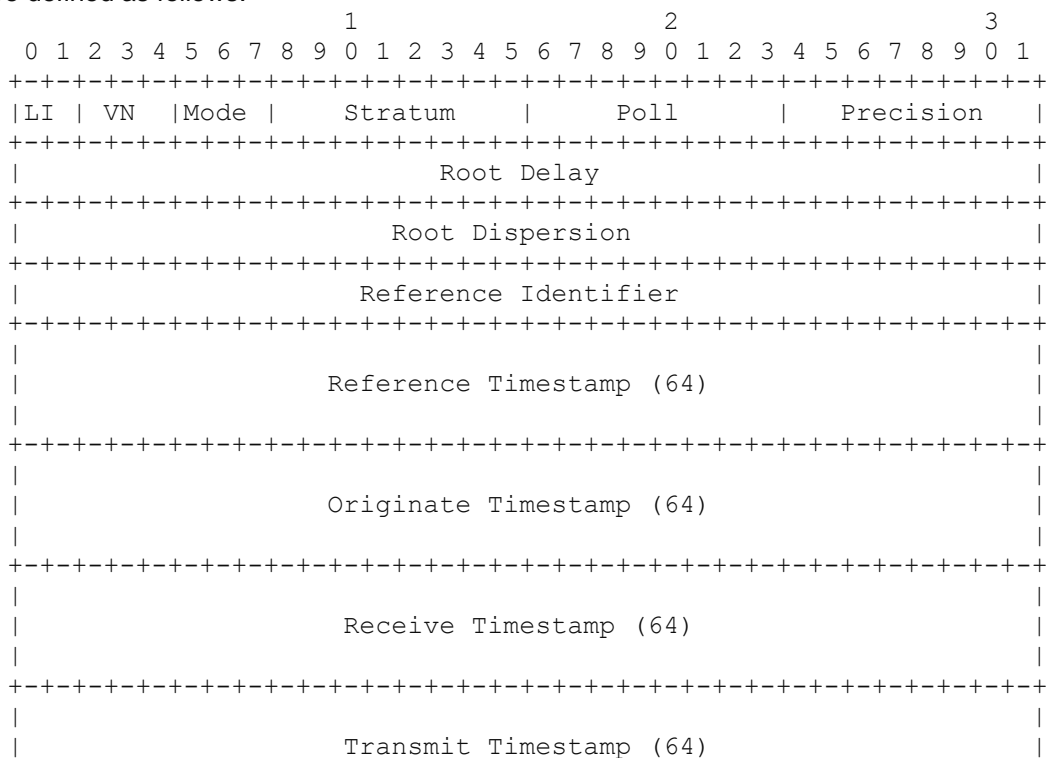
This memorandum obsoletes RFC 1769, which describes SNTP Version 3 (SNTPv3), and RFC 2030, which describes SNTPv4. Its purpose is to correct certain inconsistencies in the previous documents and to clarify header formats and protocol operations for NTPv3 (IPv4) and SNTPv4 (IPv4, IPv6, and OSI), which are also used for SNTP. A further purpose is to provide guidance for home and business client implementations for routers and other consumer devices to protect the server population from abuse. A working knowledge of the NTPv3 specification, RFC 1305, is not required for an implementation of SNTP.

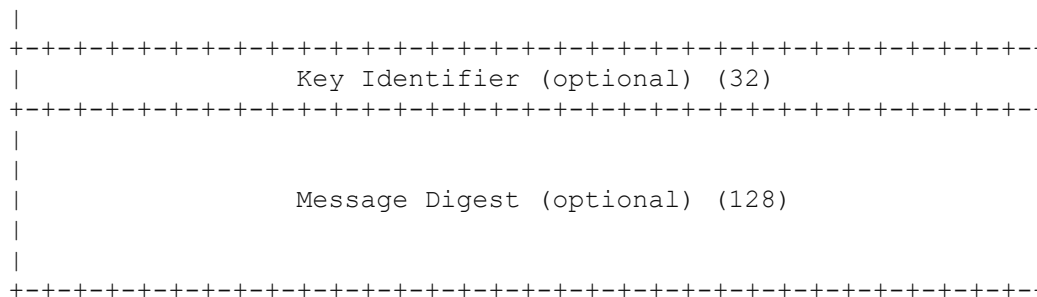
RFC 1305-2030: valid NTP packet lengths

- NTP packets are 64 bits long, unless MD5 is enabled

From RFC 2030 (<http://www.apps.ietf.org/rfc/rfc2030.html>)

Below is a description of the NTP/SNTP Version 4 message format, which follows the IP and UDP headers. This format is identical to that described in RFC-1305, with the exception of the contents of the reference identifier field. The header fields are defined as follows:





Background: Customer is using a NTP Client for VX Works and Time Server is responding that the NTP requests are invalid. Customer sent us an Ethereal capture: Below are Paul's comments about the capture.

- Customer's NTP request was 80 bytes long.
- The normal NTP packet length is 48 bytes. See <http://www.apps.ietf.org/rfc/rfc2030.html>
- The NTP Packet with MD5 hashes are supposed to be 48 bytes for the normal NTP packet and 20 bytes for the Key ID and Hash. Thus, the packet length should be 68 bytes.
- Per David Mills the fields in the packets are to be big-endian order. They need to use an NTP Client which is compatible with RFC 2030 and RFC 1305. Is it possible they are trying to communicate with our SNTP Server in the 91XX units as if it is an NTP 4.x.x server running full-blown NTP from David Mills.

****NTP Burst/iBurst modes**

- **Burst Mode:** 8 packets requested every poll.
- **iBurst mode:** 8 packets requested at NTP startup.

Modified excerpt From: <http://www.eecis.udel.edu/~mills/ntp/html/ntpd.html>:

With this option (iburst) a volley of 8 NTP packets is exchanged between the NTP Server and each configured NTP Server (listed in the "NTP Servers") table to groom the data and set the NTP clock in about ten seconds. If nothing is heard after a few minutes, the daemon times out and exits without setting the clock.

A) iBurst mode for NetClock 9300/9200 series

- NTP iBurst was added as an optional configuration via the browser in the NetClock 9200/9300s starting with Application version 3.6.1 (Jan 2013 time frame).
- For iBurst in 9300/9200 series, refer to: [NTP iburst](#)

B) iBurst mode for SecureSync and NetClock 9400 series

- As of at least Archive version 4.8.8, iburst mode has not yet been added as a web browser selection (though it can likely be activated in NTP expert mode). Mantis case 1948 submitted to consider adding this mode to these products also.

Update: iburst was added in version 5.0.0? NTP can now sync within a couple of seconds if NTP has a valid System Time reference to sync with.

For iburst in SecureSync/9400 series, refer to: [NTP burst/iBurst mode](#)

Electrical substation specs

****IEEE 1613:**

Description: IEEE 1613 is the IEEE standard for **the environmental and testing requirements for communications networking devices in electric power substations**. Service conditions, electrical ratings, thermal ratings, and environmental testing requirements are defined for communications networking devices to be installed in electric power substations. Examples of these devices include radios, encryption devices, port switches, autodialers, modems, Ethernet hubs and switches, routers, gateways, and firewalls. This standard establishes a common reproducible basis for designing and evaluating communications networking devices for use in this harsh environment.

Note from Keith Wing-- As of at least May 2016, I do not know if we are compatible with these specs- But I'm fairly certain that we don't currently state that we compliant. I don't know which of these specs we meet and which specs we don't.

IEC 60945 (Maritime Navigation and Radiocommunication Equipment and Systems)

- Refer to Salesforce Case 247953
- For more info, refer to:
 - [IEC Standards and specs](#) (in the I:/Customer Service folder)
 - Wikipedia: https://en.wikipedia.org/wiki/Environmental_testing

Environmental testing is the measurement of the performance of equipment under specified environmental conditions, such as:

- extremely high and low temperatures
- large, swift variations in temperature
- blown and settling sand and dust
- salt spray and salt fog
- very high or low humidity
- wet environments, waterproofness, icing
- presence of corrosive material
- fungus, fluids susceptibility
- vibrations (airborne and structural), gun fire
- accelerations
- solar radiation
- high and low pressures (especially for aeronautical and space equipment)
- operating at angles (especially for marine, aeronautical and space equipment)
- electromagnetic interference (EMI), ESD, Lightning
- acoustic measurements
- power input variations

Such tests are most commonly performed on equipment used in military, maritime, aeronautical and space applications. See [Environmental test chambers](#) for more information about environmental testing equipment.

Environmental test standards include

- [MIL-STD-810](#), "Test Method Standard for Environmental Engineering Considerations and Laboratory Tests", presently (2010) version G, issued in 2009
- [MIL-HDBK-2036](#), "Preparation of Electronic Equipment Specifications", issued 1999
- [IEC 60068](#), "Environmental Testing", with many parts.
- [IEC 60945](#), "Maritime navigation and radiocommunication equipment and systems – General requirements – Methods of testing and required test results", issued 2002 and due for review in 2007
- [RTCA DO-160](#), "Environmental Conditions and Test Procedures for Airborne Equipment", first published in 1975
- [MIL-STD-461](#), "Department of Defense Interface Standard: Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment (11 DEC 2015)", presently version G.

****IEC 61850: Synchronization of IEC 61850 devices via SNTP (electrical substation automation specifications)**

➤ For more info, refer to:

- [IEC Standards and specs](#) (in the I:/Customer Service folder)
- Wikipedia: http://en.wikipedia.org/wiki/IEC_61850

IEC 61850 is a standard for the design of electrical substation automation. IEC 61850 is a part of the International Electrotechnical Commission's (IEC) Technical Committee 57 (TC57) reference architecture for electric power systems. The abstract data models defined in IEC 61850 can be mapped to a number of protocols. Current mappings in the standard are to MMS (Manufacturing Message Specification), GOOSE, SMV and soon to Web Services. These protocols can run over TCP/IP networks or substation LANs using high speed switched Ethernet to obtain the necessary response times below four milliseconds for protective relaying.

Note from Keith Wing-- As of at least July 2013, I do not know if we are compatible with these specs- But I'm fairly certain that we don't current state that we compliant. I don't know which of these specs we meet and which specs we don't. Hongbo inquired about this spec and Sam Otto forwarded to Dave Sohn for comment.

Email from Dave Sohn to Sam Otto (31 July 13) SecureSync has not been tested or investigated against IEC 61850. I am not aware that we have a copy of the specification to really check against it. Looking at articles on 61850, it looks like there are different levels of time accuracy ranging from T1 (+/- 1ms) to T5 (+/- 1us).

Q (From Sylvain, 1 July 14) Do you know if the SecureSync is conform to this specification: • IEC 61850: Synchronization of IEC 61850 devices via SNTP. I know that we support SNTP but in order to drive some devices that comply to IEC 61850, does the SecureSync comply?

A. (per Dave Lorah 1 July 14) We have had this request one or two times in the past. Here is the answer: The SecureSync does not have compliance with the IEC 61850. It has never been tested against the IEC 61850 standard.

Reply from Sylvain I think it is a pity because we think (Gilles and I) that the SecureSync can do it. And regarding what market we want to address with the SecureSync especially the ENTERPRISE market, I think we will receive more and more this kind of compliance requirement.

I think we should ask R&D and product management to investigate about the need (or not) to qualify the SecureSync against IEC 61850 standard. I have copied them in this way.

Email from Denis to Sylvain (30 June 2014) I don't think we have a copy of that spec here (at least, I don't have one, maybe Gilles does?) I think there are other things in the spec besides timing so we probably cannot claim compliance until we have seen the Spec.

However, I have read that that standard calls for a timestamping resolution of 1 ms. Before PTP came along, IRIG-B was a popular choice for getting that performance. Some vendors also tried using SNTP. While getting SNTP to 1 ms accuracy can be a challenge, it is possible.

See this LinkedIn discussion:

<http://www.linkedin.com/groups/Time-Synchronization-using-SNTP-IEC61850-119621.S.67160841>

If they are simply interested in using SNTP to get their devices within 1 ms, the SecureSync may comply with that, depending on the network. But I don't think that is the same question they are asking....

Newer versions of the standard will push the accuracy requirements into the microsecond range, which is why these people are also interested in PTP.

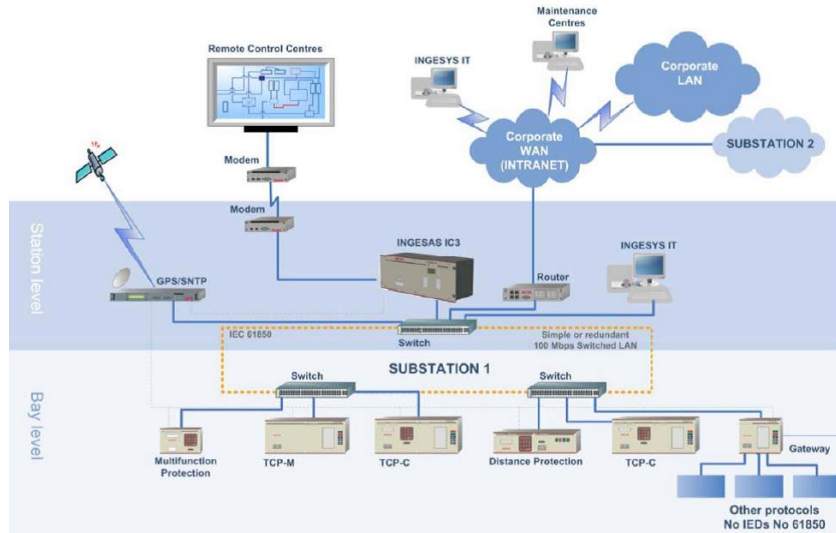
Reply from Gilles (1 July 14) To be more detailed, IEC 61850 is very wide coverage. 10 sub-standards are dealing with everything from architecture/engineering to test/maintenance. I guess customer is expecting IEC 61850-3 ed.2 but not IEC 61850-5 about communication requirements. -3 describes general requirements about communication network and systems for power utility automation.

Main clauses are:

- Environment conditions including EMC in line with IEC 60255 series and IEC 61000-6-5, -4-6
- Ratings
- Design and construction including safety based on IEC 60255-27 that is dedicated to relay and protection

- equipment included in the power grid (not applicable to information equipment)
- Tests
- Marking labelling and packaging
- Rules for transport, storage, Installation, operation and maintenance
- Product documentation

Severity class shall be specified for application: availability, maintainability, climatic range with scale of IEC 60870-2-2 table 1 and 2 and air temp within §3.3.1 pressure within §3.3.2,
The typical grid architecture suggests NTP server is outside IEC 61850 communication network.



I attached a non-last version of IEC 61850-3, but with minor deviation from the version in force.
I also attached an industry presentation of the context of application for IEC 61850 full set.

****NTPSTAT / NTPQ (ntpq -p) / NTPDC**

- NTPQ and NTPDC are special tools for monitoring and controlling NTP
- NTPDC was eliminated in NTPv4.2.8 (software version 5.2.1). Most of the NTPDC commands were rolled into NTPQ with the same names.

ntpstat command

- **ntpstat**: Command to verify a Linux box running NTP is synced, and what its synced with. Example:
synchronized to NTP server (149.20.54.20) at stratum 3
time correct to within 42 ms
polling server every 1024s

NTPQ/NTPDC (Mode 7)

List of CLI commands available for ntpq

- Type **help** <enter> while in ntpq
- For more info on a particular command, type **help command** <enter>

```
ntp> help
ntp> commands:
;config      drefid      mreadlist    readvar
addvars      exit         mreadvar     reslist
aspeers      help         mrl          rl
associations host         mrulist      rmvars
authenticate hostnames    mrv          rv
authinfo     ifstats     ntpversion   saveconfig
cl           iostats     opeers       showvars
clearvars    kerninfo    passassociations sysinfo
clocklist    keyid       passwd       systats
clockvar     keytype     peers        timeout
config-from-file lassociations poll          timerstats
cooked       lpeers      pstats       version
cv           lpassociations quit          writelist
debug        lpeers      raw          writevar
delay        monstats    readlist

ntp> version
```


NTPQ -p /ntpq -p (peers command)

- For a list of available NTPQ commands (such as ntpq -p, the peers command), refer to: <http://www.eecis.udel.edu/~mills/ntp/html/ntpq.html>
- To use NTPQ commands, login to the CLI (RS-232, telnet, ssh) and type **ntpq -p** <enter>.

Example

```
spadmin@Spectracom ~ $ ntpq -p
      remote           refid      st t when poll reach  delay  offset  jitter
=====
PCI_TSYNC(0)      .HOST.        16 l   -   16    0   0.000   0.000   0.000
*10.2.100.177     .TSYN.        1 u    1    8   377   0.220  -0.049   0.254
spadmin@Spectracom ~ $
```

Fields of ntpq -p

- refer to: <https://www.eecis.udel.edu/~mills/ntp/html/ntpq.html>

peers	
Display a list of peers in the form	
(tally)remote refid st t when poll reach delay offset jitter	
Variable	Description
(tally)	single-character code indicating current value of the <code>status</code> field of the <code>peer_status_word</code>
remote	host name (or IP number) of peer
refid	association ID or <code>box_code</code>
st	stratum
t	u: unicast or multicast client, b: broadcast or multicast client, l: local (reference clock), s: symmetric (peer), x: manycast server, s: broadcast server, m: multicast server
when	sec/min/hr since last received packet
poll	poll interval (log ₂ s)
reach	reach shift register (octal)
delay	roundtrip delay
offset	offset of server relative to this host
jitter	jitter

- **Tally (character reporting NTPs current selection capability)**
- refer to the “Tally Codes” section further below for more details

Tally code	Green = (Sync) Red = (Not in Sync) (if the Reach is not 0)	Truechimer (good) or falselticker (bad) (as determined by the Clock Select Algorithm)
*	The Selected Time reference	Truechimer
o	The Selected PPS reference	Truechimer
+	A high quality candidate for NTP reference input that can be selected by NTP as its time reference (Good reference, but not selected)	Truechimer
x	“Falselticker” Listed NTP Peer was discarded from selection (NTP won't select this peer as its reference)	falselticker
-	“Outlier” Listed NTP Peer was discarded from selection (NTP won't select this peer as its reference)	falselticker
(blank)	Source discarded: Failed Sanity check	falselticker

- **refid column shows the current source of synchronization (see details further below)**
- **st column reveals the stratum**
- **t the type (u = unicast, m = multicast, l = local, - = don't know),**
- **poll the poll interval in seconds.**
- **when column shows the time since the peer was last heard in seconds.**
- **reach column shows the status of the reachability register (in octal).**

During a normal startup the registers values are these: 0, 1, 3, 7, 17, 37, 77, 177, 377

an 8-bit left-rotating register. Any 1 bit means that a "time packet" was received. The right most bit indicates the status of the last connection with the NTP server. It is Octal number. Use calculator in programmer interface to translate from OCT to BIN: For example, 377 translates to 11111111. Each 1 means a successful connection to the NTP server. If you just start a NTP service, and it connects successfully with its server, this number will change as follows (assuming connectivity is good):

```
00000001 = 001
00000011 = 003
00000111 = 007
00001111 = 017
00011111 = 037
00111111 = 077
01111111 = 177
11111111 = 377
```


(Delay, offset and jitter in milliseconds).

- **Delay:** indicates the roundtrip time, in milliseconds, to receive a reply
- **Offset:** indicates the time difference, in milliseconds, between the client server and source

Email Keith sent about Offset (24 Jul 17) The NTP Offset is the time offset (reported in milliseconds) between this NTP device and the reference it's directly syncing with (as calculated by NTP). When an NTP client's time source is co-located at the same site and on the same subnet, this offset is usually very low (with ntpd, this value is typically 1 to 10 ms, while the Legacy VelaSync typically provides better NTP performance).

However, if there are several network hops between this NTP client and its NTP sever, the Offset value can become much higher, directly due to asymmetric path delays between the two NTP devices. As NTP can only measure the path delay in one direction, any time differences between this delay and the return path delay cannot be compensated for. So it becomes an automatic time Offset between it and its NTP Time source.

For instance, if the network delay between an NTP client and the Legacy VelaSync is 10 milliseconds in one direction, but due to the variance in return path, the delay in the other direction is only 5ms. NTP is going to account for the original 10ms delay. it can't account for the 5ms difference in the return path, so this results in a 5ms offset between the client and the server.

Other variables can also minimally influence the Offset value (such as hardware time stamping, versus software time stamping). But asymmetric path delays due to multiple network hops in between causing asymmetric delays is usually the biggest factor in how large the NTP offset value will be.

For example, I have seen cases where the Client and Server are located on the opposite sides of the US, and the offset value is in the tens of milliseconds (such as around 90ms or even higher) due to asymmetric path delay, as a direct result of changing network paths in one direction compared to the opposite direction. Minimizing the number of hops between the client and its time server helps to minimize the asymmetric delays that NTP can't account for, thereby decreasing the time Offset between the two devices.

- **Jitter:** indicates the difference, in milliseconds, between two samples

Info below is from <http://nlug.ml1.co.uk/2012/01/ntp-q-p-output/831>

“ntp -c rl” output parameters:

- **precision** is rounded to give the next larger integer power of two. The achieved resolution is thus $2^{\text{precision}}$ (seconds)
- **rootdelay** – total roundtrip delay to the primary reference source at the root of the synchronization subnet. Note that this variable can take on both positive and negative values, depending on clock precision and skew (seconds)
- **rootdisp** – maximum error relative to the primary reference source at the root of the synchronization subnet (seconds)
- **tc** – NTP algorithm [PLL](#) (phase locked loop) or [FLL](#) (frequency locked loop) time constant (log2)
- **mintc** – NTP algorithm PLL/FLL minimum time constant or ‘fastest response’ (log2)
- **offset** – best and final offset determined by the combine algorithm used to discipline the system clock (ms)
- **frequency** – system clock period (log₂ seconds)
- **sys_jitter** – best and final jitter determined by the combine algorithm used to discipline the system clock (ms)
- **clk_jitter** – host hardware(?) system clock jitter (ms)
- **clk_wander** – host hardware(?) system clock wander ([PPM](#) – parts per million)

Jitter (also called timing jitter) refers to short-term variations in frequency with components greater than 10Hz, while wander refers to long-term variations in frequency with components less than 10Hz. (Stability refers to the systematic variation of frequency with time and is synonymous with aging, drift, trends, etc.)

Desire to use Mode 7 queries

- If it's desired to enable Mode 7 queries from anywhere on the network, select the "Allow queries from NTPDC or NTPQ over IPv4" and/or the "Allow queries from NTPDC or NTPQ over IPv6" checkboxes (as applicable) at the top of the "NTP Access" tab
- If there are custom entries added in the Access table (below the list of checkboxes) and it's desired to enable NTPQ/NTPDC, uncheck the Allow queries from NTPDC or NTPQ over IPv4" and "Allow queries from NTPDC or NTPQ over IPv6" checkboxes at the top of this NTP Access tab, and select the individual "Enable Query" checkboxes in the last column of the NTP Access table. These individual checkboxes override the two "Allow queries..." checkboxes at the top of this tab.

```
Linux 3.8.13-gentoo <tul> <2>
tul login: spadadmin
Password:
Spectracom NetClock 9489 Version 5.1.2
spadadmin@tul ~ $ ntpq -p
=====
remote               refid           st t when poll reach  delay  offset  jitter
=====
+PCI_TSYNC<0>        .GPS.           0 l  1   16  377  0.000  0.014  0.002
oPPS<0>              .PPS.           1 l  -   16  377  0.000  0.000  0.002
*10.2.100.93         .GPS.           1 u  7    8  377  0.301 -0.037  0.009
+spectracom.int.     .PPS.           1 u  6    8  377  0.273  0.002  0.008
spadadmin@tul ~ $
```

The graphs displayed in the NTP section have dynamic vertical scales. The bottom scale is the number of seconds since UTC midnight. The graph shows about 22 hours across.

A) Time Offset Graph

- Reports the time offset (in scientific notation) between NTP and its selected reference.

The vertical scales vary depending upon the actual error values so pay close attention to the labeling. Above a certain value, a decimal notation is used (such as 0.01 seconds). Once the error value decreases, the values change to scientific notation (such as 2e-06).

The scientific breakdown is as follows:

1e-09 = 1 ns or 0000.000000001
1e-08= 10 ns
1e-07= 100ns
1e-06= 1 microsecond or 0000.000001000
1e-05= 10 microseconds 0000.000010000
1e-04= 100 microseconds or 0000.000100000
1e-03= 1 milliseconds or 0000.001000000
1e-02= 10 milliseconds or 0000.010000000
1e-01= 100 milliseconds or 0000.100000000
1e+00=1 second or 0001.000000000
1e+01= 10 Seconds or 0010.000000000
1e+02= 100 Seconds or 0100.000000000
1e+03= 1000 Seconds 1000.000000000

Note: If the first digit isn't a "1", multiply the first digit by the "time" value in the table above

Examples

2e-05= 20 microseconds or 0000.000020000 ("2" times "10 microseconds" is 20 microseconds)

5e-06= 5 microseconds or 0000.000050000 ("5" times "1 microsecond" is 5 microseconds)

B) RMS Jitter Graph

- Reports the variance in time offset (in seconds), from one calculation to the next
- **Official definition:** The value reported by NTP is the exponential average of the square root of the sum of the squares of past offset differences

When repeatedly reading the time, the difference may vary almost randomly. The difference of these differences (second derivation) is called *jitter*.

Examples:

0.000002 seconds = 2 microseconds
0.0000019 seconds = 1.9 microseconds
0.0000022 seconds = 2.2 microseconds

C) Frequency Offset Graph

- Reports how much time drift our kernel is experiencing, based on the frequency disciplining of NTP.
- This is the amount of time error our kernel time would have drifted, if NTP was not synced by a reference.
- Our typical frequency offset appears to be around **13 PPM** (about one second per day).

Below is from <http://www.ntp.org/ntpfaq/NTP-s-sw-clocks-quality.htm#AEN1230>

Unfortunately, all the common clock hardware is not very accurate. This is simply because the frequency that makes time increase is never exactly right. Even an error of only 0.001% would make a clock be off by almost one second per day. This is also a reason why discussing clock problems uses very fine measures: One PPM (Part Per Million) is 0.0001% (1E-6).

Real clocks have a frequency error of several PPM quite frequently. Some of the best clocks available still have errors of about 1E-8 PPM (For one of the clocks that is behind the German DCF77 the stability is told to be 1.5 s/day (1.7E-8 PPM). See <http://www.ptb.de/english/org/4/43/432/real.htm> or http://www.ptb.de/en/org/4/44/441/real_e.htm).

****As most people have some trouble with that abstract *PPM* (parts per million, 0.0001%), I'll simply state that 12 PPM correspond to one second per day roughly. So 500 PPM means the clock is off by about 43 seconds per day.**

Examples:

12 PPM = about one second per day of time drift.
69 PPM= about six seconds per day of time drift.
500 PPM= about 43 seconds per day of time drift.

****Ref ID (RefID) (such as .gps, .pps, .init, .drop, .step, .xfac, rtc)**

- Refer to sites such as: <http://www.eecis.udel.edu/~mills/ntp/html/decode.html#kiss>

The following info is from: <http://nlug.ml1.co.uk/2012/01/ntp-p-output/831>

The **refid** can have the status values:

- An IP address – The [IP address](#) of a remote peer or server;
- **.LOCL.** – This local host (a place marker at the lowest stratum included in case there are no remote peers or servers available);
- **.PPS.** – [“Pulse Per Second”](#) from a time standard;
- **.IRIG.** – [Inter-Range Instrumentation Group](#) time code;
- **.ACTS.** – American [NIST time standard](#) telephone modem;
- **.NIST.** – American NIST time standard telephone modem;
- **.PTB.** – German [PTB](#) time standard telephone modem;
- **.USNO.** – American [USNO time standard](#) telephone modem;
- **.CHU.** – [CHU](#) ([HF](#), Ottawa, ON, Canada) time standard radio receiver;
- **.DCFa.** – [DCF77](#) ([LF](#), Mainflingen, Germany) time standard radio receiver;
- **.HBG.** – [HBG](#) ([LF](#) Prangins, Switzerland) time standard radio receiver;
- **.JJY.** – [JJY](#) ([LF](#) Fukushima, Japan) time standard radio receiver;
- **.LORC.** – [LORAN-C](#) station ([MF](#)) time standard radio receiver. Note, [no longer operational](#) (superseded by [eLORAN](#));
- **.MSF.** – [MSF](#) ([LF](#), Anthorn, Great Britain) time standard radio receiver;
- **.TDF.** – [TDF](#) ([MF](#), Allouis, France) time standard radio receiver;
- **.WWV.** – [WWV](#) ([HF](#), Ft. Collins, CO, America) time standard radio receiver;
- **.WWVB.** – [WWVB](#) ([LF](#), Ft. Collins, CO, America) time standard radio receiver;
- **.WWVH.** – [WWVH](#) ([HF](#), Kauai, HI, America) time standard radio receiver;
- **.GOES.** – American [Geosynchronous Orbit Environment Satellite](#);
- **.GPS.** – American [GPS](#);
- **.GAL.** – [Galileo](#) European [GNSS](#);
- **.ACST.** – manycast server;
- **.AUTH.** – authentication error;
- **.AUTO.** – Autokey sequence error;
- **.BCST.** – broadcast server;
- **.CRYPT.** – Autokey protocol error;
- **.DENY.** – access denied by server;
- **.INIT.** – association initialized;
- **.XFAC.** – association changed (IP address changed or lost);
- **.MCST.** – multicast server;
- **.RATE.** – (polling) rate exceeded;
- **.TIME.** – association timeout;
- **.STEP.** – step time change, the offset is less than the panic threshold (1000ms) but greater than the step threshold (125ms).

Specific refid values

A) .INIT

- should only remain “.init” until after about the initial NTP packet return from the SecureSync
- Indicates the NTP mode of the reference has not yet been identified (see additional info further below).
- “.init” is **494e4954** (in hex)
- Indicates NTP is trying to reach the reference for the first time, but can’t initiate communications with this

reference.

Most likely causes:

- The default gateway is not configured correctly, or
- There is a network issue with port 123, or
- NTP symmetric key is being enforced, but not correctly configured in all devices (preventing auth from being successful)

To troubleshoot “.init” refID not changing shortly after NTP has started

- is the “init SecureSync” able to sync any other NTP clients
- Does the “init” SecureSync respond to pings (If no response, likely network issue or problem with the “init” SecureSync)
- perform a **tracert -p 123 xxx.xxx.xxx** CLI call to the init SecureSync
- verify it's a valid NTP server that is known to be up and running.
- Check if **NTP Symmetric key authentication** is being enforced in either SecureSync

To determine if a SecureSync requires successful symmetric key authentication, on the left side of the **Management** -> NTP Setup page of the browser, click the “**Access Restrictions**” button. In the pop-up window, see if there is a “1” in the first row (for “IP4”), for the “Auth **Only**” column (as shown below)



Type	IP Version	IP	IP Mask	Auth Only	Enable Query
Allow	IPv4	default	default	1	Change Delete
Allow	IPv6	default	default		Change Delete

email Keith sent about “init and symmetric authentication: (18 Dec 2018) I was just talking with one of our Apps Engineers about NTP's refid value of “init”. In addition to this being the initial refid for a peer/server when NTP first starts-up (until it starts getting NTP responses back from the particular peer/server), I wasn't sure if NTP would continue reporting “init” if there was a larger time error than its expecting

He said he didn't believe so, especially if the Reach value for this same NTP sever is remaining “0” as well, And the testing I've been performing shows this doesn't appear to be the case- time error doesn't affect “init” and doesn't stop the reach from incrementing. These two values in ntpq -p just need to see a time stamp returned.

But I just thought of another factor (besides a firewall in between blocking port 123) which I suspect could very well also affect both items– NTP symmetric key authentication, (one SecureSync requiring it, while its peer/server SecureSync/NTP either not configured to use it, or not correctly configured with an identical kestring/digest, or a key not marked as trusted. Symmetric key is a function of NTP often required for switches to sync to an NTP server, especially Cisco switches.

After first verifying normal/expected NTP peering operation (Reach incrementing and “init” changing mere moments later) with no symmetric keying configured, I then ran a simple test to see if NTP symmetric key, if not correctly configured in both SecureSyncs, will prevent “init” from changing/Reach from incrementing for a peer.

I had “B” peered to “A” and told “A” to require symmetric key (even though “B” has no keys configured). This provided a case where successful authentication isn't possible. As I suspected, just like if there was a network issue between the two SecureSyncs – such as port 123 being closed, the Reach value stayed 0 and the refid stayed init for the peer which was not able to successfully authenticate.

Based on this observation that it definitely affects init and Reach, I now suspect the issue you are observing is that there is a symmetric key configuration mis-match between the “init” server and the other SecureSync(s),.

If the server that you were running ntpq -p command on has been configured to require authentication (not the factory default state), and its peer(s) SecureSync is not configured with an identical kestring, this will prevent them from peering to each other, as exactly as you are seeing.

To determine if a SecureSync requires successful symmetric key authentication, on the left side of the **Management** -> NTP Setup page of the browser, click the “**Access Restrictions**” button. In the pop-up window, see if there is a “1” in the first row (for “IP4”), for the “Auth **Only**” column (as shown below)

NTP Access Restrictions

Type	IP Version	IP	IP Mask	Auth Only	Enable Query	
Allow	IPv4	default		1		Change Delete
Allow	IPv6	default				Change Delete

If this field is blank, this SecureSync doesn't require successful authentication in order to exchange NTP packets with other NTP clients/other SecureSyncs. But if there is a "1" in the field (as shown above) symmetric key is being enforced and so it will only exchange NTP packets with other devices which are configured with an identical keystring.

Next, to see what trusted symmetric keys, if any, have been added to every SecureSync desired to be peered together (and every NTP client you wish to sync to the SecureSync), click the **"Symmetric Key"** button, also on the left side of the **Management -> NTP setup** page. The pop-up table will be empty if there are no keys configured. Or it will list a key ID, digest and a keystring, for each configured key

NTP Symmetric Key

Trusted ☐ Trusted

Symmetric Key ID

Digest Scheme

Symmetric Key String

Submit

For authentication to be successful between an NTP server requiring authentication and another NTP device, the Key IDs don't have to match (they can, though it's not necessary), but:

the keystring on both NTP devices have to be IDENTICAL

the Trusted checkbox needs to be selected (which will place a "1" in the Trusted field for each key listed in the SecureSync)

if the Keys table for the SecureSync requiring auth has at least one key in it and its marked as Trusted, but the other NTP server has no keys listed, none of the keystings are identical and/or a key with a matching string isn't marked as trusted, this is the problem. You will need to either create a new key having the trusted box selected and a matching keystring, or edit an existing incorrect key to make it a trusted/matching key.

To add a new Symmetric key, press the "+" sign in the upper-right corner of the "symmetric key table" (after pressing the Symmetric keys button on the left side of the NTP Setup page). The pop-up will look like the following screenshot. Select the Trusted box, enter an arbitrary Key ID Number, match the Digest Scheme selected in the other servers, and enter the identical key string. Then press Submit.

NTP Symmetric Key

Trusted ☐ Trusted

Symmetric Key ID

Digest Scheme

Symmetric Key String

Submit

Note that most Cisco switches use MD5 for the Message Digest, but SecureSyncs also optionally support several other digests, also (such as SHA and SHA1 for examples)

two time servers.

.step

- A step time change in system time has occurred, but the association has not yet resynchronized.

- Time change of less than the panic threshold of 1000 seconds occurred.

.deny

- NTP access was denied by the NTP server

.bcst (broadcast server)

- NTP broadcast time server

.pps (atom clock driver)

- As long as the “**Timing System 1PPS Reference**” field is **Enabled** in the NTP Servers tab, NTP can select the reference, if it wishes to (it’s not guaranteed that it will). When Enabled, the **Status -> NTP** page of the browser will list System PPS as an NTP reference for NTP selected. But if it’s an “X”, NTP won’t be able to select it as a reference.
- If the “**Timing System 1PPS Reference**” field is **Disabled** in the NTP Servers tab, the **Status -> NTP** page won’t list system PPS as a possible reference for NTP input. so it can’t be selected.

Once NTP has synced to GPS inside the SecureSync (and assuming the “**Timing System 1PPS Reference**” field is Enabled in the **Network -> NTP Setup** page of the browser, **NTP Servers** tab, as shown below), we enable another NTP input reference that uses the 1PPS generated by the GPS signal. This “PPS” reference helps stabilize/optimize the NTP functionality, if NTP decides to select it as its input. This input is known as NTP’s PPS clock driver and can be selected by NTP shortly after NTP syncs to GPS. If NTP selects it as its reference, NTP changes the Ref ID from “.GPS” to “.PPS” to indicate this PPS clock driver had been enabled.

NTP SETUP

General Settings | NTP Peers | **NTP Servers** | Symmetrical Keys | Autokey | NTP Broadcasting | NTP Access

Timing System Reference: Enabled ☒ Preferred ☐

Typically references like GPS or IRIG provide better accuracy than NTP.
Check this box to use those references as the preferred timing input to NTP.
Uncheck this box if NTP servers or peers are the only input references available.

Timing System 1PPS Reference: Enabled ☒

If you are configuring NTP servers or peers as either the preferred reference or as a backup to the timing system, do not enable the timing system 1PPS reference.

If you look at the **Status -> NTP** page of the SecureSync’s browser when the **Timing System 1PPS Reference** is enabled, you will see the following, with the NTP Reference Status table showing both GPS and .PPS. Note that when the SecureSync is able to get time from other NTP servers (NTP Peer or NTP Server modes), we recommend the “**Timing System 1PPS Reference**” be set to disabled, in which case the PPS reference is not listed as a reference and not sent to NTP. In this case, it will always remain “.gps” instead of “.pps”.

NTP INPUT STATUS

Status

Time Offset

RMS Jitter

Frequency Offset

Sync	Selected Reference	Stratum	LI	Delay (ms)	Offset (ms)	Jitter (ms)
Yes	System Time	1	00	0.000	-0.001	0.002

NTP Selected Reference Status

Sync	Host	Ref ID	Stratum	LI	Mode	Type	Auth Status	Last (Sec)	Poll Interval (Sec)	Reach	Delay (ms)	Offset (ms)	Jitter (ms)
---	System Time	.GPS.	0	00	Client	local	none	8	16	377	0.000	-0.001	0.002

NTP Reference Status

Sync	Host	Ref ID	Stratum	LI	Mode	Type	Auth Status	Last (Sec)	Poll Interval (Sec)	Reach	Delay (ms)	Offset (ms)	Jitter (ms)
---	System Time	.GPS.	0	00	Client	local	none	8	16	377	0.000	-0.001	0.002
'S'	System PPS	.PPS.	0	00	Client	local	none	6	16	377	0.000	-0.004	0.002
'S'	10.10.100.15	.GPS.	1	00	Client	local	none	6	16	377	0.000	-0.004	0.002


```
kwing@Spectracom ~ $ ntpq -pn
```

remote	refid	st	t	when	poll	reach	delay	offset	jitter
*127.127.45.0	.GPS.	0	l	13	16	377	0.000	0.043	0.002
o127.127.22.0	.PPS.	0	l	12	16	377	0.000	0.009	0.014
+10.2.100.93	.GPS.	1	u	3	8	377	0.229	0.013	0.097

```
kwing@Spectracom ~ $
```

OR

At the login prompt, type **ntpq** <enter>. Then type either **peer** or **peers**

```
Spectracom spectracom # ntpq
```

```
ntpq> peers
```

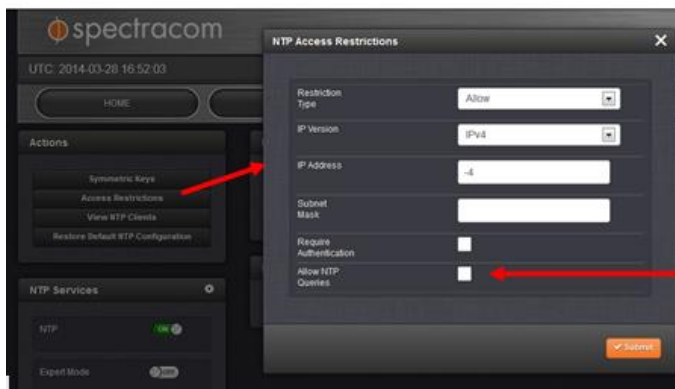
remote	refid	st	t	when	poll	reach	delay	offset	jitter
*PCI_TSYNC(0)	.GPS.	0	l	14	16	377	0.000	0.012	0.002
oPPS(0)	.PPS.	0	l	13	16	377	0.000	-0.001	0.002

```
ntpq>
```

To disable NTPQ/NTPDC

A) Software versions 5.1.2 and above)

To disable NTPQ/NTPDC, navigate to the Management -> NTP Setup page. Then click on Access Restrictions in the upper-left corner. In the "IPv4" row of the table that opens, click "Change". Verify Allow NTP Queries is disabled (as shown below).



B) (Software versions 5.02 and below)

Refer to knowledge article: https://na8.salesforce.com/articles/FAQ/CVE-2013-5211-for-SecureSync?navBack=H4sIAAAAAAAAAAluuVipVsILSjy_N1M_Oyy_PSU1JT9UHcrxhHI_83FT74tTEouQM29z8vJzM4hIIHaVioCYUJUCxbKBYQWJ6akhmSU6qUm0sAAR0v2VcAAAA&popup=false

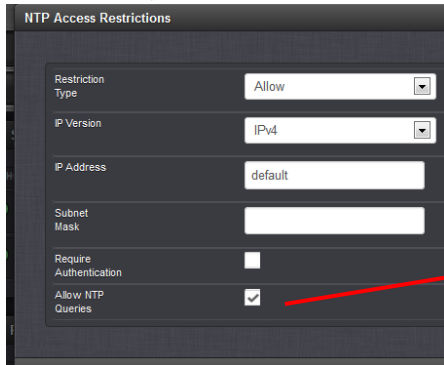
To verify NTPQ and NTPDC are really disabled:

A) Have to use either a linux box on the network running NTP OR another Spectracom time server.

- NTPQ and NTPDC will still work on the same box, even if queries are disabled.

From another NTP server on the same network, login to the CLI (RS-232, telnet or ssh) and at the command prompt, type **ntpq -p** (or **ntpq -pn**) followed by the IP address of the other NTP server being checked.

B) With NTPQ/NTPDC enabled in the other server, the peers command will work:



NTP Access Restrictions

Restriction Type: Allow

IP Version: IPv4

IP Address: default

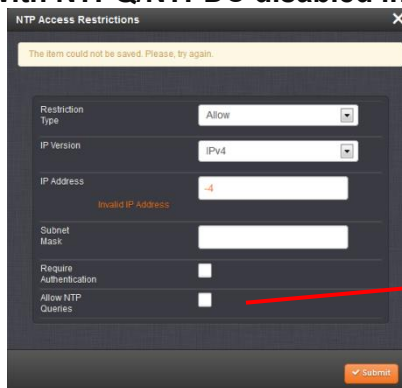
Subnet Mask:

Require Authentication: ☐

Allow NTP Queries: ☒

```
spadmin@Spectracom ~ $ ntpq -p
remote refid s
=====
10.2.100.93 .INIT. 1
spadmin@Spectracom ~ $
```

C) With NTPQ/NTPDC disabled in the other server, the peers command will not work:



NTP Access Restrictions

The item could not be saved. Please, try again.

Restriction Type: Allow

IP Version: IPv4

IP Address: 10.2.100.177
Invalid IP Address

Subnet Mask:

Require Authentication: ☐

Allow NTP Queries: ☐

Submit

```
***Request timed out
spadmin@Spectracom ~ $ ntpq -p 10.2.100.177
10.2.100.177: timed out, nothing received
***Request timed out
spadmin@Spectracom ~ $
```

*NTP Status Symbols (Tally Codes)

In the front of each listed reference is a “Tally Code”. The Tally Code reports the “status” of each reference.

Tally code	Green = (Sync) Red = (Not in Sync) (if the Reach is not 0)	Truechimer (good) or falseticker (bad) (as determined by the Clock Select Algorithm)
*	The Selected Time reference	Truechimer
o	The Selected PPS reference	Truechimer
+	A high quality candidate for NTP reference input that can be selected by NTP as its time reference (Good reference, but not selected)	Truechimer
x	“ Falseticker ” Listed NTP Peer was discarded from selection (NTP won't select this peer as its reference).	falseticker
-	“ Outlier ” Listed NTP Peer was discarded from selection (NTP won't select this peer as its reference).	falseticker
(blank)	Source discarded: Failed Sanity check	falseticker

Symbol	Indication
*	The Selected Time reference
o	The Selected PPS reference
#	"#" selected for synchronization but distance exceeds maximum
+	A high quality candidate for NTP reference input that can be selected by NTP as its time reference (Good reference, but not selected)
x	“ Falseticker ” Listed NTP Peer was discarded from selection (NTP won't select this peer as its reference).
-	“ Outlier ” Listed NTP Peer was discarded from selection (NTP won't select this peer as its reference).
(blank)	Source discarded: Failed Sanity check

**NTP Reach Value

From the website of: <http://www.linuxjournal.com/article/6812> describing the Reach value

For reasons that seemed good to the developers, this register is displayed to the user in octal values instead of binary, decimal or even hex. The maximum value of an eight-bit binary number is 11111111, which is 377 in octal, 255 in decimal and 0xFF in hex.

So why does the value of the reach field drop when packets are being successfully sent and received? For those of you who dream in octals, this next part may seem obvious. For ordinary mortals, it requires closer scrutiny. The answer is that the lower numerical values are caused by the left-shifting of the reachability register. Remember, the buffer is not a metric, it is a FIFO log. So, if you have received the last eight NTP packets successfully, the log contains all 1s and the reach field contains the octal value of 377.

Let's assume that on the next update, a packet is dropped. Because NTP is a UDP-based protocol with no delivery guarantees, this is not necessarily a cause for alarm. But the NTP daemon dutifully logs the failure in the circular buffer and waits for the next poll period. The log now contains 11111110 and a reach field value of 376.

If the next seven polls are successful, seven 1s are added from the right-hand side of the register, pushing the 0 representing the dropped packet further towards the left (and digital oblivion). Listing 4 shows the progression of a single dropped packet through the reachability register.

From: <http://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-110/15171-ntpassoc.html>

Examples of Reach Field Values

The reach field is a [circular](#) bit buffer. It gives you the status of the last eight NTP messages (eight bits in octal is 377, so you want to see a reach field value of 377). If an NTP response packet is lost, the missing packet is tracked over the next eight NTP [update](#) intervals in the reach field. The table below provides explanations for possible reach field values using the loss of an NTP response packet as an example.

reach column shows the status of the reachability register (in octal).

an 8-bit left-rotating register. Any 1 bit means that a "time packet" was received. The right most bit indicates the status of the last connection with the NTP server. It is Octal number. Use calculator in programmer interface to translate from OCT to BIN: For example, 377 translates to 11111111. Each 1 means a successful connection to the NTP server. If you just start a NTP service, and it connects successfully with its server, this number will change as follows (assuming connectivity is good):

Reach Field Value (Reported/Binary)	Explanation
377 = 1 1 1 1 1 1 1 1	Time 0: Last eight responses from server were received
376 = 1 1 1 1 1 1 1 0	Time 1: Last NTP response was NOT received (lost in network)
375 = 1 1 1 1 1 1 0 1	Time 2: Last NTP response was received
373 = 1 1 1 1 1 0 1 1	Time 3: Last NTP response was received
367 = 1 1 1 1 0 1 1 1	Time 4: Last NTP response was received
357 = 1 1 1 0 1 1 1 1	Time 5: Last NTP response was received
337 = 1 1 0 1 1 1 1 1	Time 6: Last NTP response was received
277 = 1 0 1 1 1 1 1 1	Time 7: Last NTP response was received
177 = 0 1 1 1 1 1 1 1	Time 8: Last NTP response was received
377 = 1 1 1 1 1 1 1 1	Time 9: Last NTP response was received

ntpq associations (show ntp associations, as command)

- Refer to: great info at: <https://www.cisco.com/c/en/us/support/docs/ip/network-time-protocol-ntp/116161-trouble-ntp-00.html> or <http://doc.ntp.org/4.1.0/debug.htm>
- Provides detailed info for each peer/server
- if using this command from outside of SecureSync (not from its CLI interface) requires "enable queries" (for NTPQ/NTPDC) to be Enabled (disabled by default).

A) Versions 5.2.1 and below (NTP version 4.2.8 and below)

ntpq -c as

To enable NTPQ/NTPDC queries (to optionally allow ntpq to be accessible from outside the SecureSync)

In the newer black browser: **Management** -> **NTP Setup** page and click **Access Restrictions** on the left side of the page. Press Change and enable Queries.

After enabling NTP queries (if desired)

1) Need to first define the “host” as the particular peer or server the info will be provided for

- First go into ntpq by typing **ntpq** <enter> at the command prompt
- Use the command of **host xxx.xxx.xxx.xxx** <enter> (where x is the IP address of the time server).

Term Explanation

Characters before the address have these definitions:

- * Synchronized to this peer
- # Almost synchronized to this peer
- + Peer selected for possible synchronization
- Peer is a candidate for selection
- ~ Peer is statically configured

address This is the IP address of the peer. In the example, the first entry shows 127.127.7.1. This indicates that the local machine has synced with itself. Generally, only an NTP master syncs with itself.

ref clock This is the address of the reference clock for the peer. In the example, the first six peers/servers have a private IP as the reference clock, so their masters are probably routers, switches, or servers within the local network. For the last four entries, the reference clock is a public IP, so their masters are probably a public time source.

st NTP uses the concept of a stratum in order to describe how far away (in NTP hops) a machine is from an authoritative time source. For example, a stratum 1 time server has a radio or atomic clock directly attached to it. It sends its time to a stratum 2 time server through NTP, and so on up to stratum 16. A machine running NTP automatically chooses the machine with the lowest stratum number with which it can communicate and uses NTP as its time source.

when The time since the last NTP packet was received from a peer is reported in seconds. This value should be lower than the polling interval.

poll The polling interval is reported in seconds. The interval usually starts with a minimum of 64-second poll intervals. The RFC specifies that no more than one NTP transaction per minute is needed in order to synchronize two machines. As NTP becomes stable between a client and a server, the poll interval may increase in small steps from 64 seconds up to 1024 seconds and generally stabilizes somewhere in between. But, this value dynamically changes, based on the network conditions between the client and the server and the loss of NTP packets. If a server is unreachable for some time, the poll interval is increased in steps to 1024 seconds in order to reduce network overhead.

It is not possible to adjust the NTP poll interval on a router, because the interval is determined by heuristic algorithms.

reach Peer reachability is a bit string reported as an octal value. This field shows whether the last eight packets were received by the NTP process on the Cisco IOS® software. The packets must be received, processed, and accepted as valid by the NTP process and not just by the router or switch that receives the NTP IP packets.

Reach uses the poll interval for a time out in order to decide whether a packet was received or not. The poll interval is the time that NTP waits before it concludes that a packet was lost. The poll time can be different for different peers, so the time before reach decides that a packet was lost can also be different for different peers.

In the example, there are four different reach values:

- 377 octal = 11111111 binary, which indicates the NTP process received the last eight packets.
- 0 octal = 00000000, which indicates the NTP process did not receive any packet.
- 1 octal = 00000001, which indicates the NTP process received only the latest packet.
- 357 octal = 11101111, which indicates the packet before the latest four packets was lost.

Reach is a good indicator of whether NTP packets are being dropped because of a poor link, CPU issues and other intermittent problems.

[Convert octal <-> binary](#) is an online unit converter for this and many other conversions.

delay The round-trip delay to peer is reported in milliseconds. In order to set the clock more accurately, this delay is taken into account when the clock time is set.

offset Offset is the clock time difference between the peers or between the master and client. This value is the correction that is applied to a client clock in order to synchronize it. A positive value indicates the server clock is higher. A negative value indicates the client clock is higher.

disp Dispersion, reported in seconds, is the maximum clock time difference that was ever observed between the local clock and server clock. In the example, dispersion is 0.3 for the server 10.50.36.42, so the maximum time difference ever observed locally between the local clock and the server clock is 0.3 seconds.

You can expect to see a high value when the clocks are syncing initially. But, if the dispersion is too high at other times, the

NTP process on the client does not accept NTP messages from the server. Maximum dispersion is 16000; in the example, that is the dispersion for servers 10.50.44.69 and 10.50.44.133, so the local client does not accept time from these servers.

If the reach is zero and dispersion is very high, the client is probably not accepting messages from that server. Refer to the second line of the example:

```
•address ref clock st when poll reach delay offset disp
~10.50.44.69 10.50.36.106 5 21231 1024 0 3.8 -4.26 16000.
```

•
Even though the offset is just -4.26, the dispersion is very high (perhaps due to a past event), and the reach is zero, so this client does not accept time from this server.

10) Type **as** <enter> (if already in ntpq) or **ntpq -c as** <enter> (if already in ntpq)

```
spadmin@Spectracom176 ~ $ ntpq -c as

ind assid status conf reach auth condition last_event cnt
=====
  1 42295 965a yes yes none sys.peer sys_peer 5
  2 42296 973a yes yes none pps.peer sys_peer 3
spadmin@Spectracom176 ~ $
```

Peer is reachable/peer is unreachable

<https://rags.wordpress.com/2011/10/17/how-to-debug-ntp-issues/>

The * indicates that this particular association is the chosen ntp source.

The + indicates that this ntp peer is a candidate (a peer is a ntp server on the same stratum).

- **An empty space indicates** that the server is **unreachable** and therefore rejected (stratum 16).

rv and rvi commands (readvar)

- Refer to <http://www.novell.com/coolsolutions/trench/418.html>
- In ntpdc with software versions 5.2.0 and below - or in ntpq in software versions 5.2.1 and above
- Provides leap_arm for pending leap second. Stratum level, LI bits etc.
- Somewhat similar to the “ntpq -p sysinfo” command (further below)
- I found reference to “rvi” command but the response to it is “unknown”.

Note (may need to perform one or the other):

- Type either **as** or **host xxx.xxx.xxx.xxx** (where x is the IP address of the time server) to define the specific time server before performing the rv command.
- Type **rv <association>** (where the applicable <association number> for the time server can be obtained by typing “as”)

```
precision=-18, rootdelay=0.000, rootdisp=1.000, refid=GPS,
reftime=d9383eb3.5f38193e  Fri, Jun 26 2015 21:12:19.371,
clock=d9383eb4.1cc822fb  Fri, Jun 26 2015 21:12:20.112, peer=40430, tc=3,
mintc=3, offset=0.000378, frequency=-11.628, sys_jitter=0.003815,
clk_jitter=0.004, clk_wander=0.000
ntpq> -c rv
***Command '-c' unknown
ntpq> as

ind assid status  conf reach auth condition  last_event cnt
=====
  1 40429  965a   yes   yes  none   sys.peer   sys_peer   5
  2 40430  973a   yes   yes  none   pps.peer   sys_peer   3
  3 40431  8011   yes   no   none   reject     mobilize   1
ntpq> rv
associd=0 status=0118 leap_none, sync_pps, 1 event, no_sys_peer,
version="ntpd 4.2.8p2@1.3265-o Tue Apr 21 15:01:53 UTC 2015 (1)",
processor="i586", system="Linux/3.18.11-gentoo", leap=00, stratum=1,
precision=-18, rootdelay=0.000, rootdisp=1.075, refid=GPS,
reftime=d9383ec3.5f38266c  Fri, Jun 26 2015 21:12:35.371,
clock=d9383ec9.5e0f914e  Fri, Jun 26 2015 21:12:41.367, peer=40430, tc=3,
mintc=3, offset=0.000488, frequency=-11.628, sys_jitter=0.003815,
clk_jitter=0.004, clk_wander=0.000
ntpq> sysinfo
```

Kerninfo (display kernel information)

- Displays leap second status, precision status, lock status, etc

ntpq -c kerninfo (or just **kerninfo** if already in ntpq directory)

```
spadmin@Spectracom176 ~ $ ntpq -c kerninfo
associd=0 status=0118 leap_none, sync_pps, 1 event, no_sys_peer,
pll offset:          -0.022059
pll frequency:       -20.1659
maximum error:       0.0025
estimated error:     3e-06
kernel status:      pll nano
pll time constant:   4
precision:          1e-06
frequency tolerance: 500
pps frequency:      0
pps stability:      0
pps jitter:         0.000
calibration interval 4
calibration cycles:  0
jitter exceeded:    0
stability exceeded:  0
calibration errors:  0
spadmin@Spectracom176 ~ $
```

NTPDC

- For a list of available NTPDC commands (such as monlist as well as clockstats, peerstats and loopstats), refer to: <http://www.ece.udel.edu/~mills/ntp/html/ntpdc.html>

Note: ntpdc was removed from ntp in ntp version 4.2.8 (starting in our software version 5.2.1)

NTPQ

- Refer to sites such as: <http://doc.ntp.org/4.2.8/ntpq.html>

***ntpq -p sysinfo / ntpq -c sysinfo commanda (system information)

- Provides **leap_arm** for pending leap second, Stratum level LI bits etc.
- Similar to the “rv” command

sysinfo: Display operational summary (below info from <http://doc.ntp.org/4.1.2/ntpdc.htm>)

Description and fields in sysinfo

Print a variety of system state variables, i.e., state related to the local server. All except the last four lines are described in the NTP Version 3 specification, RFC-1305.

System flags show various system flags, some of which can be set and cleared by the enable and disable configuration commands, respectively. These are the auth, bclient, monitor, pll, pps and stats flags. See the ntpd documentation for the meaning of these flags. There are two additional flags which are read only, the kernel_pll and kernel_pps. These flags indicate the synchronization status when the precision time kernel modifications are in use. The kernel_pll indicates that the local clock is being disciplined by the kernel, while the kernel_pps indicates the kernel discipline is provided by the PPS signal.

Stability (reported in PPM): The stability is the residual frequency error remaining after the system frequency correction is applied and is intended for maintenance and debugging. In most architectures, this value will initially decrease from as high as 500 ppm to a nominal value in the range .01 to 0.1 ppm. If it remains high for some time after starting the daemon, something may be wrong with the local clock, or the value of the kernel variable tick may be incorrect.

****As most people have some trouble with that abstract PPM (parts per million, 0.0001%), I'll simply state that 12 PPM correspond to one second per day roughly. So 500 PPM means the clock is off by about 43 seconds per day.**

Examples:

12 PPM = about one second per day of time drift.

69 PPM= about six seconds per day of time drift.

500 PPM= about 43 seconds per day of time drift.

Broadcastdelay: shows the default broadcast delay, as set by the broadcastdelay configuration command.

Authdelay: shows the default authentication delay, as set by the authdelay configuration command.

A) Versions 5.2.1 and above (NTP version 4.2.8 and above)

example response from the internet

```
# ntpq -c sysinfo
associd=0 status=0018 leap_none, sync_unspec, 1 event, no_sys_peer,
system peer: 0.0.0.0:0
system peer mode: unspec
leap indicator: 00
stratum: 3 (means this host / NTP client is a "stratum 3" time server)
log2 precision: -24
root delay: 1.184
root dispersion: 789.028
reference ID: 169.254.169.254
reference time: dbdfd9c3.4d614c5a Wed, Nov 23 2016 9:02:59.302
system jitter: 0.000000
clock jitter: 18.991
clock wander: 0.000
broadcast delay: -50.000 (shows the default broadcast delay, as set by the broadcastdelay config command)
symm. auth. delay: 0.000
```

Example response to ntpq -c sysinfo from one of our time servers

```
spadmin@Spectracom176 ~ $ ntpq -c sysinfo
associd=0 status=4119 leap_add_sec, sync_pps, 1 event, leap_armed,
system peer: PPS(0)
system peer mode: client
leap indicator: 01
stratum: 1
log2 precision: -18
root delay: 0.000
root dispersion: 24.404
reference ID: PPS
reference time: d93da98e.a27d9db1 Tue, Jun 30 2015 23:49:34.634
system jitter: 23.270989
clock jitter: 10.332
clock wander: 0.000
broadcast delay: 0.000
symm. auth. delay: 0.000
spadmin@Spectracom176 ~ $ ntpq -as
```

B) Versions 5.2.0 and below (NTP versions 4.2.6 and below)

Ntpdc -> Sysinfo command


```

[1]+  Stopped                  ntpq
spadmin@Spectracom ~ $ ntpdc
ntpdc> sysinfo
system peer:          PPS(0)
system peer mode:     client
leap indicator:       00
stratum:              1
precision:            -19
root distance:        0.00000 s
root dispersion:      0.00035 s
reference ID:         [PPS]
reference time:       d8718f94.08fc9b86  Tue, Jan 27 2015  4:16:20.035
system flags:         auth monitor ntp kernel stats
jitter:               0.000000 s
stability:            0.000 ppm
broadcastdelay:       0.000000 s
authdelay:            0.000000 s
ntpdc>

```

Stability

NTPDC -> monlist command (And DRDoS/Amplification Attack)

(Note: screenshot below was taken with version 5.1.3 software installed)

```

spfactory@Spectracom ~ $ ntpdc
ntpdc> help
ntpdc commands:
addpeer      controlkey  fudge      keytype    quit        timeout
addrefclock  ctlstats    help       listpeers  readkeys    timerstats
addserver    debug       host       loopinfo   requestkey  traps
addtrap      delay       hostnames  memstats   reset        trustedkey
authinfo     delrestrict ifreload   monlist    reslist     unconfig
broadcast    disable     ifstats    passwd     restrict    unrestrict
clkbug       dmpeers     iostats    peers      showpeer    untrustedkey
clockstat    enable      kerninfo   preset     sysinfo     version
clrtrap      exit        keyid      pstats     sysstats
ntpdc>

```

To use NTPDC commands, login to the CLI interface (RS-232, telnet or SSH). At the command prompt, type **ntpdc** <enter>.

Monlist command

RDoS Amplification attack:

Refer to <http://support.ntp.org/bin/view/Main/SecurityNotice>

Mitigation:

- Upgrade NTP to 4.2.7p26 or later.

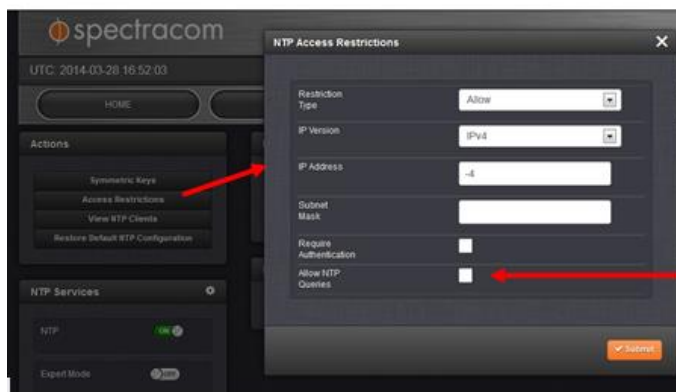
SecureSync and 9400s, update to versions 5.2.1 or higher which updated NTP to 4.2.8)
NetClocks 9300 and 9200: this option not available as of at least version 3.6.7/ June 2015.

- **Users of NTP versions before 4.2.7p26 should either:**
Use **noquery** in your default restrictions to block all status queries.
Use **disable monitor** to disable the ntpdc -c monlist command while still allowing other status queries.
- Disabling NTPQ/NTPDC is one of two ways to prevent the amplification attack in NTP versions prior to version 4.2.7 (the other method is Disable Monitor – more info on this below)

To disable NTPQ/NTPDC

A) (Software versions 5.1.2 and above)

To disable NTPQ/NTPDC, navigate to the **Management -> NTP Setup** page. Then click on **Access Restrictions** in the upper-left corner. In the “IPv4” row of the table that opens, click “Change”. Verify Allow NTP Queries is disabled (as shown below).



B) Software versions 5.02 and below

Refer to knowledge article: https://na8.salesforce.com/articles/FAQ/CVE-2013-5211-for-SecureSync?navBack=H4slAAAAAAAAAluuVipVslLSjy_N1M_Oyy_PSU1JT9UHcrxhHI_83FT74tTEouQM29z8vJzM4_hIIHaVioCYUJUCxbKBYQWJ6akhmSU6qUm0sAAR0v2VcAAAA&popup=false

To verify NTPQ/NTPDC are really disabled, try performing the **ntpq-p** command from a Linux box on the network running NTP software. In none is available, and there is more than one SecureSync on the network, try running the command from the other server.

Login with telnet or ssh and at the command prompt, type **ntpq -p**. The time server with the query disabled should not be reported in the results.

Or, to use monlist from the other server, type **ntpdc**. Then type **monlist**.

```
Spectracom spectracom # ntpdc
ntpdc> monlist
remote address      port local address      count m ver rstr avgint  lstint
=====
10.2.100.87         123 10.2.100.177           80 3 4  c0  1016   337
ntpdc>
```

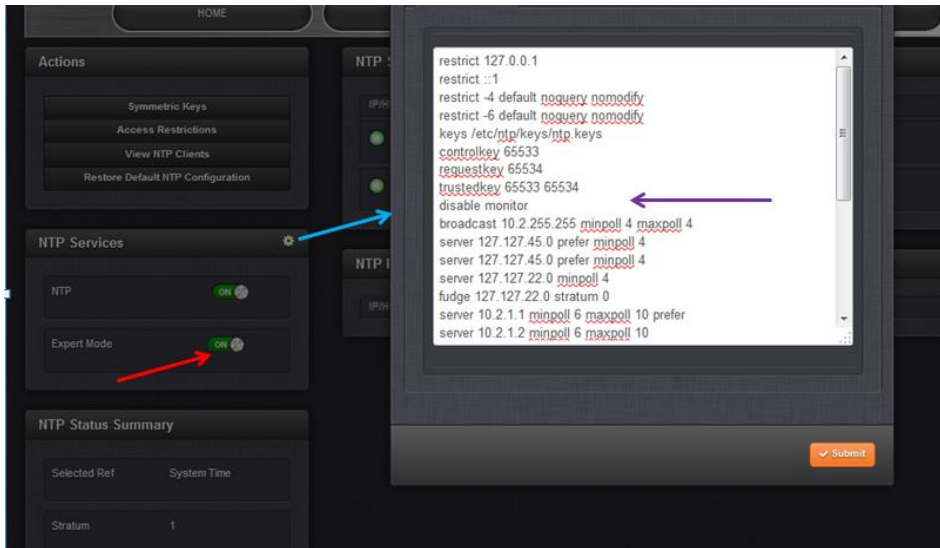
**Disable Monitor (Used to prevent Amplification attack by turning off monlist)

- Disable Monitor is a second method to prevent amplification attack (instead of disabling all NTPQ/NTPDC functionality)

- This is the less restrictive of the two methods, still allowing other ntpq/ntpd functionality to be available.
- Unlike disabling NTPQ/NTPDC which can be done via the browser, “Disable Monitor” requires Expert Mode be used.

To turn on “Disable Monitor”

in the **Management** -> **NTP Setup** page, switch **Expert Mode** to **On**. Then, to edit the ntp.conf file to add disable monitor, click on the gear box next to “NTP Services” just above the NTP enable/disable switch. This will open the ntp.conf file, just like it was in the previous software version (as shown below). Then keep Expert Mode enabled to preserve the change.



Per <http://support.ntp.org/bin/view/Main/SecurityNotice> there are two ways to prevent the Amplification Attack using Monlist:

Use noquery in your default restrictions to block all status queries.

Use disable monitor to disable the ntpdc -c monlist command while still allowing other status queries.

The method we typically recommend is to use **noquery** to block all NTPQ/NTPDC queries from external to the SecureSync (including monlist). This method is the more restrictive method of the two and can be configured without the need to use NTP Expert Mode in the browser (keeping in mind that Expert Mode needs to remain enabled to preserve any changes made to ntp.conf, and overrides the ability to use the browser to make other changes to NTP). The settings I sent to you about disabling all NTPQ/NTPDC queries for IPv4 and IPv6 is this method.

However, if you wish to be less restrictive (in order to be able to perform other NTPQ/NTPDC queries, besides monlist) this can still be done as it was in the previous version, using Expert mode in version 5.1.2.

If you prefer to continue using Disable Monitor, instead of using noquery, in the Management -> NTP Setup page, switch Expert Mode to On. Then, to edit the ntp.conf file to add disable monitor, click on the gear box next to “NTP Services” just above the NTP enable/disable switch. This will open the ntp.conf file, just like it was in the previous software version (as shown below). Then keep Expert Mode enabled to preserve the change.

**NTP Statistics (NTP ClockStats, NTP loopstats and NTP Peerstats)

- Refer to: <http://www.eecis.udel.edu/~mills/ntp/html/monopt.html>

List of Fields included in loopstats and peerstats

Table 3. Statistic Files

File Type	Version	List of Fields
loopstats	3	day, second, offset, drift compensation, polling interval
	4	day, second, offset, drift compensation, estimated error, stability, polling interval
peerstats	3	day, second, address, status, offset, delay, dispersion
	4	day, second, address, status, offset, delay, dispersion, skew (variance)

A) NTP Clockstats (our “System Time” Reference Clock Driver to NTP)

Enables recording of clock driver statistics information. Each update received from a clock driver appends a line of the following form to the file generation set named **clockstats**:

The first two fields show the date (Modified Julian Day) and time (seconds and fraction past UTC midnight). The next field shows the clock address in dotted-quad notation. The final field shows the last timecode received from the clock in decoded ASCII format, where meaningful. In some clock drivers a good deal of additional information can be gathered and displayed as well. See information specific to each clock for further details.

To calculate MJD: <http://www.csgnetwork.com/julianmodifdateconv.html> (drop down to “Convert from MM-DD-YYYY to MJD”)

MJD (Date)

Seconds since midnight

clockstats

Record reference clock statistics. Each update received from a reference clock driver appends one line to the clockstats file set:

49213 525.624 127.127.4.1 93 226 00:08:29.606 D

Item	Units	Description
49213	MJD	date
525.624	s	time past midnight
127.127.4.1	IP	reference clock address
Message	text	log message

The message field includes the last timecode received in decoded ASCII format, where meaningful. In some cases a good deal of additional information is displayed. See information specific to each reference clock for further details.

Example entry from an NTP.log: 56203 2963.366 127.127.45.0 277 00:49:39.203031

Where:

56203 = Modified Julian Day (<http://www.csgnetwork.com/julianmodifdateconv.html>)

2963.366 = Seconds since midnight (<http://www.aelius.com/njh/unixtime/>)

127.127.45.0 = Spectracom's NTP reference clock driver

277 = Day of Year (<http://www.esrl.noaa.gov/gmd/grad/neubrew/Calendar.jsp>)

00:49:39.203031 = last timestamp received from System Time (where 277 is the Julian date followed by hours, minutes and seconds since midnight).

B) NTP Loopstats (NTP's Local clock for NTP to go to Stratum 16)

Enables recording of loop filter statistics information. Each update of the local clock outputs a line of the following form to the file generation set named **loopstats**: example: 50935 75440.031 0.000006019 13.778190 0.000351733 0.0133806

The first two fields show the date (Modified Julian Day) and time (seconds and fraction past UTC midnight).

The next five fields show time offset (seconds), frequency offset (parts per million - PPM), RMS jitter (seconds), Allan deviation (PPM) and clock discipline time constant.

PPM), RMS jitter (seconds), Allan deviation (PPM) and clock discipline time constant.

loopstats

Record clock discipline loop statistics. Each system clock update appends one line to the loopstats file set:

50935 75440.031 0.000006019 13.778 0.000351733 0.013380 6

Item	Units	Description
50935	MJD	date
75440.031	s	time past midnight
0.000006019	s	clock offset
13.778	PPM	frequency offset
0.000351733	s	RMS jitter
0.013380	PPM	RMS frequency jitter (aka wander)
6	log ₂ s	clock discipline loop time constant

Where:

50935 = Modified Julian Day (<http://www.csgnetwork.com/julianmodifdateconv.html>)

75440.031 = Seconds since midnight (<http://www.aelius.com/njh/unixtime/>)

C) NTP peerstats (data from other NTP servers that this NTP server is syncing to / peering with)

Enables recording of peer statistics information. This includes statistics records of all peers of a NTP server and of special signals, where present and configured.

Each valid update appends a line of the following form to the current element of a file generation set named

peerstats: 48773 10847.650 127.127.4.1 9714 -0.001605376 0.000000000 0.001424877 0.000958674

- **The first two fields** show the date (Modified Julian Day) and time (seconds and fraction past UTC midnight).
 - **The next two fields** show the peer address in dotted-quad notation and status, respectively.
 - **The status field** is encoded in hex in the format described in Appendix A of the NTP specification RFC 1305.
- Refer to: <https://thomasvachon.com/articles/ntp-peerstats-status-word-secret-decoder-ring/> (discusses how to decode each byte)
- **The final four fields** show the offset, delay, dispersion and RMS jitter, all in seconds.

peerstats
Record peer statistics. Each NTP packet or reference clock update received appends one line to the `peerstats` file set:

```
48773 10847.650 127.127.4.1 9714 -0.001605376 0.000000000 0.001424877 0.000958674
```

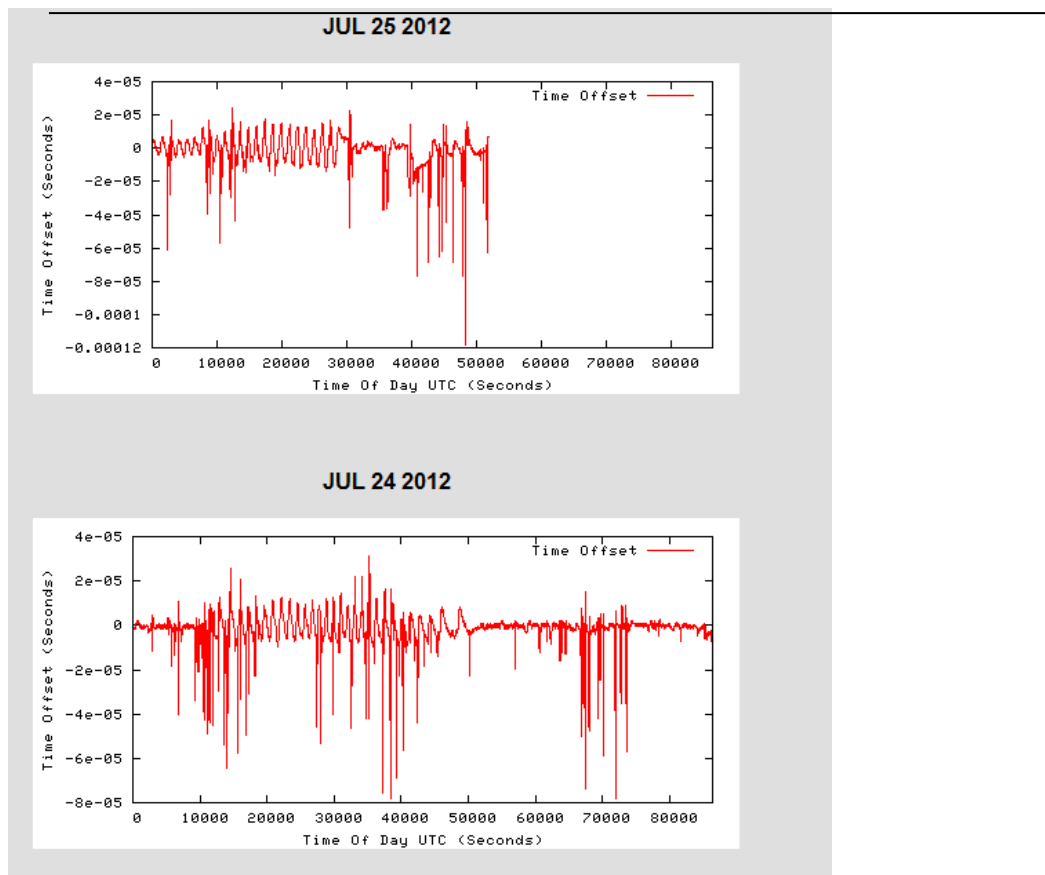
Item	Units	Description
48773	MJD	date
10847.650	s	time past midnight
127.127.4.1	IP	source address
9714	hex	status word
-0.001605376	s	clock offset
0.000000000	s	roundtrip delay
0.001424877	s	dispersion
0.000958674	s	RMS jitter

The status field is encoded in hex format as described in Appendix B of the NTP specification RFC 1305.

Where:

48773 = Modified Julian Day (<http://www.csgnetwork.com/julianmodifdateconv.html>)

108547.650 = Seconds since midnight (<http://www.aelius.com/njh/unixtime/>)



Example NTP.conf

```
restrict 127.0.0.1
restrict -4 default noquery nomodify
restrict -6 default noquery nomodify
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
server 127.127.45.0 minpoll 4
enable pps
server 127.127.22.0 minpoll 4
fudge 127.127.22.0 stratum 1
server 127.127.1.0 minpoll 4
```



```

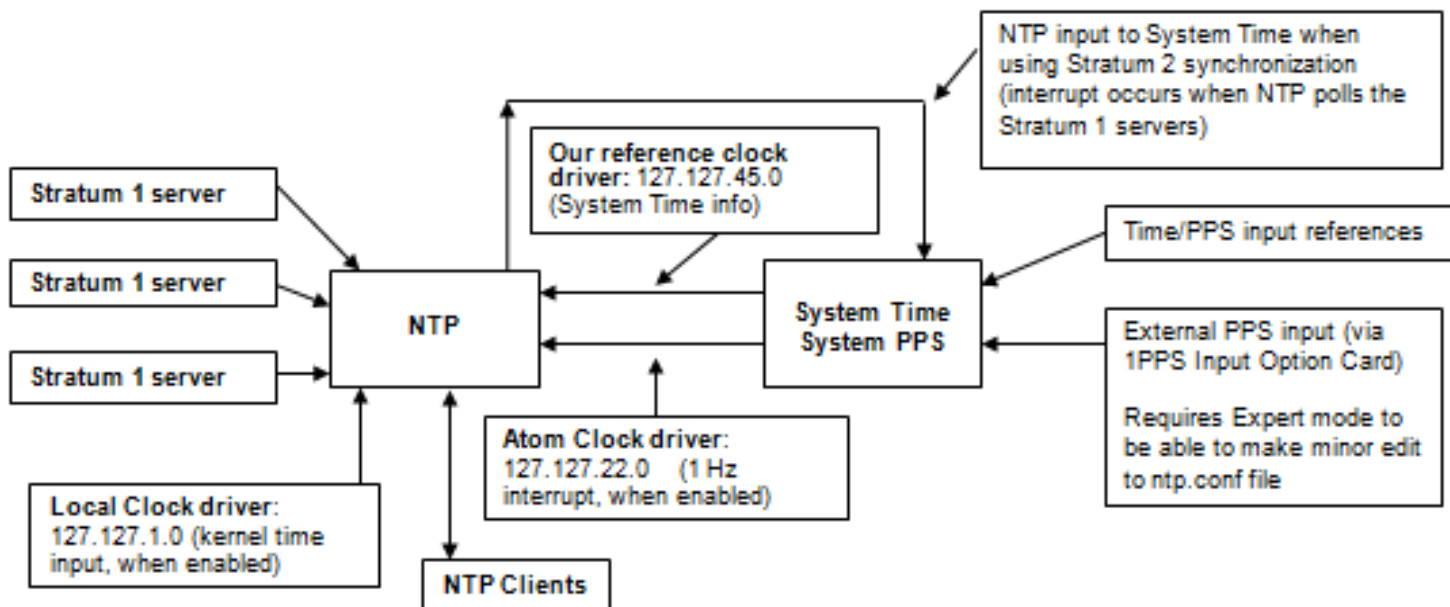
fudge 127.127.1.0 stratum 15
server 74.112.39.70 minpoll 6 maxpoll 10 prefer iburst burst
server 74.112.39.69 minpoll 6 maxpoll 10 iburst burst
server 10.10.128.24 minpoll 6 maxpoll 10 iburst burst
server 10.10.128.28 minpoll 6 maxpoll 10 iburst burst
keysdir /etc/ntp/keys/
driftfile /etc/ntp/ntp.drift
logfile /home/spectracom/log/ntp.log
statsdir /home/spectracom/log/ntpstats/
statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable

```

**Monitoring and Controlling NTP

- Refer to <http://support.ntp.org/bin/view/Support/MonitoringAndControllingNTP>

**127.127.1.0 (Atom clock driver), 127.127.22.0 (PPS driver) AND 127.127.45.0 (Spectracom Clock driver)



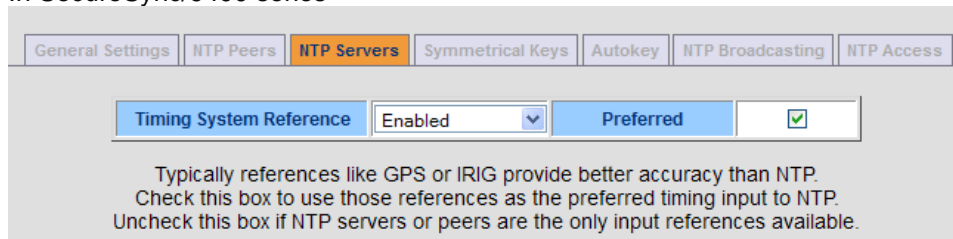
When using NTPQ/NTPDC, a reference to three distinct values may be displayed. These values are as follows:

Spectracom Reference Clock driver (127.127.45.0) - “TSync(0)”

- Allows NTP to sync to System Time
- Enabled when the “timing System Reference (Network -> NTP Setup, NTP Servers tab) is Enabled.
- When enabled, adds a “System Time” row to the Status -> NTP page (as shown below).
- Reference ID (Ref ID) for the Spectracom driver reference is “.GPS”

127.127.45.0 is the **Spectracom Reference Clock driver** which allows NTP to obtain time from System Time.

In SecureSync/9400 series



General Settings | NTP Peers | **NTP Servers** | Symmetrical Keys | Autokey | NTP Broadcasting | NTP Access

Timing System Reference ☒ Enabled ☒ Preferred ☒

Typically references like GPS or IRIG provide better accuracy than NTP.
Check this box to use those references as the preferred timing input to NTP.
Uncheck this box if NTP servers or peers are the only input references available.

In SecureSync/9400 series NTP expert mode

server 127.127.45.0 prefer minpoll 4

(**Note:** “prefer” being present indicates the “preferred” checkbox is enabled)

In NTP log (when synced to System Time): ntpd[826]: synchronized to PCI_TSYNC(0), stratum=0

Note: The Reference Clock driver (127.127.45.0) is valid for NTP input when input references such as GPS, IRIG, Havequick, etc, are valid or if in Self mode. However, it’s not valid when syncing SecureSync to other NTP servers.

NTP Reference Status													
Sync	Host	Ref ID	Stratum	LI	Mode	Type	Auth Status	Last (Sec)	Poll Interval (Sec)	Reach	Delay (ms)	Offset (ms)	Jitter (ms)
✔	System Time	.USER.	0	00	Client	local	none	3	16	377	0.000	0.000	0.001

- Version 4.7.0 change minpoll interval to “4 (16s)” for faster sync. The maxpoll is not specified, so according to Paul Myers, the poll interval is always every 16 seconds.

“Timing System 1PPS Reference” (aka “Atom Clock Driver” or “PPS driver”) “127.127.22.0”

- For detailed info on the atom clock driver, refer to:
<http://www.eecis.udel.edu/~mills/ntp/html/drivers/driver22.html>.

From the link above

“This driver furnishes an interface for the pulse-per-second (PPS) signal produced by a cesium clock, radio clock or related devices. It can be used to augment the serial timecode generated by a GPS receiver, for example. It can be used to remove accumulated jitter and re-time a secondary server when synchronized to a primary server over a congested, wide-area network and before redistributing the time to local clients. The driver includes extensive signal sanity checks and grooming algorithms. A range gate and frequency discriminator reject noise and signals with incorrect frequency. A multiple-stage median filter rejects jitter due to hardware interrupt and operating system latencies. A trimmed-mean algorithm determines the best time samples. With typical workstations and processing loads, the incidental jitter can be reduced to a few microseconds.”

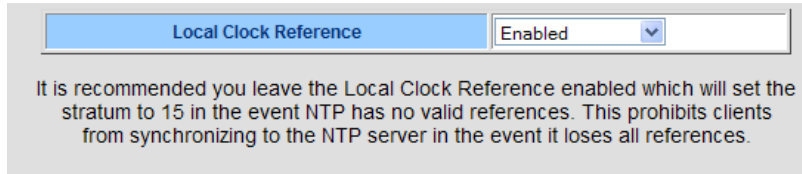
Reference ID

- Reference ID for the NTP PPS driver reference is “.PPS”

127.127.22.0 is the **NTP 1PPS driver (Atom clock driver/Atomic clock driver)**. This driver allows for better stability of NTP by providing it with a 1PPS input reference (See additional info on this driver further below).

When this driver is enabled, we send the kernel a once-per-second interrupt at the top of each second, based on the System Time.

In SecureSync/9400 series web browser



The screenshot shows a web browser interface for the SecureSync/9400 series. At the top, there is a blue header bar with the text 'Local Clock Reference' and a dropdown menu set to 'Enabled'. Below this, a text box contains the following message: 'It is recommended you leave the Local Clock Reference enabled which will set the stratum to 15 in the event NTP has no valid references. This prohibits clients from synchronizing to the NTP server in the event it loses all references.'

In SecureSync/9400 series NTP expert mode

```
enable pps
server 127.127.22.0 minpoll 4
fudge 127.127.22.0 stratum 0
```

(**Note:** The “fudge” Statum value is changed from “0” to “1” when using external 1PPS input to SecureSync)

In NTP log (when synced to System PPS): [synchronized to PPS\(0\)](#), [stratum=0](#)

The Atom clock (PPS) driver provides NTP with a 1PPS input that it can discipline with, after NTP has synced to a time reference (such as GPS, for instance). Several minutes after NTP has synced, an NTP log entry of **ntpd[708]: synchronized to PPS(0), stratum=0** will be asserted.

Requirements for NTP to use this driver

- The PPS signal must be present and within nominal jitter and wander tolerances.
- In addition, the prefer peer must be a truechimer; that is, survive the sanity checks and intersection algorithm.
- Finally, the offset of the system clock relative to the prefer peer must be within ± 0.5 s.
- The kernel maintains a watchdog timer for the PPS signal; if the signal has not been heard or is out of tolerance for more than some interval, currently two minutes, the kernel discipline is disabled and operation continues as if it were not present.

“**71.80.83**” displayed in the **Status ->NTP** page when this Atom clock is the selected reference: This decimal value equates to “GPS” when converted to ASCII characters.

Why the “Timing System 1PPS Reference” SHOULD be DISABLED when NTP Peers/Servers are listed.

- The “Timing System 1PPS Reference” should ONLY be ENABLED when NTP Peers/Servers are NOT listed in the NTP settings.
- The “Timing System 1PPS Reference” should be DISABLED when NTP Peers/Servers are listed.
- Having the “Timing System 1PPS Reference” enabled with NTP Peers configured can adversely affect the system when NTP is synced to a listed peer.

When NTP syncs to a listed Peer, NTP’s Time is the based on the selected peer. With the “Timing System 1PPS Reference” (Atom Clock driver) enabled, an interrupt is sent to the System Time to make any necessary corrections of the System PPS to align it with the incoming NTP packets. This is done by staggering the System PPS into alignment. This will adversely affect the 1PPS outputs and all outputs that are derived from the System PPS (The oscillator is in freerun when synced to NTP, so the 10 MHZ output is not affected by the Atom clock driver being.

NTP peers command (Side-by-side comparison of the times reported by NTP servers)

- Refer to <http://www.eecis.udel.edu/~mills/ntp/html/ntpq.html#mrulist>
- To compare the output times from more than one NTP server, use the NTP peers command. This can be run from any Linux machine running NTP software.
- To allow the NTP peers command in the NTP -> General page of the browser, select the “**Allow queries from NTPDC or NTPQ over IPv4**” checkbox”.
- Example response below:

```
ntpq> pe
remote      refid  st  t  when poll  reach  delay  offset  jitter
=====
-10.10.2.1   .ACTS.  1  u  51   64   377   1.914  -2.610  6.239
+10.10.2.2   .GPS.   1  u  53   64   377   1.933   0.049  1.410
```

NTP Peers field descriptions (from <http://www.eecis.udel.edu/~mills/ntp/html/ntpq.html#mrulist>)

peers Display a list of peers in the form [tally]remote refid st t when pool reach delay offset jitter	
Variable	Description
[tally]	single-character code indicating current value of the select field of the peer status word
remote	host name (or IP number) of peer
refid	association ID or kiss code
st	stratum
t	u: unicast or multicast client, b: broadcast or multicast client, l: local (reference clock), s: symmetric (peer), a: manycast server, B: broadcast server, M: multicast server
when	sec/min/hr since last received packet
poll	poll interval (log ₂ s)
reach	reach shift register (octal)
delay	roundtrip delay
offset	offset of server relative to this host
jitter	jitter

To allow the NTP peers command to be performed on both NetClocks, just temporarily select the “Allow queries from NTPDC or NTPQ over IPv4” checkbox. (NTP -> General page of the web browser).

Once the NTP peers command has been run, unselect this checkbox.

This log entry can be viewed via SSH or the web browser, but this required manual intervention. If it's desired to obtain this info automatically, enable NTPQ and use scripting to read the NTPQ peers command.

There is no way to have the NetClock automatically send the NTP log entries, without some user-intervention being required. However, I spoke to one of our engineers about this. You can use the NTPQ peers command to determine when NTP is using the PPS for disciplining. Then, scripting can be used to read this information from the peers command.

The NetClocks have the ability to enable NTPQ functionality (disabled by default). Once NTPQ has been enabled (by selecting the “Allow queries from NTPDC or NTPQ over IPv4” checkbox in the NTP/General page of the browser), the peers command can start to be used.

In the NTPQ peers response will be a reference to the PPS. Once NTP indicates in this query that its synced to this PPS, the "synchronized to PPS(0), stratum=0" message is then generated by NTP.

NTP Mode 6 and Mode 7 (NTPQ and NTPDC)

NTP **Mode 6 (NTPQ)** and **Mode 7 (NTPDC)** are both supported in NetClocks, starting in version 3.4.3, as well as all SecureSyncs. It is not available in Model 91xx series NTP servers.

NTP Mode 7 Request Denial of Service

Report from Todd Christianson from State Street Bank regarding 9200/9300 (12/9/09)

A vulnerability has been reported in NTP, which can be exploited by malicious people to cause a DoS (Denial of Service). The vulnerability is caused due to an error in the processing of mode 7 requests in ntpd. This can be exploited to cause an NTP packet reply loop by sending a specially crafted packet with a spoofed source IP address to an affected NTP server. The vulnerability is reported in versions prior to 4.2.4p8. Solution: Update to version 4.2.4p8.

Per Paul Myers:

Workaround:

Turn off support for NTPDC and NTPQ.

GO to the NTP General page and make sure that for IPv4 and IPv6 we do **NOT** "Allow queries from NTPDC or NTPQ"

Long term we will need to update NTPD version we are using or apply a patch to our version if we want to stay at this version for NetClock and Lafayette.

This is a better description:

<http://support.ntp.org/bin/view/Main/SoftwareDownloads>

NTP mode 7 (MODE_PRIVATE) is used by the ntpdc query and control utility. In contrast, ntpq uses NTP mode 6 (MODE_CONTROL), while routine NTP time transfers use modes 1 through 5. Upon receipt of an incorrect mode 7 request or a mode 7 error response from an address which is not listed in a restrict ... noquery or restrict ... ignore statement, ntpd will reply with a mode 7 error response (and log a message). In this case:

- If an attacker spoofs the source address of ntpd host A in a mode 7 response packet sent to ntpd host B, both A and B will continuously send each other error responses, for as long as those packets get through.
- If an attacker spoofs an address of ntpd host A in a mode 7 response packet sent to ntpd host A, A will respond to itself endlessly, consuming CPU and logging excessively.

Q Looking at license notices in the manual one can see that Spectracom uses the ntp4 implementation from David Mills... Is it an unmodified version? If no, what are the modifications? What are your politics regarding actualizations? Every time that there is a new version of ntp, is there a new firmware version?

A. The unit does use the NTP4 implementation from David Mills. The current version installed is version 4.2.0.A. But, a custom reference clock driver has been added to allow NTP to communicate with our internal timing system. Any version changes to NTP will not automatically be implemented in the software, but any changes that are made will be reviewed and implemented as warranted.

****Who is using my NTP server?**

Refer to: <http://support.ntp.org/bin/view/Support/MonitoringAndControllingNTP>

And <http://www.eecis.udel.edu/~mills/ntp/html/ntpq.html#mrulist>

MONlist- monlist [version]

Obtain and print traffic counts collected and maintained by the monitor facility (Shows packet counts).

This is an NTPDC query command that can be monitored using a free Windows-based NTP control and monitoring

program from Meinberg (Called Time Service Monitor). The program performs functions like stopping and starting NTP, and performing NTPQ queries (such as peerstats and loopstats) to monitor the performance of NTP. According to a customer, we apparently support at least parts of this program with the Model 9200/930series with software version 3.4.3 and higher with NTPQ enabled. Refer to <http://www.meinberg.de/english/sw/time-server-monitor.htm>

Remote address	Port	Local address	Count	Mode	Version	Drop	Last	First
127.0.0.1	4416	127.0.0.1	64	7	2	0	2	0
10.2.128.19	123	10.2.128.15	3	4	4	0	66	12

Monlist Field descriptions (from NTP.org website
<http://www.eecis.udel.edu/~mills/ntp/html/ntpq.html#mrulist>)

Column	Description
lstatint	Interval in s between the receipt of the most recent packet from this address and the completion of the retrieval of the MRU list by ntpq.
avgint	Average interval in s between packets from this address.
rstr	Restriction flags associated with this address. Most are copied unchanged from the matching restrict command, however 0x400 (kod) and 0x20 (limited) flags are cleared unless the last packet from this address triggered a rate control response.
r	Rate control indicator, either a period, 1 or x for no rate control response, rate limiting by discarding, or rate limiting with a KoD response, respectively.
m	Packet mode.
v	Packet version number.
count	Packets received from this address.
rport	Source port of last packet from this address.
remote address	DNS name, numeric address, or address followed by claimed DNS name which could not be verified in parentheses.

You can check which hosts are talking to your time server by using the **mrulist** command of ntpq (or in older versions of NTP, the **monlist** command of ntpdc), e.g.
 ntpq -c mrulist

Please note that a maximum of 600 entries is supported with current versions of ntpq and ntpdc. The protocol (or better: the contents of the return packets) used by ntpq or ntpdc is not standardized, therefore it is recommended to only use ntpq or ntpdc with a matching ntpd, i.e. both should have the same version number.

To get by this 600 entry limitation, many server operators run client statistics scripts, such as Wayne Schlitt's ntp_clients and ntp_clients_stats scripts, which can be found at <http://www.schlitt.net/scripts/ntp/index.html> . They work very well, but can use quite a bit of system resources if your client counts are in the high thousands. Examples of these scripts in action can be found at:

- http://www.schlitt.net/ntpstats/ntp_stats.txt
- http://saturn.dennishilberg.com/ntpstats/ntp_clients_stats.php (slightly modified)

Keith's comments using NTPDC (I couldn't get this to work in NTPQ)
 On a Windows PC or a Linux box running full NTP (not just Windows Time Service)

1. **Enable NTPQ and NTPDC in the Spectracom NTP server**
2. **Open a command prompt window on the PC.**
3. **Change to the NTP directory (for Meinberg NTP, go to c:\program files\ntp)**
4. **Type: `ntpd` <enter> to change to NTPDC**


```
H:\>C:
C:\>cd program files
C:\Program Files>cd ntp
C:\Program Files\ntp>ntpd
ntpd>
```

5. Type: **host xxx.xxx.xxx.xxx** (where x is the IP address of the NTP server).

```
***request timed out
ntpd> host 10.2.100.15
current host set to 10.2.100.15
ntpd>
```

6. Type **monlist** <enter>

```
ntpd> monlist
remote address      port local address      count m ver rstr avgint  lstint
=====
pm-wing2.int.oria.co 1163 10.2.100.15           396 7 2   80    11     0
localhost           47719 127.0.0.1             22312 6 2    0     0     0
pm-lorah.int.oria.co 6010 10.2.100.15           209 3 4   80    16    10
10.2.100.130        123 10.2.100.130          208 3 4    1    16    12
ntpd> _
```

**Automachron program: Time Program for testing NTP with Time Servers

- Displays time stamps even if Time Server not synced.
- Freeware program.
- Refer to: <I:\Customer Service\Automachron>

Minimum sync interval: Appears to be the default “Sync Every” field value of 16 seconds. I lowered this value to 1 second and the program still only synced once every 16 seconds.

Note: When the program is minimized to the System Tray (GUI not displayed), to display the GUI again, right click on the icon in System tray and select “Properties”.

Ref Ident (Ref ID) field

- Reported in hex
- Refer to sites such as: <http://www.asciitohex.com/>

Hex	Text conversion
494e4954	.init
55534552	.user
677073	.gps
50505300	.pps

****Syncing Virtual Servers (VMWare)**

Email from Paul Myers to Will Hickey (9/23/13) Mark Robertson is TELLING us ByteFusion PresentTense does not work well.

We need a new product offering or GUIDANCE on how to sync the actual Machine's OS and configure VM's to get time from that sync'ed OS

It might be an opportunity for us, but we need to ask ourselves:

1. Can we sync the underlying OS the VMs run on.
2. Do the VM's simply need to take time and sync to the underlying OS?
3. Are the VM software machine writers going to do this?
4. There are many VM writers. They need to sync time... If we write our own we have to pick VM to work with.

I doubt we are going to compete writing an entire VM software package, and we would need APIs to sync the time.

Why would anything we write be BETTER than ByteFusion or TimeKeeper?

Does TimeKeeper WORK in VMs?

I think we could do something but there is a product management effort to determine how much?

Email from Paul Myers (23 Sept 2013) This is a good document regarding Time Sync in VM's from our vendor of tools we use.

It states time sync is hard in VMs...

<http://www.vmware.com/files/pdf/techpaper/Timekeeping-In-VirtualMachines.pdf>

NTP operation

****Number of NTP requests per second/NTP Stress test**

Refer to: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP stress testing](#)

Q. What is the max number of NTP requests per second?

A. from Section 1.7.4 in the SecureSync manual, "Loading: ~7,000 NTP requests per second, typical"

Signal 15 ("NTP Exiting on Signal 15") or other Signals

- Refer to <http://stackoverflow.com/questions/16723626/what-is-signal-15-received>
- This indicates the linux has delivered a `SIGTERM` to your process. This is usually at the request of some other. This signal requests an orderly shutdown of your process.

****NTP Authentication (MD5/SHA1)**

MD5

- Make sure the key is marked “**Trusted**” in the Symmetric Key table.
- With the original web browser design (versions prior to 5.1.0) do not use characters such as a “\$” (dollar sign). MD5 won’t work. See note below.

MD5 authentication not working with non-ASCII characters (Applicable to original web browser design only, versions 5.0.2 and below)

Note: Update to at least version 5.1.2 (new browser) for non-ASCII characters.

- In original web browser- Do not use symbols such as the “\$” (dollar sign). The browser will accept the characters, but it will prevent authentication from working at all. This is a limitation of the browser and not a limitation of NTP/MD5. Engineering believes the new web browser handles all characters correctly

SHA1 instead of MD5 authentication

Refer to Mantis case 1990 <http://cvsmantis.int.rolia.com/mantis/view.php?id=1990>

- **(12 Apr 2013)** with at least Archive versions 4.8.9 and below, we only support NTP authentication using **MD5** (we don’t support using SHA1 or other hash generators). We don’t provide access to the ntp keys file to switch to other mechanisms.
- Versions 4.8.9 and below- This is a limitation of the version of NTP we currently use (version 4.2.0).
- Version 5.0.0 upgraded NTP to v4.2.6P5, but did not add any changes to the web browser to be allow SHA1 to be selected. So, it won’t be available until sometime after Archive version 5.0.0.
- Update to this: I believe this will be available in archive 5.1.2.

Email from Paul Myers

NTP technically supports MORE than MD5. SHA1/SHA may not be supported in NTP 4.2.0

Second email from Paul Myers

<http://lists.ntp.org/pipermail/questions/2011-December/031192.html>

On Thu, Dec 8, 2011 at 14:38, Joe Smithian <joe.smithian@gmail.com> wrote:

- > A,N,S, and M keys are defined in the man ntp.keys
- >
- > <http://www.gsp.com/cgi-bin/man.cgi?section=5&topic=ntp.keys>

That's a good example of why one should be suspicious of man pages for ntpd and friends -- the distribution docs are maintained as HTML and any man page variant is likely to be based on out of date information.

That page describes a ntp.keys scheme where the type column is always a single letter and it determines not only the digest algorithm, but also the representation. That's not how ntp.keys works today. The type column specifies only the digest algorithm, and only 'M' (or MD5) is supported prior to ntp 4.2.6. With 4.2.6 and later, the type column can specify the name of any suitable OpenSSL-provided digest algorithm which produces a 16-20 octet digest.

The format choice (between hexadecimal and ASCII) is driven by the length of the key value. If it is 20 characters or less, the ASCII is used directly as the key value. If it is 21 characters or longer, it is interpreted as hexadecimal-encoded. Summary- SO FOR OUR NTP 4.2.0 ONLY MD5 works

Issue with MD5 authentication not working with clients after updating from version 4.8.9 (NTP version 4.2.0) to versions 5.x.x (NTP version 4.2.6p5)

- Refer to Mantis case 2756 (http://cvsmantis.int.rolia.com/mantis/view_all_bug_page.php)
- Also refer to Salesforce case 13501 for Paul Lindblad.
- Internal Knowledge article: <https://na8.salesforce.com/ka0C0000000L6H1>.

- He needed to edit **Management** -> **NTP Setup**, "**Access Restrictions**" after updating to archive version 5.x.x.

Our clients are now seeing the upgraded NTP server. I went to management /NTP setup/Access restrictions It seemed to be messed up. When I looked at it in the classic interface it looked OK. On the new GUI interface in the IP address column there were "-4"s I decided to change the IP in one column. When I did, all columns changed to that IP address. Then I tried to change the mask in one column. All columns changed to that mask. So I just deleted them all and manually typed the correct info in, one by one. This worked OK except for the fact that the IP version column kept wanting to say IPv6. I had to change this back to IPv4 on several of them. It seems stable now and the clients are seeing the NTP server.

**** Automatic FTP of NTP Statistics**

Q. Does the SecureSync/NetClock 9400 series have the option of send "Automatic FTP of Statistics", equal to 9300 series (every 30 minutes).

A. (as of 28 Aug 2013 per Keith) No. This capability was not brought forward into the newer SecureSyncs.

For your information, the NTP Statistics data is still available from the SecureSync and Model 9400s. It just not automatically sent out via FTP in the newer Models. Though it's not automatically sent out, it can still be easily retrieved via a single file of bundled logs.

The NTP statistics files that are sent out in the Model 9300s are the NTP Clockstats, Peerstats and Loopstats files. These files can be easily bundled into a single file, along with the other logs and then manually extracted whenever desired, using a manual FTP connection. The instructions below to do this are specific to SecureSync, but are very similar for NetClock 9400s as well.

In order to capture the log files, simply copy/paste all of the log entries (from all of the log tabs) in the SecureSync's **Tools** -> **Logs** page of its web browser (such as all of the log entries in the "Event" tab, "Alarms" tab, "Oscillator" tab, etc). Paste all of the log entries into a single Microsoft Word document and then send us this document for our review.

Instead of copy/pasting all of the logs to a Word document, you can also bundle the logs into a single log file. Then export this bundle file from the SecureSync using an FTP or SCP session. Then, simply attach this extracted file to a reply email. Below is additional information on how to bundle and extract all of the unit's logs:

Attached you will find an example log save file. In this Text document, you will find the Clockstats, loopstats and peerstats logs (just like with the Model 9300s). Just search this file for all three of these words.

**NTP broadcast/ NTP Multicast modes

For troubleshooting/addition info, refer to: [NTP Broadcast/Multicast modes](#)

- NTP broadcast can be enabled without stopping/restarting NTP (starts broadcasting after being enabled)
- MD5 key needs to be defined, if the NTP client requires MD5 authentication.
- NTP Broadcast can be configured to go out all Ethernet ports if the Gigabit Card 1204-06 is installed
 - **NOTE:** Need to use NTP Expert Mode. Refer to the NTP expert mode tech note: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert Mode- Broadcast and Multicast](#)
- NTP Multicast (224.0.1.1) only goes out one Ethernet port (the first network it sees as valid, such as Eth0 for instance (if it's desired to multicast to more than on network, this has to be handled outside of the SecureSync).
- **Note:** If the NTP client can configure which multicast address it monitors, the static routes in the main default gateway page can be configured for one multicast address to be sent out one specific network interface, while another multicast address can be sent out a different interface. We can multicast any IP address, so we can multicast 224.0.1.1 (the address reserved for NTP) on one interface (such as Eth1) and 224.0.0.1 (as an example) on a different interface (such as Eth2).

A) NTP Broadcast Mode

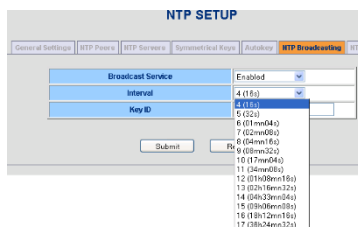
- Packet capture of NTP broadcast

438	10.338948	10.3.1.4	10.2.100.29	Jabber / Response: Stp XmitMs= jabber:client: 110
530	12.725603	Dell_6a:3e:32	LLDP_Multicast	LLDP Chassis Id = 00:1c:23:6a:3e:30 Port Id
525	12.585466	10.2.100.20	10.2.255.255	NTP NTP broadcast
441	10.269676	10.2.100.44	10.2.100.29	Syslog LOCAL7.NOTICE: spectracom: [system] AUT
328	7.508441	10.2.100.29	10.7.0.131	TCP ms-wbt-server > psmond [ACK] Seq=100492

Email Keith sent to John Jenkins To begin, configuring the SecureSync for NTP broadcast mode is extremely easy. In fact, you don't even need to stop and restart NTP in the process for it to start (many other NTP config changes require it to be restarted before the change takes effect).

To enable NTP broadcast mode, simply navigate to the **Network -> NTP setup** page of the browser, NTP Broadcasting tab. As shown below, change the "Broadcast Service" field to enabled and change the "Interval" drop-down to the desired broadcast interval (as indicated inside the parenthesis). Then hit Submit.

Note the "KEY ID" field should remain blank, unless the Harris equipment requires an MD5 authentication hash be sent with each NTP time stamp, in order for it to accept the time stamp. If MD5 is required (as it with many Cisco devices), let Dave or me know and we can tell you more about this particular configuration.



The screenshot shows the 'NTP SETUP' page with the 'NTP Broadcasting' tab selected. The 'Broadcast Service' is set to 'Enabled'. The 'Interval' is set to '4 (18s)'. The 'Key ID' field is empty. A dropdown menu is open, showing a list of MD5 key IDs from 1 to 17, each followed by its corresponding MD5 hash in parentheses. The 'Submit' button is visible at the bottom left of the form.

After hitting Submit, the NTP packets will start to be transmitted at the interval specified. No other steps are required for them to go out. I just confirmed this with a wireshark capture, shown below. Wireshark capture is the best way to prove the time stamps are occurring. The packet(s) should indicate "NTP broadcast" originating from the IP address of the NTP server and going out to the broadcast address for the network.

438	10.338948	10.3.1.4	10.2.100.29	Jabber / Response: Stp XmitMs= jabber:client: 110
530	12.725603	Dell_6a:3e:32	LLDP_Multicast	LLDP Chassis Id = 00:1c:23:6a:3e:30 Port Id
525	12.585466	10.2.100.20	10.2.255.255	NTP NTP broadcast
441	10.269676	10.2.100.44	10.2.100.29	Syslog LOCAL7.NOTICE: spectracom: [system] AUT
328	7.508441	10.2.100.29	10.7.0.131	TCP ms-wbt-server > psmond [ACK] Seq=100492

Lastly, most if not all NTP clients will ignore the SecureSync's NTP packets if the SecureSync is not synced to either an external reference or to itself. To verify the SecureSync's NTP packets are useable, navigate to the **Status -> NTP** page of the browser. In the top row of this page is the current NTP Status. If the stratum value is a value such as 1 or 2, the NTP packets are useable. But if it indicates NTP is Stratum 16, the SecureSync is not in sync and the packets will likely be ignore by any NTP client. Below is an example of NTP at Stratum 2. Its NTP packets are useable.

NTP INPUT STATUS

StatusTime OffsetRMS JitterFrequency Offset

Sync	Selected Reference	Stratum	LI	Delay (ms)	Offset (ms)	Jitter (ms)
Yes	10.2.100.44	2	00	0.391	0.834	0.320

- Scott with Larcen desired to broadcast NTP to all four subnets. Refer to Salesforce case 9886.
- Requires the use of NTP Expert mode (to add multiple NTP "Broadcast" lines to the ntp.conf file
- Refer to the NTP Broadcast Tech Note: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert Mode- Broadcast to more than one port](#)

Regarding the Spectracom SecureSync's NTP broadcast functionality, I have some information for you. I apologize for the delay in getting back to you (there are never enough hours in a day ☺)!!!

This morning, instead of looking at your SecureSync, I decided to test NTP broadcast on all isolated ports using one of our SecureSyncs here at the factory. This test went VERY well. I was able to confirm NTP is able to broadcast on every one of the four network ports, with each network port configured to be on different, isolated subnets.

Page | 639


```

restrict 127.0.0.1
restrict -4 default noquery nomodify
restrict -6 default noquery nomodify
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
broadcast 10.2.255.255 minpoll 4 maxpoll 4
broadcast 192.168.255.255 minpoll 4 maxpoll 4
broadcast 194.168.255.255 minpoll 4 maxpoll 4
broadcast 196.168.255.255 minpoll 4 maxpoll 4
server 127.127.45.0 prefer minpoll 4
enable pps
server 127.127.22.0 minpoll 4
fudge 127.127.22.0 stratum 0
server 127.127.1.0 minpoll 4
fudge 127.127.1.0 stratum 15
keysdir /etc/ntp/keys/
driftfile /etc/ntp/ntp.drift
logfile /home/spectracom/log/ntp.log
statsdir /home/spectracom/log/ntpstats/

```

After editing the ntp.conf file, I then edited the IP addresses for Eth 0, Eth 1, Eth 2 and Eth 3 as follows:

Eth 0

Version	IP Address	Prefix	Delete	Info
IPv4	10.2.100.147	16	na	net mask = 255.255.0.0

Eth 1

IP Version	IP Address	Prefix	Delete	Info
IPv4	192.168.1.1	16	na	net mask = 255.255.0.0

Eth 2

IP Version	IP Address	Prefix	Delete	Info
IPv4	194.168.1.1	16	na	net mask = 255.255.0.0

Eth 3

IP Address Setup				
IP Version	IP Address	Prefix	Delete	Info
IPv4	196.168.1.1	16	na	net mask = 255.255.0.0

With the ntp.conf and Ethernet ports all configured, I then restarted NTP (**Network -> NTP Setup** page, **General Settings** tab

Once NTP restarted, and with the SecureSync in sync (this is important, in order for NTP broadcast packets to be generated), I performed a wireshark capture on all four network connections.

Attached is a copy of each of the network port captures, showing NTP broadcast packets being successfully transmitted from the same SecureSync on each isolated subnet. The second value is the IP address for the SecureSync, and the third value is the broadcast address configured in NTP, for that particular network port.

I'm not sure why you weren't receiving the NTP broadcast packets. Make sure that you restart NTP after editing NTP and the network

port settings. Were you using Wireshark to capture the NTP broadcast packets, or seeing if your equipment was syncing to the packets? If you weren't using Wireshark to look for the packets, I definitely recommend you do so, especially if you try the steps above again and the equipment still doesn't sync sometime with the NTP broadcast schedule. Also make sure the Sync LED on the front of the SecureSync is green. Another good indication is the Stratum field in the first row of the Status -> NTP table should be a "1" (or a "2" if the SecureSync is synced to another NTP server that is Stratum 1).

Please let me know that you see the NTP packets broadcast on all four networks.

A) NTP Multicast mode

- Refer to NTP Multicast Tech note: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert Mode- Broadcast and Multicast](#)

Desire to output NTP Multicast on more than one Ethernet port (Gigabit Option card installed)

- Refer to Salesforce case 9886
- This configuration won't work – Multicast NTP can only go out one Ethernet port (not more than one). So the gigabit card won't work for this application.

Unlike NTP broadcast which goes out on all network ports, NTP Multicast (224.0.1.1) only goes out one Ethernet port (the first network it sees as valid, such as Eth0 for instance). If it's desired to multicast to more than one network, this has to be handled outside of the SecureSync).

We recommended a dumb hub to repeat 224.0.1.1 on all output ports. Then use a firewall with port 123 left open, if it's desired to keep subnets isolated from each other.

NTP drift file

View NTP drift file in CLI: after going to /etc/ntp directory, type **cat ntp.drift** <enter>

NTP Expert Mode

- Refer to the NTP expert mode tech note: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\NTP Expert Mode- Broadcast and Multicast](#)

**NTP Autokey

Refer to (WP-033): [S:\Engineering\Projects\Lafayette\200 Engineering Documents\Working Papers NTP Autokey](#)

[I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\MD5 and Autokey Ap Note](#)

Support for IPv6 Autokey: Apparently, IPv6 Autokey is supported in the new version of NTP (4.2.6p5). If this is correct, since SecureSyncs with version 5.0.0 or higher have NTP v4.2.6p5, they should be compatible with IPv6. Refer to the link above for additional info on Autokey in this document.

External PPS input to SecureSync

For more information, refer to: [1PPS input \(epp0\)](#)

Note: As also discussed in the NTP peering and External PPS input documents, we highly recommend listing more than one NTP server to sync with. Listing just one can cause NTP to continue to toggle between NTP input and Stratum 1 input, with periodic Holdover alarms asserted.

NTP clockstats, loopstats and peerstats

Refer to (in “NTP for all products” towards the beginning of this document): [NTP ClockStats, Loopstats and Peerstats](#)

MD5 Authentication and NTP Autokey protocols

- Refer: [EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\NTP\MD5 and Autokey Ap Note](#)

**RFC 2783 (PPS disciplining)

- Pulse-Per-Second API to discipline the Linux kernel.
- For more info, refer to <http://tools.ietf.org/html/rfc2783>

Q. Is the SecureSync model we have compliant with RFC 2783 (attached)? If yes, is there any documentation we can show that proves it is?

A (Reply From Keith) Regarding your question about RFC 2783, the answer to this is: As of Archive software version 5.0.2, SecureSync does now use an RFC 2783 interface for our timing system to source a 1PPS signal to NTP, to discipline the Linux kernel.

NTP Orphan mode

- Orphan mode replaced the NTP Local clock reference in NTP version 4.2.2
- Now used in SecureSync/9400s to cause NTP to be unusable when the time server is not in sync
- Refer to “Orphan Mode in SecureSyncCustAssist document” for info on NTP Orphan mode

**SNMP/Notifications (SNMP/MIBS/OID numbers)

SNMP package in SecureSync

- SecureSync uses the open source SNMP package called Net-SNMP (NetSNMP)

For more information on SNMP and email alerts, refer to: [I:\Customer Service\EQUIPMENT\SPECTRACOM EQUIPMENT\SecureSync\SNMP](#)

****Troubleshooting issues with SNMP

A) Issues with SNMP polls stopping/restarting later or being very sluggish when walking (walk) the MIBS

- Refer to Salesforce cases such as 12049 (Ultra Electronics <https://na8.salesforce.com/500C000000UdWVe>)
- Likely walking the SNMP MIBS
- Review the **rexd.log** log to see if there are entries showing SNMPSAD being reset (examples below), These entries indicate SNMP is crashing and needing to be restarted to resume operation. (note rexd log is in versions 5.0.2 and higher)

Oct 18 14:17:01 [RESTART] Restarting initiated for snmpsad
Oct 18 14:17:08 [SUCCESS] Successfully restarted snmpsad

Oct 18 16:46:25 [RESTART] Restarting initiated for snmpsad
Oct 18 16:46:32 [SUCCESS] Successfully restarted snmpsad

Follow-up to this issue

(9 Jan 2014 KW) We have since found that one particular NTP Status OID needs to take longer than all of the other OIDs to fully respond. The SNMP Manager is not waiting long enough for it to receive the response from the SecureSync before it's moving on to the next OID in the walk. But the response to the previous query is still waiting inside the SecureSync to be sent, even though the SNMP Manager has already moved ahead to the next OID. This causes the data to be sent to a buffer, and continuously walking the MIB causes the buffer to continue to fill.

The solution is to give the SNMP Manager a little extra time to receive the response to this "NTP" OID. A 10 second timeout is marginal. Sometimes it will provide enough time and others, it misses it. Our Engineers recommend using a timeout value of 20 seconds to be safe. Since changing this timeout, we are no longer seeing this same condition here.

Note: Not all SNMP Managers have ability to change the timeout value. Oleg said the freeware programs seem to be hard-set at 5 seconds, which isn't long enough to handle this particular OID.

does not test email alerts. Refer to the SecureSync SNMP Ap note for more info on testing traps and email alerts

Leap Second insertion

For general info on NTP handling leap seconds, refer to: [Leap Seconds](#)

Q I wanted to make sure that leap seconds events information is automatically passed down to Stratum-3 clients.

A Reply from Sam Otto (2 Apr 2013) which was reviewed by Dave Sohn: Correct, The Stratum-2 does pass along the leap second bits 24 hours prior to the leap second event.

Email from Paul Myers (15 Feb 2013)

The scheduled leap second will tell the KTS clock to make a leap second adjustment.

The KTS will be read by the network processor using the NTP Reference Clock driver.

The NTP daemon will be aware of a pending leap second and will schedule one in the Linux kernel.

There will be a single leap second inserted by the KTS, received on the 60th second of the havequick input, and the NTP and linux kernel will be aware of only a single leap second.

There is not issue with 2 leap seconds, being adjusted.

The NTP step should occur at or be logged shortly after the leap second. I do agree I have seen the step logged slightly late before, but I can't remember under which circumstance of testing. If it was a unscheduled leap second or a scheduled one...

To ensure your customer is satisfied I recommend you have someone perform this test:

- Handset the time to several hours before a leap second adjustment on 2 SecureSyncs and let them sync the linux time to NTP
- Using a SecureSync with HaveQuick output schedule a leap second using the format without notification
- Sync SecureSync with a havequick input card
- Ensure NTP is synced and the time is set correctly.
- Hand set a scheduled leapsecond several hours hence
- Allow the NTP to sync
- Verify the LI bits indicate a leap second is pending
- Configure the Front Panel, ASCII output, etc so you can watch the leap second rollover
- Observe the rollover
- You will observe the 58, 59, 60, 0, 1, 2

- You will observe a 1 second step in the NTP log slightly after the rollover
- This is normal behavior.
- KTS, Linux and NTP are all aware of the 60th second.
- NTP will distribute the scheduled leapsecond by sending leap indicator LI bits set to other NTP servers.

From: Paul Myers

Subject: Leap Second Document

<\\Roc.spectracom.us\ICS\Engineering\Projects\Lafayette\301 Verification Test Results\Release 4.8.2\Leap Second Changes.docx>

This is my first cut at the leap second document. I will improve it where it is not clear, or additions are needed.

In general, what was done was:

- F) Improve Clock Service to better handle leap seconds when operating in Time Scales other than UTC and provide functions to facilitate time scale conversions
- G) Time Manipulation library
- H) Output 60 for the leap second when appropriate
- I) Fix Time conversions so errors don't happen
- J) Fix NTP stratum 2 to avoid premature leap second announcers.
- K) Fix Leap Indictors in any Outputs that were not working
- L) Detect leap seconds as appropriate in any Input References that did not.
- M) Fix any error conditions found
- N) Implement and test HaveQuick Leap Seconds

The document above contains a list of all files changed since 4.8.0 to NOW (pre-4.8.3) which were changed for Leap Second related reasons.

Also, it contains at the end information for Keith to write Leap Second Application note as to what features are improved and why.

I think Keith should read it, if it is not clear enough tell me, and I can fix it, and then he can shorten it to say if you are using ASCII and you need this update. If you don't you may have this problem such as skipped Leap Second, late adjustment, no 60 values, wrong GPS-UTC offset briefly, etc.

I will likely update it with any of Mark's changes and any feedback he has.

Email from Paul Myers about manually scheduling a leap second (14 Feb 2013)

I believe the manual is incorrect about scheduling leap seconds.

Mark Goodlein designed the interface to set Leap Seconds in both the SecureSync and in the KTS.

The time to 'schedule' them was 1 second after the adjustment. In theory they can be added or removed.

The constant is the time after.

I ran the GSG Leap Second test and observed what was 'scheduled' in KTS.



Note that for a +1 adjustment at 23:59:59 on 182/2012 the above scheduled date is shown.

To similarly schedule a leap second you must do the same. SO the 23:59:59 in the manual is incorrect in my opinion.

Note: when testing Leap Second functionality, make sure no external references are connected/present. If a user manually sets a leap second with a reference connected, the reference will interfere with the test results, and may cause abnormal output time stamps!

Email from Paul Myers:

To simulate a Leap Second Rollover you CANNOT have a reference attached as it will try to correct the time if you handset a leap second that is NOT provided by a Reference.

To handset a leap second condition:

- Remove all references.
- Handset the clock to the desired time say 23:58:00 hours Day 366 of a leap year or 365 of a non-leap year
- Handset the rollover to the first second of the next day. 1/year 00:00:00
- Watch the rollover condition

Note: Responses to questions below are from Paul Myers

- To confirm, if an input reference doesn't provide Leap Second pending notification (such as not using extended havequick), a user can still manually schedule a pending leap second via the "Set Leap Second" section of the **Setup- > Time Management** page? Manually scheduling the leap second should result in System Time making a one second time jump at the last second of the scheduled month.

[PEM] The user can schedule a leap second when a reference is present or not.

[PEM] The leap second gets automatically updated if the reference is aware of leap seconds.

[PEM] NTP will be made aware leap seconds from the Reference clock driver or in the case of NTP Stratum 2-15 servers from NTP packets LI bits.

- If the leap second section is filled in by a user (because the input reference can't set these fields), will NTP know to apply a one second jump correction at the last second of the scheduled month? Or, as I suspect, will NTP instead slew its time by one second, once System Time makes the one second time jump at the last second of the month).

[PEM] Yes. NTP will be informed of the pending leap second because the reference clock driver communicates this information along with time to the NTP from the KTS. NTP will make its leap second adjustment 58, 59, 60, 0, 1, by adjusting the kernel time. NTP can step the second and slew in the remainder. If NTP is NOT notified of the pending leap second it will have to step/slew to correct the offset later based upon poll rate.

NTP sets its LI bits to indicate a leap second is pending 24 hours before the leap second insertion.

- If NTP slews its time for the one second time jump that occurs in System Time, over how long of a period will NTP need to slew the time until its correct again? Does the current poll interval affect how long it takes to slew its time by one second?

[PEM] It depends up on poll rate, but scheduled leap seconds are known to the kernel and NTP to be handled. Unplanned offsets can take longer.

LI Bits now displayed in the Status -> NTP page of the browser

Starting in version 4.8.4, the LI bits were added to the NTP input references tables. Earlier versions of software did not

display the LI bits in each row of the tables.

Leap second testing only allows leap second to occur last day of June or last day of December

Paul Myers coded the Leap Second functionality to allow Leap Second to only be able to occur on the last day of June or December. When testing for Leap second, set the leap second to occur on one of these two days only. Then with User mode enabled, manually set the date/time for a day prior to leap second, to see it occur.

NetClock 9400/SecureSync that is synced via NTP

- The following is from <http://www.meinberg.de/english/info/leap-second.htm#irig>:

[IRIG time codes](#) are often used to synchronize time between computers and other devices via cables or fiber optic connections.

Several [IRIG frame types](#) have been specified to transport time information between two IRIG devices. Most of the commonly used IRIG frames carry the day-of-year and the current time, but they do neither contain the year number which would be required to convert the day-of-year to a calendar date unambiguously in leap years and non-leap years, nor the UTC offset of the transported time, or a leap second announcement.

The IRIG frame type **IEEE1344** contains all this information. However, by specification the leap second is announced only about 60 seconds before it actually occurs.

If such an IRIG receiver is used as a reference time source for NTP then there's a good chance the NTP daemon misses the leap second announcement at a polling interval of 64 seconds and thus is unable to handle the leap second correctly. Even if the NTP daemon received the leap second announcement, it was too late to pass the announcement on to the clients, so most of the NTP clients would probably miss the leap second.

This is the reason why in general a [leap second file](#) should be installed for NTP if an IRIG receiver is used as reference time source.

If the NTP server that SecureSync is synced to is synced via IRIG, as IRIG only changed the LI bits one minute before the leap second occurs, will require NTP to step the time about 15-20 minutes thereafter, to account for the one second time change.

Email from Keith to Rob Amos (ASX) 7/13/12

Hi Rob,

We have reviewed the SecureSync logs you sent to us (thanks for sending them to us)!! I have some feedback for you that should help!

To begin, attached are individual documents for each SecureSync, with each document excerpting the log entries relating to the leap second time-frame. At the end of each document is a list of our findings, for that particular SecureSync.

In short summary of all of the logs, the SecureSyncs properly handled the leap second insertion. However, we fell "victim" to the IRIG reference not providing enough advance warning of the pending leap second. Because only one minute of advanced warning was provided to the kernel, the leap second time correction was delayed by several minutes after the leap second insertion occurred.

Now for the details:

First: two points for clarification:

NTP adjusts the SecureSync's kernel "Time" by one second for the leap second insertion.

The System Time's (displayed in the Time Management page of the browser) leap second flag adjusts the Timing System's time scale offsets (such as the UTC to TAI offset, as needed for PTP) by one second when the leap second insertion has occurred.

The SecureSync's System time for its outputs is derived from the kernel time, which is updated by NTP and its selected reference. NTP can select various input references to synchronize with (such as GPS or NTP, for examples). When NTP is synced to GPS (via the System Time) NTP has a direct and continuous time reference to sync with. However, when NTP is syncing to another NTP time server, the time stamps to sync NTP with are only periodically available (with the interval based on the poll rate of its selected NTP server (as determined by NTP, to be between the configured MinPoll and MaxPoll intervals).

Even though the Stratum 1 server only gave one minute of advanced notice of the pending leap second, we were fortunate that the SecureSync had been able to sync to GPS at least once since March. When the SecureSync synced to GPS, it flagged the system to the pending leap second, well in advance. If it hadn't been for this GPS selection, the only way SecureSync would have known to update its time offset corrections (such as the TAI offset) at the moment of the leap second is if NTP had been provided ample notice to the pending leap second. Since GPS had already flagged the leap second prior to the leap second, SecureSync was able to correct the

offsets just after the leap second was asserted.

In addition to the System Time offset for TAI needing to be updated at the leap second, the System time (kernel time) also needed to be updated by one second, as well. NTP updates the kernel (which is the time reference for the system) for this one second correction. As long as NTP can obtain from its selected reference, sufficient notice of the pending leap second before it actually occurs, the kernel time is automatically corrected at the correct second. However, if NTP cannot obtain sufficient advanced notice from its selected reference before it's inserted, the time correction is delayed until it can receive the LI bit change from its reference.

The PTP Option Cards, when configured as a PTP Master, read the System time every second. So once both the UTC to TAI offset as well as the kernel time have been corrected by one second, the PTP Master sends out the corrected time, immediately thereafter.

Specific to the logs you sent:

The logs you sent show that the System's time correction (the kernel "step") occurred on all of the SecureSyncs between 15:29 and 19:53 (Minutes / Seconds) after the leap second had been inserted. This is because this was the first opportunity it had to obtain the LI bit change from its selected NTP reference and to apply the leap second to the kernel time.

If the SecureSyncs had been synced to GPS prior the leap second insertion (instead of to the Stratum 1 NTP server) the SecureSync's time would have adjusted at 23:59:60 two to three seconds after the leap second was inserted, instead of 15 to 20 minutes thereafter (as a result of the poll interval for the Stratum 1 server).

For any future leap second that may occur, we initially discussed potentially having you change both the Min and Max Poll intervals for the Stratum 1 server configuration to "4 (16 seconds)" on the day of the leap second. This would ensure NTP polled the Stratum 1 server every 16 second and therefore a couple of times during the one minute period that the Stratum 1 server has the LI bits set to indicate the pending leap second. However, we tested this and found that only one minute of advanced notice from the NTP reference, even at the quickest possible NTP poll interval, does not provide enough advanced notice to the kernel to apply the time correction at the leap second. Because the kernel was not able to flagged to correct the time at the Leap second, when the selected input is another NTP server, a few polls after the leap second occurred, NTP realized a one second step was needed. So about 15 to 20 minutes later, NTP stepped the kernel time on your SecureSyncs (other SecureSyncs using input references such as GPS, did not need to step the kernel after the leap second- the time was automatically corrected at the correct second because the kernel had ample notice of the pending leap second).

In summary of the above information:

The GPS input had flagged the timing system of the pending leap second, well in advance (GPS started broadcasting this information on the leap second back in the March time-frame) this allowed the timing system to adjust the TAI offset within just a couple of seconds of the leap second. However, the IRIG signal limiting the LI bit change to only one minute did not provide the kernel with enough advanced notice.

So, our recommendation to you, if another leap second is scheduled in the future (and since its unlikely that the IRIG reference can provide a longer advanced notice with the LI bit change occurring earlier than just one minute prior), would be to temporarily select GPS as the highest priority reference (instead of NTP) on the day of the leap second, via the Reference Priority table. This will provide both NTP and the timing system with sufficient advanced notice to prevent the need for NTP to have to step the time several minutes after the leap second has been inserted. Then, switch back to using NTP as the selected reference by making it the highest priority reference. Otherwise, using NTP as the input during the leap second will result in a delay of the one second time correction of the NTP and PTP timing outputs.

PTP Precision Timing Protocol (IEEE 1588) (for all products)

Links

Shortcut to PTP info in custservice folder: <I:\Customer Service\PTP\FCS errors>

Shortcut to Sam Otto's PTP Tech notes: <I:\Customer Service\PTP\Technotes>

Recommended links for PTP information:

<http://ieee1588.nist.gov/>

http://en.wikipedia.org/wiki/Precision_Time_Protocol (not bad actually)

http://ieee1588.nist.gov/2006%20IEEE1588%20Agenda/Eidson_1588_Version%202.pdf (GOOD)

<http://www.webcitation.org/5qaJpYqCH>

<http://www.webcitation.org/5qaBMRXjA>

http://www.butlergroup.ie/wp-content/uploads/wpsc/product-files/854_Calnex_Technical_Brief_IEEE_1588v2_PTP_Mar10.pdf

IEEE-1588 PTP specifications

Shortcut to the Engineering copy of the IEEE1588 standard: [I:\Engineering\Specs and Standards\IEEE \(Institute of Electrical and Electronics Engineers\)\IEEE 1588](I:\Engineering\Specs and Standards\IEEE (Institute of Electrical and Electronics Engineers)\IEEE 1588)

- For the latest specs, refer to IEEE-1588-2006V2, at the following link in Sharepoint

<https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/Projects/GeneralPTP/SitePages/Home.aspx?RootFolder=%2FSpectracom%2FEngineering%2FProjects%2FGeneralPTP%2FShared%20Documents%2FStandards&FolderCTID=0x0120001C144F4F864D1D45AC2929A4327F8AB1&View={D793DF9A-1DF4-4C45-BF93-0BA34459C1FE}&InitialTabId=Ribbon%2EDocument&VisibilityContext=WSSTabPersistence>

- Other data also in <I:\Company Wide\Project Folders\Standard\LEGO\Project Development Folder\9. Standards\IEEE1588>

PTP v2.1 Authentication

excerpt below from the Greyware Domain Time website (16 July 2019): <https://www.greyware.com/kb/kb2019.331.asp>

The forthcoming version 2.1 of IEEE 1588 (PTP) allows the option for grandmasters to add an Authentication TLV to each message they send. The specification supports multiple authentication methods using symmetric keys. Key selection and distribution methods, as well as the cryptographic algorithms, are implementation-dependent. The only requirement is that HMAC-SHA256-128 must be supported. PTP v2.1 is not yet standardized, so Domain Time's support for Authentication may need to evolve in future versions.

Each Authentication TLV carries a Security Parameter Pointer ("SPP"), which may be used in conjunction with a Key Distribution Center ("KDC") to select a group of keys. The SPP may also be static, without reference to a KDC, in which case the keys themselves must also be static and already known to the receiver. Valid values for the SPP are 0-255, inclusive.

Each Authentication TLV also carries a KeyId, a 32-bit value indicating which key associated with the SPP is being used to sign the message. Implementations are free to use a single KeyId for all message types, or separate KeyIds for each message type. Domain Time only allows KeyIds in the range of 1-65535 (inclusive).

Authentication TLVs do not contain information about the cryptographic algorithm that corresponds to the hash being sent. When using a KDC, the SPP can be used to fetch this information from the KDC. If the SPP is static, HMAC-SHA256-128 must be assumed.

*PTP v1 versus PTP v2

- For info on PTPv1, refer to: (IEEEspec1588-2002) <I:\Customer Service\PTP\PTPv1>

(Update to info below, Oct 2016) We only support PTPv1 via the timekeeper license. The 1204-12 and 1204-32 PTP Cards do not support PTPv1.

(July 2014) We only support PTPv2 (we don't support PTPv1). PTPv2 added Unicast mode, transparent clocks, redundancy, greater accuracy and higher sampling/message rates, etc.

Email from Dave Lorah (30 July 14) PTPv1 vs PTPv2 is described here:

<http://tekroninternational.blogspot.com/2009/10/difference-between-version-1-and.html>

Spectracom is looking into implementing PTPv1 in an upcoming firmware version to support older legacy systems that cannot be updated to PTPv2. This should be available in the next year or so.

GENERAL INFO ABOUT PTP

*Accuracies of PTP

Accuracies of the PTP input sync is typically measured as a few microseconds unless direct connect of the Master and the Slave together. Performance depends on Variable Packet Delay (VPD) of network elements (PTP-optimized network can achieve <100 nsec accuracy).

From the TSync-PCIe datasheet:

8 nS (± 4 nS) packet timestamping- This is the max resolution of the PTP packets.

30nS accuracy Master to Slave via cross-over cable. This is direct-connect with no routers/switches or collisions

1024 Syncs/sec = (This is actually about 980 Syncs/Sec as measured by Engineering). This is the number of packets in an ideal environment that can be exchanged between the Master and Slave in the period of time needed for the packet exchanges to occur.

Q. Can we get some testing results master to slave time error at a day interval, e.g.? Both with crossover cabling and in a LAN/WAN (if available).

A. (Response from John Fisher) Our tests with a crossover cable demonstrate +/- 25 nS accuracy, 3 sigma. We achieve this because we have the highest resolution timestamping hardware in the industry -- +/- 4 nS. For a LAN/WAN environment, the performance is entirely dependent on the switches, routers and traffic on the network, and performance varies widely. If you are able to control or influence the switches and routers in your application, then using PTP Enabled switches will greatly improve performance. These switches perform the PTP Transparent Clock function to eliminate the Variable Packet Delay (VPD) through the network which degrades the accuracy.

Q. What would the accuracy be using our PTP and their PTP? Do we have a relationship with Cisco?

A. Reply from Denis Regarding accuracy of PTP with Cisco Switches; because PTP accuracy is heavily influenced by the network infrastructure we cannot give a precise accuracy spec. Below is some information on how PTP works and what we've seen with other customer who work with Cisco:

Even though PTP is a master/slave protocol, PTP communication is bi-directional. PTP makes a fundamental assumption that the delays on a network are symmetrical. PTP also works best when the delay does not change much with time. Modern switching equipment has all manner of queues and delay sources that can foul this up – if packets are queued in one direction and not the other, this will affect timing performance. To help compensate for this, there are two special types of PTP equipment defined in the standard. One type or the other is implemented in "PTP Enabled" switches:

Ordinary Clocks/Transparent Clocks/Boundary Clocks

A) Ordinary Clocks (OC)

- Switches that just pass-through the PTP packets with no modifications.
- No compensation for the switch delays

Note: Excessive jitter through the ordinary clock switch can result in high 1PPS phase and intermittent Frequency Error alarms being asserted (specific example-Raytheon was seeing phase errors of 60ns up to about 1 microsecond phase errors through a single OC switch with only one Master and one Slave connected to it).

B) Transparent Clock (TC)

- Devices that time packet delays and put this into the message, so the slaves can account for the delays.
- Similar to an Ordinary clock, except the switch adds its delays to the Sync packet's correction field before sending it back out.

Transparent Clocks timestamp the delay through the switch, and inserts the delay value on-the-fly into the PTP Sync packet. The PTP device takes this delay value into account when calculating its time, effectively accounting for any variable delay through the switch.

Note: The Transparent Clock functionality may need to be enabled in the switch. If it's not enabled, it will operate like a standard switch. It will still pass PTP packets but will not insert its delay into the PTP Sync packets. So, the PTP Slave will not be able to account for its delays.

C) Boundary Clock (BC)

- Devices that place a Slave/Master on each subnet. The purpose is to segment networks to avoid the slaves having multiple hops (Like NTP, PTP assumes path delay is the same in both directions)

"A boundary clock is an IEEE 1588 component that allows the synchronization of IEEE 1588 clocks across subnets defined by a router or other devices that blocks the transmission of all IEEE 1588 messages. A boundary clock serves to eliminate the large fluctuations in communication latency typically generated by routers and similar devices.

Boundary Clocks run separate PTP clocks on each network interface port. These clocks are linked so that if one clock is connected to the Best Master, all the other clocks can obtain their time from it and become "mini-masters" (my term). This breaks up the timing path into separate parts, and the variable delay through the switch is now "in between" the timing paths, and no longer affects timing.

Cisco has very good PTP equipment. Cisco thinks that transparent clocks do not scale well (there is only one field in the PTP protocol for delay, so once you layer a few clocks it can get messy) so they are pushing Boundary Clocks to their financial customers (which would also most likely apply to defense customers who also have tight timing requirements).

All switches will accept PTP packets, but only switches that are transparent clocks or boundary clocks will perform well. We/Spectracom products run very well through a crossover cable. But, again, PTP accuracy is heavily dependent on the network infrastructure.

How do IEEE 1588 Boundary Clocks work?

An IEEE 1588 Boundary Clock serves as a time transfer standard between the subnets defined by the router or other network device. The router or other device must be configured to block all IEEE 1588 messages. The boundary clock has a network connection to each of the subnets. When viewed from a subnet the boundary clock appears exactly like any other (ordinary) 1588 clock in the system. Within a subnet the ordinary clocks and the portion of the boundary clock visible from the subnet synchronize with each other as though they were all ordinary clocks. The boundary clock itself resolves all of the times of the several subnets by establishing a parent child hierarchy of clocks. In a system with a single IEEE 1588 Boundary Clock, the boundary clock will typically be the at the root of this hierarchy and will be the master clock for all of the clocks in each of the subnets.

In addition to the synchronization functionality, an IEEE 1588 Boundary Clock provides for the appropriate retransmission of 1588 management messages.

Known issues/Specific configurations with PTP boundary switches

A) Known issues:

1. Cisco/Nexus switch reporting "Uncalibrated" and not syncing to PTP Grandmaster

One example- I just performed a quick Google search of "Cisco" and "uncalibrated" and found a known issue related to this (not sure if this applies to your particular Model, as excepted below

<https://quickview.cloudapps.cisco.com/quickview/bug/CSCuy79978>

Products (12)

Cisco Nexus 6000 Series Switches

Cisco Nexus 5548P Switch

Cisco Nexus 5596UP Switch

Cisco Nexus 5624Q Switch

Cisco Nexus 6004 Switch

Cisco Nexus 5672UP Switch

Cisco Nexus 6001 Switch

Cisco Nexus 5548UP Switch

Cisco Nexus 5696Q Switch

Cisco Nexus 56128P Switch

Known Affected Releases 7.1(1)N1(1)

Description (partial)

Symptom:

PTP state stuck in "Uncalibrated" and corrections are not happening.

Conditions:

this problem will be seen on nexus n56 series switches when ND ISSSU is preformed from any version before 7.1.0 to later versions.

B) Specific PTP boundary switch configuration requirements/troubleshooting

1. Cisco Nexus 3000/9000 series (such as Model 3548 for instance)

➤ Refer to sites such as:

➤ <https://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/products-installation-and-configuration-guides-list.html>

➤ https://www.cisco.com/c/en/us/products/collateral/switches/nexus-3000-series-switches/white-paper-c11-731501.html#_Toc386062595

Report from a customer (24 Apr 18) I believe Cisco nexus 3548X only support IEEE 1588-2008 PTPv2 in **Multicast** mode. Should we disable Unicast? Can you walk me through how to do so?

It's using **2 step boundary mode**

https://www.cisco.com/c/en/us/products/collateral/switches/nexus-3000-series-switches/white-paper-c11-731501.html#_Toc386062595

Cisco Nexus 3548 PTP Configuration Validation

The commands shown here can be used to validate PTP on the Cisco Nexus 3548.

switch# show clock

This command can be used to verify that the switch clock is synchronized with the grandmaster clock. You cannot verify precise accuracy with this command-line interface (CLI) command, but you can at least verify that the time of day matches the grandmaster, if **clock protocol ptp** was configured.

switch# show ptp clock

This command displays the properties of the local clock, including clock identity.

This is an example of **show ptp clock** output:

switch# show ptp clock

PTP Device Type: Boundary clock

Clock Identity : 30:f7:0d:ff:fe:9b:e2:41

Clock Domain: 0

Number of PTP ports: 42
Priority1 : 255
Priority2 : 255
Clock Quality:
Class : 248
Accuracy : 254
Offset (log variance) : 65535
Offset From Master : 2
Mean Path Delay : 296
Steps removed : 1
Local clock time: Mon Dec 23 09:51:30 2013

***switch# show ptp parent**

This command displays the properties of the PTP parent. It is useful for verifying the parent clock's identity.

This is an example of **show ptp parent** output:

```
switch# show ptp parent
PTP PARENT PROPERTIES
Parent Clock:
Parent Clock Identity: 00:b0:ae:ff:fe:02:8f:fb
Parent Port Number: 1
Observed Parent Offset (log variance): N/A
Observed Parent Clock Phase Change Rate: N/A
Grandmaster Clock:
Grandmaster Clock Identity: 00:b0:ae:ff:fe:02:8f:fb
Grandmaster Clock Quality:
Class: 6
Accuracy: 33
Offset (log variance): 25600
Priority1: 0
Priority2: 0
```

switch# show ptp brief

This command displays the PTP state of all interfaces. A PTP port can be in one of the following three states:

- Master: The port is the source of time on the path served by the port.
- Slave: The port synchronizes with the device on the path on the port that is in the master state.
- Disabled: PTP is not enabled on this port.
- Passive: The port is not the master on the path, nor does it synchronize with a master.

Because the Cisco Nexus 3548 is a PTP boundary clock and supports only one PTP domain, the switch can have only one slave port. If the switch has one slave port already, a second port connected to a second grandmaster will be in the passive state. When the first grandmaster or the first slave port fails, BMCA will move the previously passive port to a slave state. With this process, grandmaster redundancy can be achieved.

This is an example of **show ptp brief** output:

```
switch# sh ptp brief
PTP port status
-----
Port State
-----
Eth1/1 Slave
Eth1/2 Master
Eth1/3 Master
Eth1/4 Master
Eth1/5 Master
Eth1/6 Master
...
Switch#
```

switch# show ptp corrections

This CLI command displays the last few PTP corrections.

Here is an example of **show ptp corrections** output:

PTP past corrections

Slave Port SUP Time Correction(ns) MeanPath Delay(ns)

Eth1/46 Mon Dec 23 09:52:11 2013 48581 -1 293
Eth1/46 Mon Dec 23 09:52:12 2013 49318 3 297
Eth1/46 Mon Dec 23 09:52:13 2013 49193 -8 297
Eth1/46 Mon Dec 23 09:52:14 2013 49208 12 298
Eth1/46 Mon Dec 23 09:52:15 2013 48625 -3 298
Eth1/46 Mon Dec 23 09:52:16 2013 47607 -13 295
Eth1/46 Mon Dec 23 09:52:17 2013 49091 0 295
Eth1/46 Mon Dec 23 09:52:18 2013 47961 2 295
Eth1/46 Mon Dec 23 09:52:19 2013 48005 -1 295
Eth1/46 Mon Dec 23 09:52:20 2013 48350 0 296
Eth1/46 Mon Dec 23 09:52:21 2013 48507 -5 292
Eth1/46 Mon Dec 23 09:52:22 2013 48105 2 292
Eth1/46 Mon Dec 23 09:52:23 2013 48188 12 301
Eth1/46 Mon Dec 23 09:52:24 2013 48021 6 301
Eth1/46 Mon Dec 23 09:52:25 2013 48239 -12 296

PTP module chipset

Q. Does Spectracom use their own chip for those PTP products?

A. (Email from Denis Reilly to Yang Yang 11/30/11)

We are using an Ethernet PHY chip (called the "PHYTER") with PTP timestamping capability. This PHY is attached to a microcontroller on the PTP board which is running the PTP stack in its microcontroller firmware.

This gives us some nice performance advantages:

Even though we are only 10/100, since we do our timestamping in the PHY we get the best timestamping resolution we can (+/- 4 ns). Many other products do their timestamping in the MAC, which has worse resolution.

Also, since the PTP stack is being run on the PTP hardware directly, it performs much better (and with lower overhead) than other PTP solutions that run on hardware that isn't dedicated to PTP. As a result, as a master we can synchronize more slaves than some of the other PTP Grand Masters out there.

IPv6 for PTP

Email from Denis (8/24/12) As far as I know, there is nothing on our roadmap for IPv6. There are products that exist, because there will be some IPv6 testing at next month's plugfest. But the bulk of the testing there is still IPv4, so I imagine that's where the bulk of the products are, too.

*IEEE 802.1AS (PTP Timing and Synchronization for time-sensitive applications)

- This is a PTP Standard for Timing and Synchronization of time-sensitive applications (such as for audio and video across LANS where transmission delays are symmetrical)
- As of at least Nov, 2016, we don't support this standard with SecureSync PTP Option Cards (1204-12 or 1204-32) or TSync-PTP boards (not sure about Legacy VelaSyncs, but probably not with this device either).

Email from Dave Sohn (18 Nov 16): We do not have support for 802.1AS with our PTP offering, and it isn't on our roadmap at this time. What is the size of the opportunity?

Per <http://www.ieee802.org/1/pages/802.1as.html>

The full title of this PAR is "Standard for Local and Metropolitan Area Networks - Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks".

This standard specifies the protocol and procedures used to ensure that the **synchronization requirements are met for time sensitive applications, such as audio and video, across Bridged and Virtual Bridged Local Area Networks consisting of LAN media where the transmission delays are fixed and symmetrical**; for example, IEEE 802.3 full duplex links. This includes the maintenance of synchronized time during normal operation and following addition, removal, or failure of network components and network reconfiguration. It specifies the use of IEEE 1588 specifications where applicable in the context of IEEE Stds 802.1D and 802.1Q. Synchronization to an externally provided timing signal (e.g., a recognized timing standard such as UTC or TAI) is not part of this standard but is not precluded.

This standard enables stations attached to bridged LANs to meet the respective jitter, wander, and time synchronization requirements for time-sensitive applications.

** IEEE 802.1Q (VLANs/VLAN trunking / VLAN tagging)

Q. Does SecureSync-PTP support VLANs

A. Reply from Denis (6 May 13) Yes it does.

Note:

- **PTP Option Card** = Yes. Does support VLANs
- **Eth 0 through Eth3 interface ports** = No. Does not support VLANs

From Wikipedia

IEEE 802.1Q is the [networking](#) standard that supports [Virtual LANs](#) (VLANs) on an [Ethernet](#) network. The standard defines a system of **VLAN tagging** for [Ethernet frames](#) and the accompanying procedures to be used by [bridges](#) and [switches](#) in handling such frames. The standard also contains provisions for a [quality of service](#) prioritization scheme commonly known as [IEEE 802.1p](#) and defines the [Generic Attribute Registration Protocol](#).

Portions of the network which are *VLAN-aware* (i.e., IEEE 802.1Q conformant) can include VLAN tags. Traffic on a *VLAN-unaware* (i.e., IEEE 802.1D conformant) portion of the network will not contain VLAN tags. When a frame enters the VLAN-aware portion of the network, a tag is added to represent the VLAN membership of the frame's port or the port/protocol combination, depending on whether port-based or port-and-protocol-based VLAN classification is being used. Each frame must be distinguishable as being within exactly one VLAN. A frame in the VLAN-aware portion of the network that does not contain a VLAN tag is assumed to be flowing on the native (or default) VLAN.

The standard was developed by [IEEE 802.1](#), a [working group](#) of the [IEEE 802](#) standards committee and continues to be actively revised with notable revisions including [IEEE 802.1ak](#), [IEEE 802.1Qat](#) and [IEEE 802.1Qay](#).

VLAN-unaware (i.e., IEEE 802.1D conformant) / **VLAN-aware** (i.e., IEEE 802.1Q conformant)

Traffic on a *VLAN-unaware* (i.e., IEEE 802.1D conformant) portion of the network will not contain VLAN tags.

When an Ethernet frame enters the VLAN-aware portion of the network, a tag is added to represent the VLAN membership of the frame's port or the port/protocol combination, depending on whether port-based or port-and-protocol-based VLAN classification is being used.

the VLAN tag is stripped before the frame leaves the VLAN-aware network.

As of at least Apr 2017, we do not support VLAN tagging.

Q. Does SecureSync support “.1 Q (1Q) trunking”?

A. **Reply from Denis Reilly (8/6/12)**

They may mean 802.1Q trunking: http://en.wikipedia.org/wiki/IEEE_802.1Q

Everything I know about it I learned from reading that Wiki article just now. But it looks like this is basically VLAN support. Some VLAN support was released for PTP as part of the last release, but I haven't tested it beyond looking at the status page.

Once Sam is done with using the PTP Testbed for Morgan Stanley stuff, maybe we should append some quality time with the VLAN feature and see if it can be used in the way the customer wants. I think it can, but we should check.

A **Another email from Dennis Reilly (9 Jul 13)**

VLAN tagging is simply adding data (“tagging”) Ethernet frames with identifying information. This information can be used to filter, separate, and prioritize packets based on the tag information. A collection of VLANs that are routed on the same routers is a trunk.

Our VLAN tagging support is limited to the PTP card: we can tag frames generated by the PTP card so that routers could prioritize them if they were set up to do so. But again, I haven't played with this at all. It sounds like a good use for the PTP testbed.

There is no support for any tagging on any of the other SecureSync ports. Odds are, if a customer is asking about VLAN support for the SecureSync in general, the answer is “no”. And I think any customer who is asking about “trunking” probably is thinking about the SecureSync in general.

In all of my looking into this topic, I see that VLAN tagging is mainly associated with routers and switches. Perhaps there are folks who are thinking of using the SecureSync OC06 as a router? I think we should discourage that: although we can set up routing among the 3 interfaces on the 1GB Ethernet card, we don't support all the features that a true router would.

VLAN Trunking Protocol (VTP)

VTP is a [Cisco proprietary protocol](#) that propagates the definition of Virtual Local Area Networks ([VLAN](#)) on the whole local area network.^[1]

Good info Email from Dick Fox to a dealer

I discussed the issue of VLAN with Spectracom's IT manager today. He explained NTP's and VLAN compatibility in terms

of the OSI model.

This helped to clarify the level of compatibility for me. I have attached a document that explains the OSI Model and different Network protocols

VLAN functionality is part of Layer 2 (Data Link Layer)

NTP functionality is part of layer 3 / layer 4 in the OSI model

So NTP is built on top the lower level layers and NTP functionality is transparent of

1. The characteristics of the physical layer (layer1)
2. The characteristics of the data link layer (layer 2)

NTP is defined by RFC 958 and is part of the TCP/IP protocol suite

The transport layer (layer 4) is where protocols like TCP/IP and UDP are defined.

This is why you have to open UDP port 123 in the firewall to enable NTP through a firewall.

To be clear NTP's functionality and operation is independent of the physical and data link layers.

That is why Spectracom's says these layers are transparent to NTP and why we work in networks where VLAN are define.

Recommendations

We can tell the network designers on the project that they can go about designing their VLAN architecture without concerns for whether Spectracom's NTP Servers will work on their VLANs.

If this is their concern, then they should be satisfied with this answer

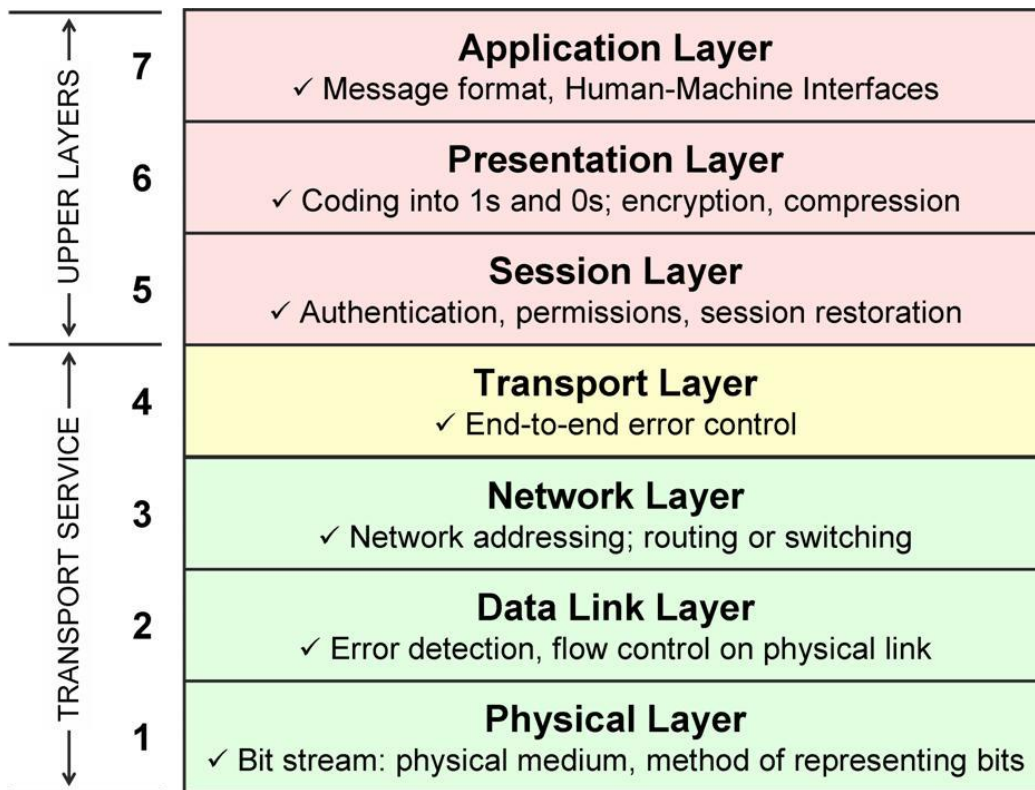
If they want something more than this, then we need to talk some more!

If they want to assign each NTP servers to only accept requests from clients on a specific VLAN, based on a VLAN –tags, then we need to discuss this some more.

Let me know what you find out.

The good thing here is we are explaining this in terms of the OSI model.

This is a language they should understand.



Gigabit Ethernet for PTP

Q. Do the TSync PTP modules and SecureSync-PTP Option Cards support “GE” (Gigabit Ethernet)

A. Regarding your earlier question on “GE”, we are assuming you are referring to Gigabit Ethernet. If this is correct, at this time, the PTP module only supports 10/100 base-T only. There are no plans at this time to add this capability to the PTP modules. For our internal reference, how important is Gigabit operation for your particular applications?

Status update to this (14 Feb 2013) According to Sam Otto, we are working on implementing a 1Gb Ethernet interface to the PTP Option Cards.

Connecting a TSync-PTP to a 1000 base-T Gigabit switch (one that does not support 10/100 base-T connection

Per Denis Reilly- This will not prevent PTP packets from getting through. They will still get through. But because the switch has to queue packets when going from 1000 to 100, they may be delayed, so the timing of the Slave could be slightly degraded because of this. But he also mentioned that if you have a 100base-T master and a 100 Base-T Slave on either side of a Gigabit switch, this essentially negates the processing delays because its happening on both end,

ITU-T Telecom Standards (G.826x and G.827x, such as SyncE)

- Refer to **Standards** [I:\Engineering\Specs and Standards\ITU\(CCITT\)\G series](I:\Engineering\Specs and Standards\ITU(CCITT)\G series)

ITU-T Standards (g.8265 series)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

A) Frequency sync

G.826x (G.8260, G.8261, G.8262, G.8263, G.8264, G.8265)

- **G.8620** provides definitions, terminology and abbreviations used in ITU-T recommendations
- **G.8261** defines sync aspects in packet networks. Specifies max network limits of jitter/wander that shall not be exceeded.
- **g.8262** SyncE (Synchronous ethernet)
- **g.8263** outlines requirements for timing devices used in synchronizing network equipment that operates in the interworking function (IWF) and other network elements as defined in Recommendation ITU-T G.8261/Y.1361. This Recommendation defines the requirements for packet-based equipment clocks.
- **g.8264** ITU-T Rec. G.8264 describes the specification of Ethernet Synchronization Messaging Channel (ESMC)
- **g.8265** contains the ITU-T precision time protocol (PTP) profile for frequency distribution without timing support from the network (unicast mode). It provides the necessary details to utilize IEEE 1588 in a manner consistent with the architecture described in Recommendation ITU-T G.8265/Y.1365. This version of the Recommendation defines the PTP profile for unicast mode only. Future versions of the Recommendation will contain a separate profile for a mixed unicast/multicast case

B) Phase/Time Sync

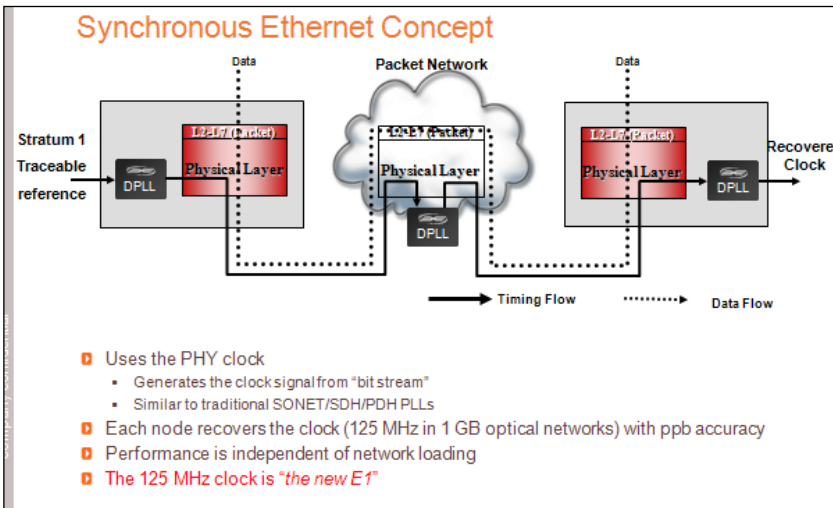
G.827x (G.8271, G.8272, G.8273, G.8275)

- **G.8271/Y.1366** defines time and phase synchronization aspects in packet networks.
- **G.8272** specifies requirement for enhanced primary reference time clocks.
- **G.8275** describes the architecture and requirements for packet-based time and phase distribution in telecom networks

Per Dave Sohn (6 Oct 17) Our Rb SecureSyncs with GPS and the 1204-32 cards can be configured to operate according to the G.826x specs. We do not have compatibility with the G.827x specs

ITU-T Standard G.8262 – SyncE (Sync-E) (Synchronous Ethernet mode)

- ITU-T Rec. G.8262 specifies Synchronous Ethernet clocks for SyncE
- Refer to: <http://www.silabs.com/Support%20Documents/TechnicalDocs/AN420.pdf>
- Also refer to the STA-61: [STA-61 \(STA61\) Sync Tester/Analyzer](#)



This mode places a 125 MHz carrier frequency on the PTP network, as a frequency input reference for PTP Slaves that support this mode for frequency locking.

When the SyncE mode is enabled, and the SecureSync/ TSync board is configured as a PTP Master, the PTP Module will output this 125MHz carrier.

When SyncE mode is enabled, and the SecureSync/ TSync board is configured as a PTP Slave, the PTP Module will accept this carrier frequency.

Sync-E removed from SecureSync's web browser

- **Note:** SyncE was removed from the web browser in v4.8.8 (Dec 2012), as it's not fully implemented.

Email from Bill Glase (20 Sept 13) our PTP products lock the Ethernet clock to the timing system; and therefore are capable of acting as a Sync-E master with traceability to GPS, etc. Informal testing with the STA-61 has confirmed that our master meets the performance requirements of a Sync-E master.

However, they do not implement the Sync-E messaging (ITU-T Rec. G.8264) which probably limits the applications in which it can be used.

Email from Bill Glase (20 Sept 2013) We don't support any kind of ESMC (those are messages sent from the Ethernet port that indicate things like whether the clock is synchronized, etc.)

I have it on the list to think about for 2014 engineering, but we definitely need to understand the applications a bit better. Sync-E is most commonly used in telecom right now which is not a target area. But are there applications that would make it worth adding to our products?

***ITU-T Standard G.8264 (ESMC)/ Messaging Channel for PTP

- ITU-T Rec. G.8264 describes the specification of Ethernet Synchronization Messaging Channel (ESMC)

From Wikipedia: In SDH, the SSM provides traceability of synchronization signals and it is therefore required to extend the SSM functionality to Synchronous Ethernet to achieve full interoperability with SDH equipment. In SDH, the SSM message is carried in fixed locations within the SDH frame. However, in Ethernet there is no equivalent of a fixed frame. The mechanisms needed to transport the SSM over Synchronous Ethernet are defined by the ITU-T in G.8264 in cooperation with IEEE. More specifically, the ESMC, defined by the ITU-T is based on the Organization Specific Slow Protocol (OSSP), currently specified in IEEE 802.3ay. The ITU-T G.8264 defines a background or heart-beat message to provide a continuous indication of the clock quality level. However, event type messages with a new SSM quality level are generated immediately.

The ESMC protocol is composed of the standard Ethernet header for a slow protocol, an ITU-T specific header, a flag field and a type length value (TLV) structure. The SSM encoded within the TLV is a four-bit field whose meaning is described in ITU-T G.781.

***ITU-T Standard G.8265 (Packet over Transport aspects- quality and availability targets)

- For SecureSyncs, refer to: [...\SecureSync Option Card information.pdf](#)
- Refer also to <https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/Projects/GeneralPTP/SitePages/Home.aspx?RootFolder=%2FSpectracom%2FEngineering%2FProjects%2FGeneralPTP%2FShared%20Documents%2FStandards&FolderCTID=0x0120001C144F4F864D1D45AC2929A4327F8AB1&View={D793DF9A-1DF4-4C45-BF93-0BA34459C1FE}&InitialTabId=Ribbon%2EDocument&VisibilityContext=WSSTabPersistence>

ITU-T Standards (g.8275 series) (8275 series not currently supported)

- As of at least versions 5.8.1 and below, **we do not support the 8275 series** with our PTP Option Cards (1204-3B, 1204-32 or 1204-12)

email from Jean Arnold (25 July 18) (pertaining to at least version 5.8.1 and below): Hi Keith, We do not support G.8275.1 on any of our product, but we do support G.8265.1.

Q Do you have plan to support G8275.1 profile?

A Keith's response (25 Jul KW) (applies to at least versions 5.8.1 and below): like the response above, we do not currently support the G.8275 series PTP specifications (including G.8275.1), and I am not aware of any plans at this time, for us to add support for this PTP profile. This is a seldom-received request. However, our SecureSync Product Manager might consider adding it to a future software release, depending on the size of a customer order to justify us adding it (or for an NRE fee that your customer could pay for this capability to be added).

ITU-T Standard G.8275.1/ G.8275.2 (PTP “Telecom profile” for phase/time synchronization with full timing support from the network)

- For SecureSyncs, refer to: [...\SecureSync Option Card information.pdf](#)
- As of at least versions 5.8.1 and below, we do not support the 8275 series with our PTP cards.

email from Jean Arnold (25 July 18) pertaining to at least version 5.8.1 and below: Hi Keith, We do not support G.8275.1 on any of our product, but we do support G.8265.1.

- For more info on this profile, refer to sites such as:
<https://www.cisco.com/c/en/us/td/docs/routers/asr903/software/guide/timing/16-5-1/b-timing-sync-xe-16-5-asr900/g-8275-2.html> or

- https://www.cisco.com/c/en/us/td/docs/wireless/asr_901/Configuration/Guide/b_asr901-scg/b_asr901-scg_chapter_0111100.pdf

Q Do you have plan to support G8275.1 profile?

A Keith's response (25 Jul KW) (applies to at least versions 5.8.1 and below): like the response above, we do not currently support the G.8275 series PTP specifications (including G.8275.1), and I am not aware of any plans at this time, for us to add support for this PTP profile. This is a seldom-received request. However, our SecureSync Product Manager might consider adding it to a future software release, depending on the size of a customer order to justify us adding it (or for an NRE fee that your customer could pay for this capability to be added).

Why G.8275.1?

The G.8275.1 profile is used in mobile cellular systems that require accurate synchronization of time and phase. For example, the fourth generation (4G) of mobile telecommunications technology.

The G.8275.1 profile is also used in telecom networks where phase or time-of-day synchronization is required and where each network device participates in the PTP protocol.

Because a boundary clock is used at every node in the chain between PTP Grandmaster and PTP Slave, there is reduction in time error accumulation through the network.

Restrictions for Using the G.8275.1 Profile

- PTP Transparent clocks are not permitted in this profile.
- Changing PTP profile under an existing clock configuration is not allowed. Different ports under the same clock cannot have different profiles. You must remove clock configuration before changing the PTP profile. Only removing all the ports under a clock is not sufficient.
- One PTP port is associated with only one physical port in this profile.
- There is no support for BDI and VLAN.
- Signaling and management messages are not used.
- PTP message rates are not configurable.
- Non-hybrid T-TSC and T-BC clock configurations are not supported.
- When the Cisco ASR900 routers with RSP2 or RSP3 modules are configured with G.8275.1 Hybrid Boundary clock (T-BC) or Hybrid Slave clock (T-TSC), the combination of PTP and SyncE drives all timing outputs except BITS. This implies that clock outputs are compliant to G.8273.2 and track the Hybrid PTP clock. BITS output always tracks only to the input electrical clock and is not influenced by PTP.
- Virtual port is not supported on the Cisco RSP2 Module.

Contract Negotitation/Unicast/Multicast/Minicast/Hybrid modes

- Both Unicast and Minicast modes were added to SecureSync in Archive version 4.8.8 (Dec 2012, ECN 3099)
- Only Multicast mode was available in SecureSync versions 4.8.7 and prior.

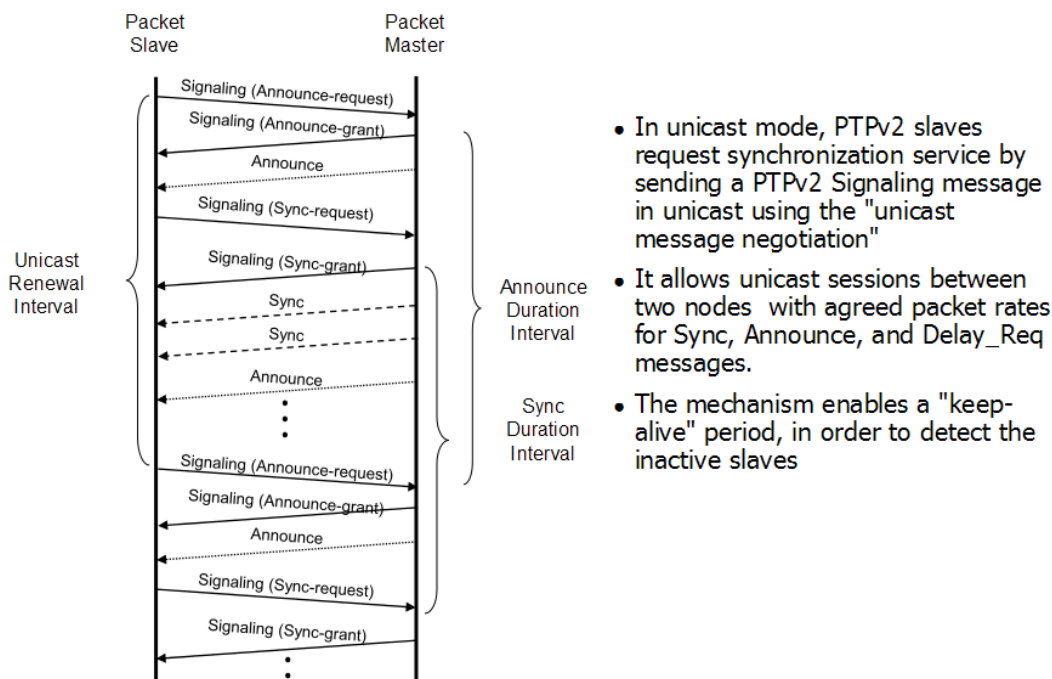
Unicast Contracts/contract negotiations

- In Unicast mode, there are three contracts negotiated between Master in Slave
 - In **Unicast** mode, Slaves shall request unicast contracts for the **Announce**, **Sync** and **Delay_Resp** packets.
 - In **minicast** mode, Slaves only request unicast contracts for the Delay_Resp packets (and so Delay_Req packets). Announce and Sync packets are still sent in multicast mode by the Master.

Unicast negotiation info <https://blog.meinbergglobal.com/2016/11/29/art-negotiation-ptp-way/>

From: http://www.chronos.co.uk/files/pdfs/itsf/2011/Day3/1425_IEEE-Silvana_Rodrigues.PDF

Unicast request mechanism



Online videos that discuss PTP Multicast mode (recommended by Sam Otto, 8 May 2013)

StormWind Live Cisco Learning Network on Youtube

Multicast Part 1 - Intro

<http://www.youtube.com/watch?v=AvbSMBKBZgY>

Multicast Part 2 - Addressing

http://www.youtube.com/watch?v=1_4MOkifX7I&feature=endscreen&NR=1

Multicast Part 3 - Components

<http://www.youtube.com/watch?v=sM0oQxYfbys&feature=endscreen&NR=1>

Multicast Part 4 PIM Dense Mode

<http://www.youtube.com/watch?v=zBiEztnKfyw&feature=endscreen&NR=1>

Multicast Part 5 - PIM Sparse Mode

<http://www.youtube.com/watch?v=OMRByA64xuA&feature=endscreen&NR=1>

Multicast Part 6 AutoRP

<http://www.youtube.com/watch?NR=1&feature=endscreen&v=KpZTf4KC3tE>

Email from Michel Reyverand (8/31/12) about Unicast, Minicast and Multicast

The minicast is a special case of the unicast mode.

In unicast mode, Slaves shall request unicast contracts for the Announce, Sync and Delay_Resp packets.

In minicast mode, Slaves only request unicast contracts for the Delay_Resp packets (and so Delay_Req packets).

Announce and Sync packets are still sent in multicast mode by the Master.

On Master Side:

- Multicast: multicast is allowed (since power-up) for sync, announce and delay_resp packets.
- Minicast mode: multicast is allowed (since power-up) for sync and announce packets (not for delay_resp packets).
- Unicast mode: multicast is prohibited (since power-up).

On Slave side:

- Unicast mode: Slave requests unicast contracts for Announce, Sync and Delay_Resp packets.
- Minicast mode: Slave requests unicast contracts for Delay_Resp packets only.
- Multicast: Slave doesn't request unicast contracts. Will sync to a Master in multicast mode (may be in minicast mode, I'm not sure)

When a Slave is in unicast mode (or minicast mode), the Master will run in unicast/minicast mode even if it is set in Multicast mode, because when the Slave unicast requests are granted by the Master, the Master switches into unicast mode with this Slave.

I've said that mix of transmission modes is out of spec. because the transmission mode is a network setting that has not to be changed once the network switches are set in one given transmission mode. Masters and Slaves should be set with the same transmission mode to ensure good conditions to sync each other.

PTP Multicast mode

- Multicast mode is "one to many" messaging.
- All SecureSync software versions (since PTP Option Card release) have supported PTP multicast mode.
- PTP Multicast address: **224.0.1.129**

IGMP (Internet Group Management Protocol)

- Refer to: https://en.wikipedia.org/wiki/Internet_Group_Management_Protocol

IGMP versions

- IGMPv1 (RFC 1112)
- IGMPv2 (RFC 2236)
- IGMPv3 (RFC 3376 and now RFC 4604)

The **Internet Group Management Protocol (IGMP)** is a [communications protocol](#) used by [hosts](#) and adjacent [routers](#) on [IPv4 networks](#) to establish multicast group memberships. IGMP is an integral part of [IP multicast](#).

The IGMP protocol is implemented on a particular host and within a [router](#). A host requests membership to a group through its local router while a router listens for these requests and periodically sends out subscription queries.

Membership Queries are sent by multicast routers to determine which multicast addresses are of interest to systems attached to its network. Routers periodically send General Queries to refresh the group membership state for all systems on its network. Group-Specific Queries are used for determining the reception state for a particular multicast address. Group-and-Source-Specific Queries allow the router to determine if any systems desire reception of messages sent to a multicast group from a source address specified in a list of unicast addresses.

PTP Unicast mode

- Unicast mode is “one to one” messaging
- Unicast mode was added in PTP v2 specs (was not available in PTPv1)
- PTP Unicast mode planned to be made available with the version 4.8.7 software update (mid-Sept 2012)

Per Michel (8/31/12) Don't forget that when the Master is in Unicast mode, multicast transmissions by the Master are prohibited.

(As of 1/26/11, anyways) The TSynC-PCIe-PTP cards (configured as either master or slave) only support the PTP multicast mode. They do not support unicast mode.

(KW As of 2/9/11, anyways) I spoke to John Fischer about unicast in the TSynCs. The last project meeting has unicast being added to SecureSync in February 2012. It's still planned for TSynC, but we aren't aware of it currently being scheduled to be added. Intentions were to add it sometime after it was added to SecureSync.

(KW 2/10/12) Email from Sylvain to Acquisys: The Unicast implementation on the TSynC PTP board development is actually in progress as for our other products (SecureSync and STA61 units).

The availability is scheduled for Q3-2012 regarding our actual priorities. But if we have a important request of TSYN-PTP boards with unicast, we can modify the plan of course.

PTP “Minicast” mode

- Minicast is similar but not exactly the same as Hybrid mode
- Minicast is a unique modification of Unicast mode.
- Minicast mode consists of:
 - **Multicast:** Sync, Follow-Up and Announce messages
 - **Unicast:** Delay Request and Delay Response messages
 - In Minicast mode, Slaves only unicast contract for Delay Responses.

Partial email from Michel Reyverand (8/31/12)

The minicast is a special case of the unicast mode. In unicast mode, Slaves shall request unicast contracts for the Announce, Sync and Delay_Resp packets. In minicast mode, Slaves only request unicast contracts for the Delay_Resp packets (and so Delay_Req packets). Announce, Sync and Follow-up packets are still sent in multicast mode by the Master.

PTP “Hybrid” Mode

Hybrid mode is a combination of simultaneous Unicast and Multicast modes:
Hybrid mode is not supported in 1204-12, but it's supported on the newer 1204-32 card.

Email from Paul Myers (7/10/12)

Symmetricon in the TimeProvider product line implemented this hybrid mode.

It is a BAD name because hybrid also implies using PTP with SyncE in other documents.
<http://www.symmetricom.com/media/files/support/tsd/product-manual/098-00172-000-RevA.pdf>

Email from Denis to Stewart Smith (7/6/12)

When we introduce Unicast, we are planning to have a mode that is similar to the “Hybrid Mode” you describe. I don’t know the details yet. When I have firm documentation about our implementation, I will forward it on.

Email from Sam Otto (8/30/12) regarding “hybrid mode” in v4.8.7

Per Michel, Mix of transmission modes is out of spec. therefore it's not being changed.
You may receive some calls from the customers asking about the systems falling out of sync when everything was working in Multicast mode. If they are not careful when a slave is added or an existing one is modified to unicast or Minicast (0001774) modes the other slaves will no longer be in sync.

****PTP Domains/PTP multicast addresses**

Refer to sites such as: http://en.wikipedia.org/wiki/Precision_Time_Protocol

According to Denis Reilly, and per [Precision Time Protocol](#), the multicast address for all domains is: **224.0.1.129**

Unlike PTP version 1, which used different multicast addresses for each domain, the multicast address for all domains with version 2 is always **224.0.1.129**

Allows groups of PTP Masters and Slaves to be able to inter-operate on the same network cable.

Email from Denis Reilly -PTP V2 will not change its multicast address based on domains. PTPv1 uses the other addresses only because that's how it implemented multiple domains. When they improved the domain features in PTPV2, they stopped using the other multicast addresses.

Just to make things more confusing, there is a second multicast address you see on V2 packets of certain types. I don't recall the distinction exactly. But the critical thing is that the multicast address for V2 PTP does not vary with domain, where it does with V1.

Definition of “domain”

A domain is an interacting set of clocks that synchronize to one another using PTP. Clocks are assigned to a domain by virtue of the contents of the *Subdomain name* (IEEE 1588-2002) or the *domainNumber* (IEEE 1588-2008) fields in PTP messages they receive or generate. Subdomains allow multiple clock distribution systems to share the same communications medium.

PTP packet timescales

Email from Denis Reilly on 10/4/11)

If an input reference does not provide the TAI offset value (such as IRIG input) the value needs to be manually entered.
Refer to: [Time Scales \(UTC/GPS/TAI\) for all products](#) to determine the current TAI offset.

The Specification defines the PTP timescale as TAI. That must be supported. Properly transferring the TAI – UTC offset to any slave so it can recover UTC time must also be supported.

Other timescales are defined as “alternate timescales” in the specification. The timescale used is supposed to be set by the PTP Master, though, and slaves are supposed to be able to use whatever the Master sets.

Supporting alternate timescales is optional, but some PTP profiles require support for the UTC timescale in particular. I think we are finding that many other products rely on transmitting time in the UTC timescale, regardless of what the spec says, so we should make it work.

The Announce message periodically transmitted from the PTP Master reports its UTC offset to each of the PTP Clients. With this value, each PTP client can calculate and convert the received TAI time to UTC time. This allows the PTP Master to be able to output TAI time (as required to be Class 6 -sync status reported per the 1588 Specs) and allow clients to be able to know UTC time. The PTP Master has to transmit TAI time if it wants to be class 6, which is what allows it to report its sync status.

Sync status of the master/grandmaster is included in the PTP messages

The PTP messages that are sent from the master to the slaves indicated whether or not time and frequency data are valid. If the TSync-PCle or SecureSync aren't synced (externally or manually set), all PTP slaves will still receive time data from the master, but won't actually sync to the master.

Important Note: Even if the master/grandmaster is synced, if the priority value of the slave is higher than the priority of the master, the slaves will ignore the sync message and will not sync to the master. The master's priority value has to be higher than the slave's priority in order for the slave to sync to the master.

Best Master Clock algorithm (BMCA)

- All of the below info for BMC is from https://en.wikipedia.org/wiki/Precision_Time_Protocol
- Refer to the Announce message break-down for the individual fields: [Announce message \(Announce packet\)](#)

- 1) **Identifier:** A universally unique numeric identifier for the clock. This is typically constructed based on a device's MAC address.
- 2) **Quality:** Both versions of IEEE 1588 attempt to quantify clock quality based on expected timing deviation, technology used to implement the clock or location in a stratum schema.
- 3) **Priority:** An administratively assigned precedence hint used by the BMC to help select a *grandmaster* for the PTP domain. IEEE 1588-2002 used a single boolean variable to indicate precedence. IEEE 1588-2008 features two 8-bit priority fields.
Priority1 and Priority2: Two separate values that can be defined in order to provide additional weighting to the selection of Best Master clock (Normally, they are assigned the same value – such as both set to 1- but don't have to be set to the same value).
Note: “1” is the highest priority value and “128” is lowest priority.
- 4) **Variance:** A clock's estimate of its stability based on observation of its performance against the PTP reference.

Performs a distributed selection of the best candidate clock based on the following clock properties (as reported in the **PTP Announce** messages)

IEEE 1588-2008 uses a hierarchical selection algorithm based on the following properties in the order indicated (all are reported in the **Announce** Message):

- 1) **Priority 1 value**
- 2) **Clock Class**
- 3) **Clock accuracy (“grandmasterClockAccuracy” field)**

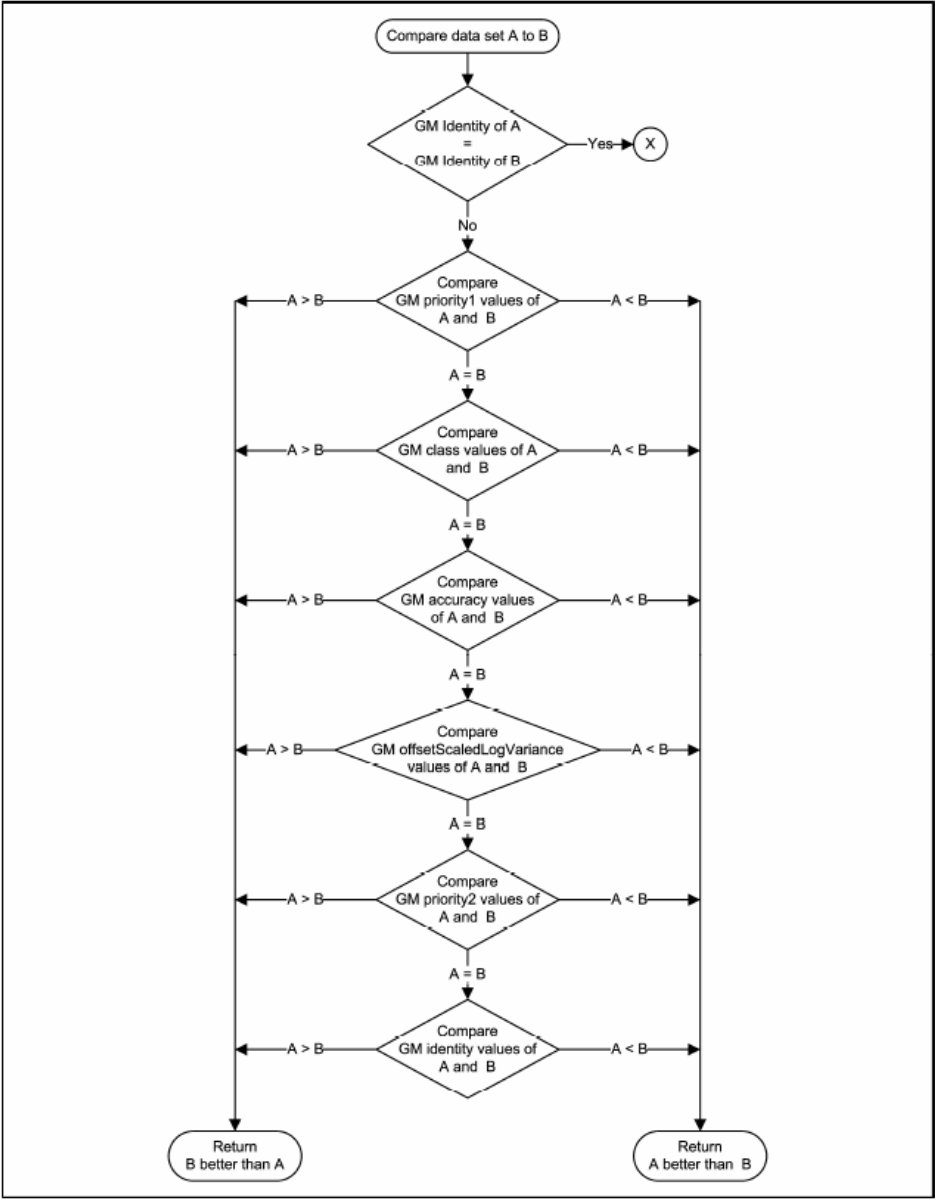
Table 6 —clockAccuracy enumeration

Value (hex)	Specification
00-1F	Reserved
20	The time is accurate to within 25 ns
21	The time is accurate to within 100 ns
22	The time is accurate to within 250 ns
23	The time is accurate to within 1 μs
24	The time is accurate to within 2.5 μs
25	The time is accurate to within 10 μs
26	The time is accurate to within 25 μs
27	The time is accurate to within 100 μs
28	The time is accurate to within 250 μs
29	The time is accurate to within 1 ms
2A	The time is accurate to within 2.5 ms
2B	The time is accurate to within 10 ms
2C	The time is accurate to within 25 ms
2D	The time is accurate to within 100 ms
2E	The time is accurate to within 250 ms
2F	The time is accurate to within 1 s
30	The time is accurate to within 10 s
31	The time is accurate to >10 s
32-7F	Reserved
80-FD	For use by alternate PTP profiles
FE	Unknown
FF	Reserved

- 4) **Variance (listed in SecureSync browser as “Offset Scaled Log Variance”)**
- 5) **Priority 2 value (used as a tie breaker)**
- 6) **Unique identifier (end tie breaker) (this is the MAC address of the PTP Masters)**
 - The ultimate tie-breaker is the **lowest** MAC address (not the highest)
(example from below email: **00:0c:ec:ff:fe:0a:1c:36** is LOWER than **00:0c:ec:0a:1c:39** - so “36” is selected)

Partial email from Denis Reilly (27 Mar 18) ... I would ask them to go find 10.11.22.125, and compare its Priority1 value to the Priority 1 value of 10.11.22.126. If those are the same, then go through the rest of the BMCA list. **If they are all the same, the ultimate tie-breaker is the lowest MAC address. 10.11.22.125 is broadcasting its Clock Identity as 00:0c:ec:ff:fe:0a:1c:36, which is lower than the MAC address of 10.11.22.126, which is 00:0c:ec:0a:1c:39 in the screenshot.**

Here is a flowchart of the master selection process.



Best Master Clock Failover to another PTP master

- If the active master stops sending packets or the BMCA determines the current master is no longer the best master (via Announce messages, another PTP master on the same PTP domain takes over as the active master
- The switchover to another PTP Master isn't "instant", so that if just a couple PTP packers were lost on the network, it wont just switch over to a secondary master.
- There is a timeout value defined that determines how many missed Announce messages will result in switchover.
- Announce message rate has an effect on how long it takes to switch (the slower they are being sent, the longer it can take to switch over to an alternate.
- The PTP masters must be able to communicate with each other over the network, in order for the failover to operate properly

CBOE reported PTPd/SFPTPd toggling back and forth between two Legacy VelaSyncs which are both operating normally

- Refer to Salesforce cases: 19002 and 188884

Issue is the **grandmasterClockAccuracy** field of both SecureSync's in their Announce messages are intermittently toggling between two Legacy VelaSyncs because clock accuracy of each keep toggling between accuracies better than 100ns and accuracies between then 25ns.

Desire to change the Priority value to weigh one PTP Master higher than another

Email from Cort w/FSMLabs Keith, the PTP BMC does weight the MAC address in order to break ties like this. The client should have no trouble staying with one GM in a proper setup.

If they set a priority higher than another in this setup they will cause the higher priority GM to always be used. That may not be what they want when one GM goes into holdover or has poor accuracy (or becomes a boundary clock).

Number of hops / Boundary and Transparent clocks/ delay mechanisms

Network switches between PTP master and PTP Slaves (Transparent clocks)

Email from Denis Reilly

If they are going through a Layer 3 switch (i.e. a switch that does routing), and that switch is not PTP-aware, they may want to check their Time-To-Live (TTL) field as well. This defaults to 1, because that's technically what the Ethernet spec says all Multicast traffic should be set to. But this means no traffic will go through a Layer 3 switch. If all else fails, they can try increasing this to 2 and see what happens

Maximum recommended number of hops between PTP Master and Slave

Email Keith sent to a customer after discussing with Denis (11 Sept 2013) Regarding your question about the maximum recommended number of hops between the PTP Master and PTP slaves, there is no specific answer to this question (other than with Multicast packets, the Time To Live – TTL – value has to be higher than the number of devices that aren't PTP aware). This is more of a general answer of simply "the fewer the hops in between the better" for the most optimized PTP timing capabilities.

Each hop in between the Master and Slave, whether or not it's a PTP-Aware device, is going to add some degradation to the overall accurate timing that PTP Master is trying to provide to the PTP Slave. For each hop in between, this degradation is additive, so the more hops in between, the less optimized the timing will be at the Slave. In fact, this is why we only spec PTP performance with a network cross-over cable between a PTP Master and Slave. Adding switches and routers in between will inherently degrade the overall PTP timing by a varying amount. Depending upon factors such as your operational requirements and Best Master Clock operation, the degradation added for each hop in between may or may not be an issue for your PTP slaves. The better you want the overall timing to be, the more you should try to limit the number of hops in between. The most optimum timing occurs when there are no hops in between.

Boundary Clocks

Boundary clocks are "ordinary" PTP clocks with at least two Ethernet ports for PTP. One is for PTP input and the others are PTP outputs to PTP slaves/

Boundary clocks block all PTP messages from going from one subnet to the next (i.e. PTP sync, follow-up, delay and peer delay messages, general status messages, etc are blocked).

Email from Denis Reilly Boundary Clock: runs separate PTP clocks on each network interface port. These clocks are linked so that if one clock is connected to the Best Master, all the other clocks can obtain their time from it and become "mini-masters" (my term). This breaks up the timing path into separate parts, and the variable delay through the switch is now "in between" the timing paths, and no longer affects timing.

SecureSync acting as a Boundary clock

Email from Dick Fox (12/28/11) Spectracom doesn't market Secure Sync as a boundary clock, but Secure Sync can behave like a boundary clock with multiple PTP modules in a Secure Sync

One of the PTP Modules can act as a slave and obtain its time from an external PTP Masters. The Other PTP modules in the SecureSync can be configured as Masters for their own networks and used the PTP module in the slave mode as the reference for the other PTP modules acting as Masters for their own networks

In this mode. Secure Sync with multiple PTP modules up to 6 can be a boundary clock

A PTP slave acts as the reference for up to 5 other PTP modules acting as Masters on other networks

Email from Denis on 12/29/11

A true boundary clock will look at all available Masters on all ports, and use the best master it can see on any port as the Master for all the other ports. If the current best master fails, the boundary clock will use the next best master, even if it is on a different port.

SecureSync PTP cards each have their own isolated PTP implementation in them. In particular, information on available masters is not shared among ports, and the Best Master Clock algorithm is run in each individual card.

It behaves "like" a boundary clock in that it can take timing information from a GrandMaster on one port and distribute it to other ports. And if the current Grandmaster fails, it will successfully fail over to another master that is visible on the same PTP card as the first grandmaster. But SecureSync may not behave like a proper Boundary Clock in the presence of multiple masters on networks connected to different cards.

Transparent Clocks

Transparent clocks allow PTP packets to get through a switch and add a time stamp to the PTP messages to account for the processing delays to get through the switch.

Email from Denis Reilly

Transparent Clock: timestamps the delay through the switch, and inserts the delay value on-the-fly into the PTP packet. The PTP device takes this delay value into account when calculating its time, effectively accounting for any variable delay through the switch.

Email from Denis Reilly

We do not have a relationship with Cisco. Cisco has very good PTP equipment; we should recommend it to customers who can afford it. From what I have gathered from working with Will and Mark Goodlein on the Financial side of things, Cisco thinks that transparent clocks do not scale do well (there is only one field in the PTP protocol for delay, so once you layer a few clocks it can get messy) so they are pushing Boundary Clocks to their financial customers.

All switches will accept PTP packets, but only switches that are transparent clocks or boundary clocks will perform well. We constantly tell our customers that their PTP accuracy is heavily dependent on their network infrastructure, and that we run very well through a crossover cable. I do not want to speculate on accuracy through any particular switch hardware. (We test through an older Cisco IE-3000 transparent clock.)

****Peer to Peer (P2P)/End to End (E2E) delay mechanisms

Note:

- **E2E (End to End) mode** uses the standard Delay Requests / Delay Responses
- **P2P (Peer to Peer) mode** changes the standard Delay Requests / Delay Responses to Peer Delay Requests/Peer Delay Responses

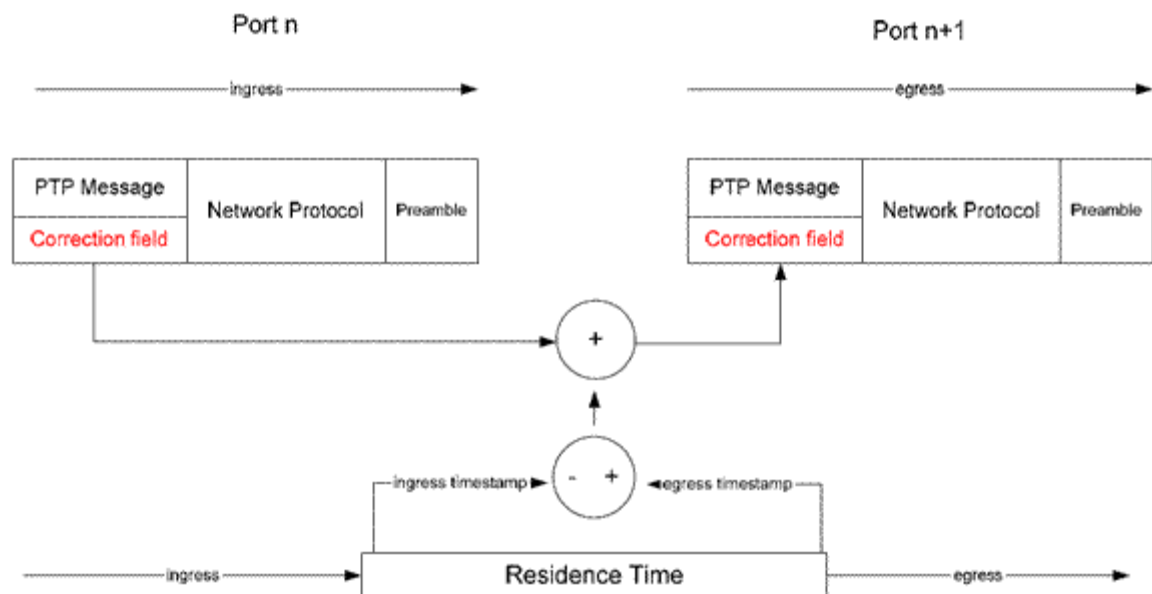
Notes from Denis, about P2P mode:

- Every network device, from the PTP Master to the PTP Slave, has to support P2P mode, to use P2P mode
- Every network device in P2P mode sends peer delay requests and peer delay responses (bi-directional)

Email from Paul Myers (12/16/11)

The Boundary clocks (BC) defined in both versions of the IEEE1588 Standard, respectively Draft Standard evidence two problems when used in (highly) cascaded networks. Namely, there is nonlinear decreasing synchronization accuracy and rising resynchronization time after network reconfiguration. To eliminate these effects, the concept of transparent clocks (TC) has been introduced in the IEEE 1588 standard version 2. Transparent clocks were added in IEEE1588 - 2008 to correct the "residence time" of the network device like an Ethernet Switch. The residence time is accumulated in a field (correction field) of the SYNC (one-step) or Follow-UP (two-step) message. [Figure 2]. Since transparent clocks are stateless they have no impact on the reconfiguration time of e.g. ring topology networks.

Transparent clock residence time calculation



The IEEE1588-2008 standard knows two types of transparent clocks, namely: **End-to-End (E2E)** and **Peer-to-Peer (P2P)**.

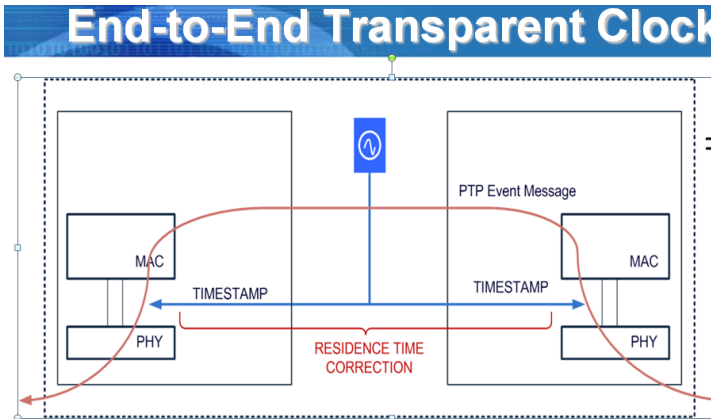
End-to-End TCs only measure the time taken for a PTP event message (those who get time stamped) to transit the bridge and provide this information to the receiving clocks in the correction field. No propagation delay of the link connected to the port is corrected by the E2E TC. E2E TCs use the delay request / delay response mechanism for the delay measurement whereby the residence time of the delay request / delay response messages are corrected in the same way stated above.

Peer-to-Peer TCs use the peer delay mechanism (Figure 3) for the delay measurement. In addition to providing PTP event transit time information the P2P TC also provides corrections for the propagation delay of the link connected to the port receiving the PTP event message (correction field).

End to End = Sync, Delay_Req, Follow_Up and Delay_Resp messages are used by *ordinary* and *boundary* clocks and communicate time-related information used to synchronize clocks across the network.

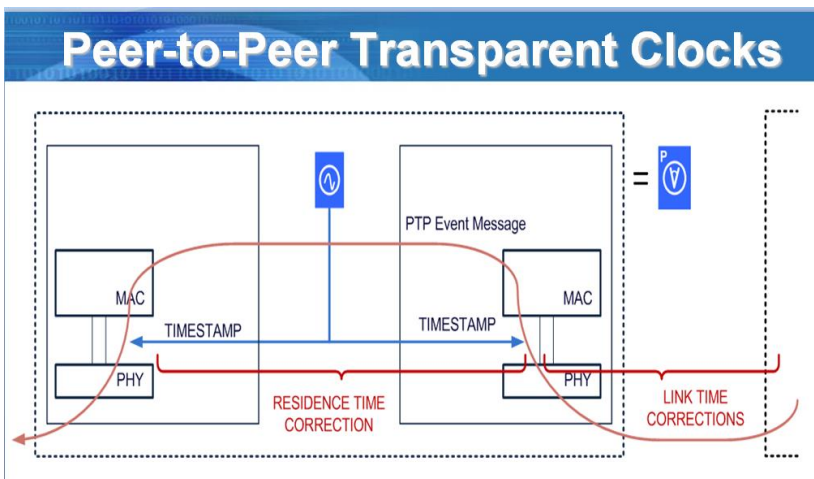
Note: “Delay requests” are packets sent from the PTP slave to the master in order to help calculate the return trip path delay (PTP calculates the total path delay and divides by 2, assuming that both trip back delays were the same).

End to End (E2E) mode— Measures the path delay as a total value between Master and Slave.



Peer to Peer (P2P) mode = Measures the path delays as individual delays between each host (measures network segments individually) and then combines the values for a total. Provides additional accuracies

Note (12/1/11): SecureSync versions 4.6.0 and below didn't have P2P capability. V4.7.0 added the mode, but the drop-down selection to enable this mode was inadvertently not added to the list of modes. It is supported, starting in version 4.8.0.



Parent: The Device that the PTP Slave is syncing to. With End to End, the Parent is either the master or grandmaster. With End to End, the parent can be the master, grandmaster or a boundary clock.

One-Step/Two-step modes:

Two Step mode is used when the PTP hardware is not fast enough to be able to send time data with the original Sync message, so it sends the time of original the sync message in a follow-up message to the clients. When the PTP hardware is fast enough to include time stamps in the sync message, one step allows the original sync message to include time and prevents the follow-up message from needing to be sent out.

With Two step, the PTP master/grandmaster sends a sync packet to the slaves. The Slave receives the sync packet and is flagged. The Master then sends a follow-up message which includes the time that the sync message was sent out (known as T1),

Note: We support both Two step and One step (even though our hardware is fast enough for one step). Some slaves may require Two step to be used, instead of One step.

Q. ...So you're confident that one-step mode will not compromise the accuracy we can achieve across our slaves (vs. two- step mode)? Is there any additional latency information that slaves can detect from the Followup message?

A. Email from Denis Reilly (31 Mar 2014) Recall that happens to generate T1 and T2 for PTP, both in one-step and in two-step:

The Master sends a Sync packet, and as the Sync packet leaves the Master, it is timestamped to generate T1. When the Slave receives the Sync packet, the packet is timestamped to generate T2.

The only difference between one-step mode and two-step mode is in how the T1 timestamp is conveyed to the Slave: In One-Step, the T1 timestamp is inserted directly into the Sync message as it goes out. In Two-Step, the T2 timestamp is saved and sent in the Follow-Up packet.

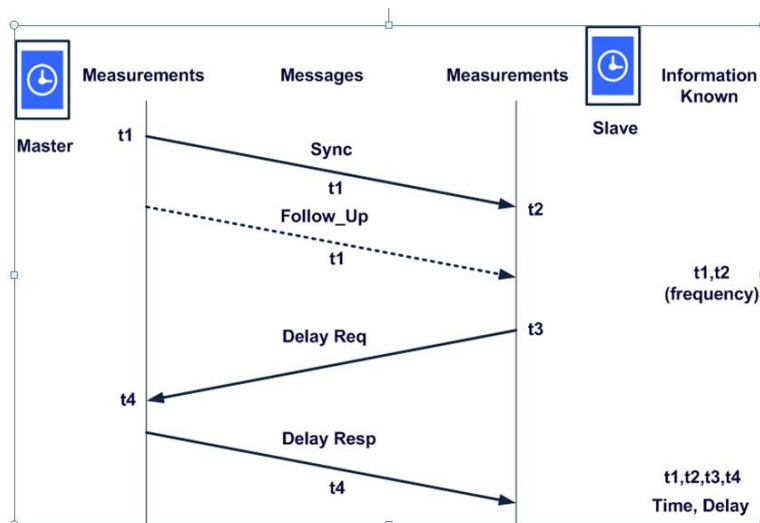
(Timestamp fields in the Sync message in two-step mode are ignored in favor of the Follow-Up Packet's time.

So, in theory, there is no difference between the two modes, other than more network traffic for two-step. For the Slave, the only difference is in knowing which packet to get the time from, and well-written Slaves should be able to handle either mode. (Recall that all the math for synchronization is done at the Slave, so there is no need to convey T2 back to the Master.)

But in practice, one-step mode is harder to implement properly in a Master, because the timestamp of the packets has to get inserted into the packet as it gets sent out, which may cause other changes in the packet (like checksums). There are many implementations that cannot use hardware time in one-step mode, because the hardware that takes the timestamps is not able to modify the packets. This timestamp is sent back to the PTP engine, which creates the follow-up packet (which will not need to be changed in flight). These implementations may change to using software time if one-step is enabled.

What we can assure the customer is that our 1204-32 card does support one-step mode with hardware timestamping properly, making all packet changes in real-time as required. It was designed to be able to support 4000 slaves at high message rates in this manner without flinching.

Note: All masters and grandmasters transmit "**Announce messages**" to the entire network to say "I'm here" so the clients know they exist on the network. However, only the master/grandmaster selected by the Best Master Clock algorithm transmits the **Sync** messages.



Dotted line above indicates two step messaging.

PTP network ports:

- **Refer to:** Port assignments and RFCs (NTP, HTTP, HTTPS, Syslog, etc) for all products
- PTP is UDP traffic (not TCP)

Email from Denis Reilly (11/1/2011)

You can also run PTP on “Layer 2”, which doesn’t use TCP or UDP but instead uses “raw” Ethernet frames. I think this might be what the customer wants. We support this on SecureSync. I don’t know off the top of my head whether we support it in TSync, I will have to check (see next paragraph).

Follow-up to the above statement regarding TSync-PCle (based on email from Denis Reilly ~11/4/11

“UDP/Layer 3 packets are supported. However, using raw Layer 2 packets is not currently supported in the TSync-PCle-PTP board”.

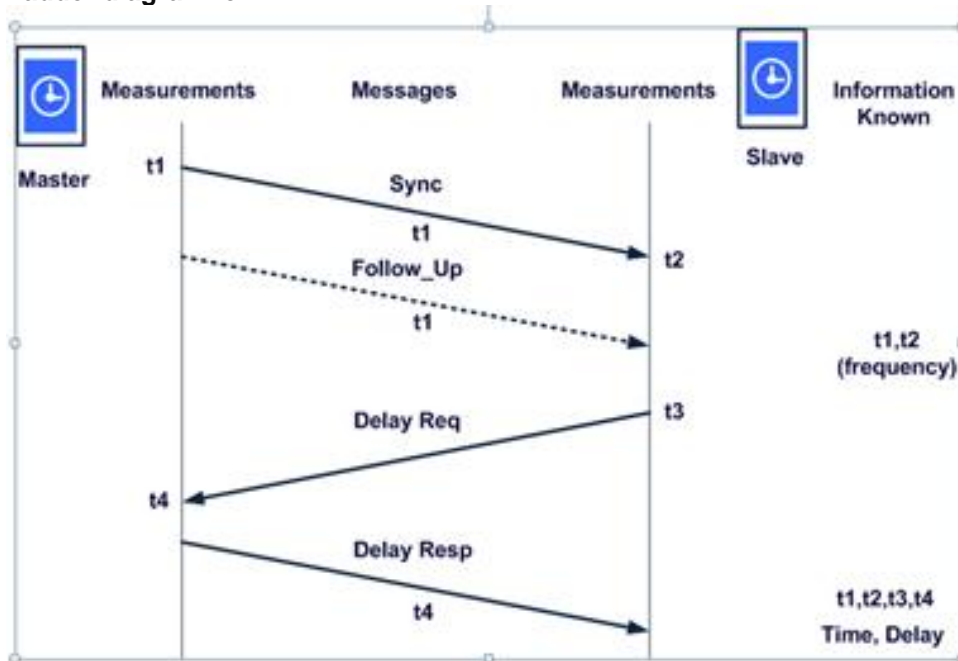
Types of PTP messages

- Refer to Section 13 of the IEEE1588-2008V2 specs for additional info: [I:\Engineering\Specs and Standards\IEEE \(Institute of Electrical and Electronics Engineers\)](I:\Engineering\Specs and Standards\IEEE (Institute of Electrical and Electronics Engineers))

(MessageType / "messageID" field)

Signaling	(0x0C)
Announce	(0x0B)
Sync	(0x00)
Follow-up	(0x08)
Delay Request	(0x01)
Delay Response	(0x09)
Peer Delay Request	(0x02)
Peer Delay Response	(0x03)
Peer Delay Response Follow up	(0x0A)
Management	(0x0D)

Ladder diagram for PTP



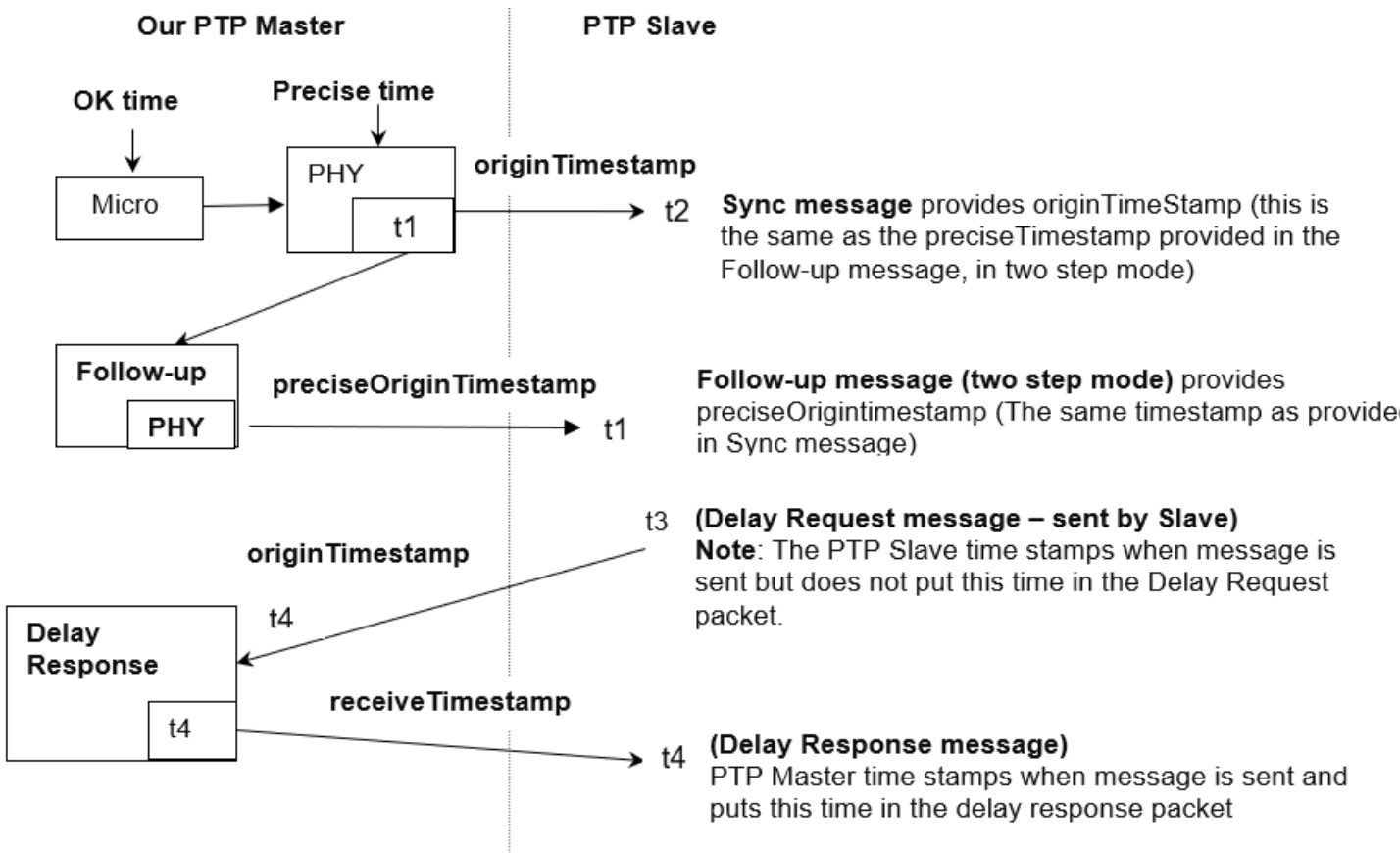
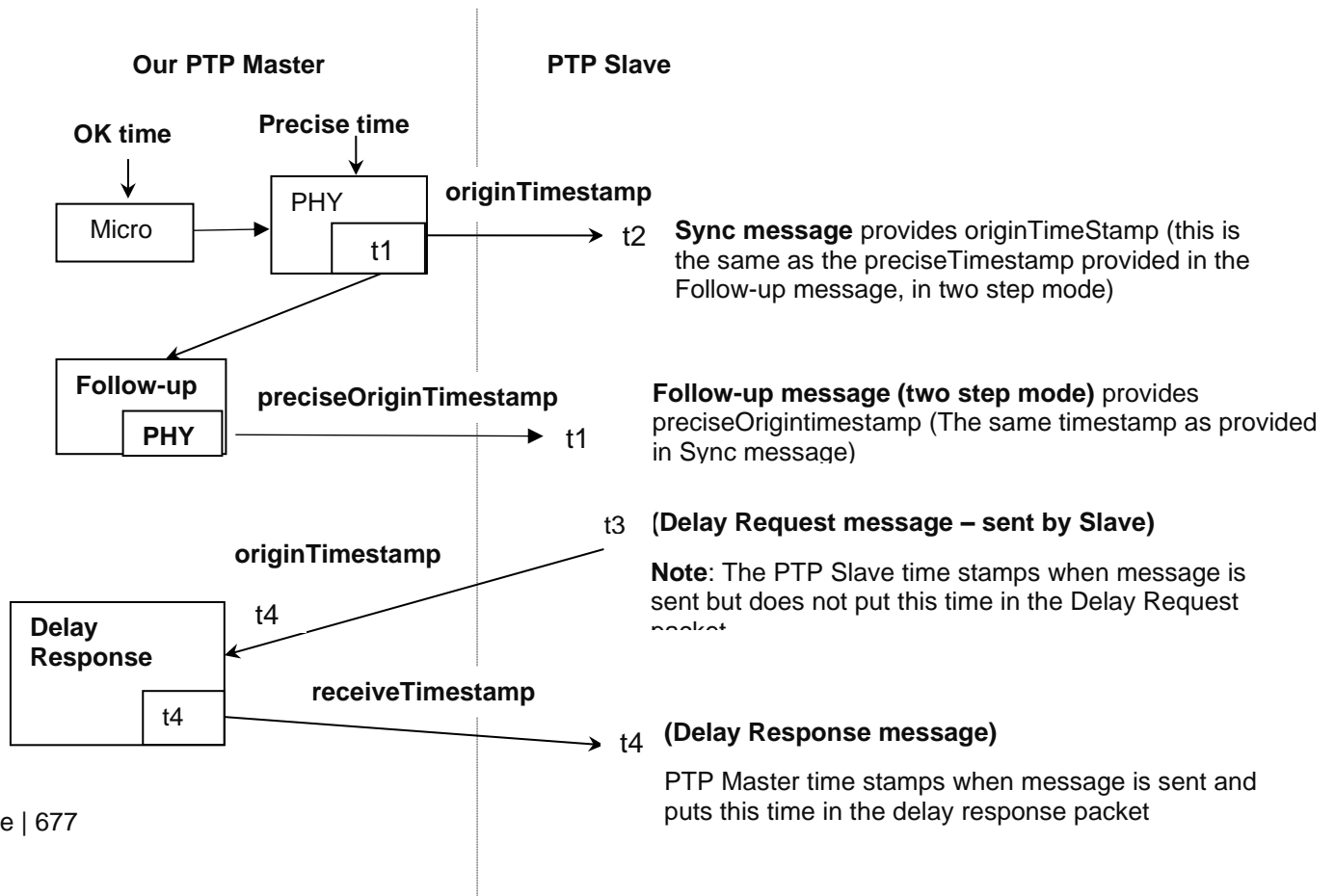


Diagram below for editing



TLVs and Signaling Messages (labeled “Signalling” in wireshark)

- Signaling messages are only sent while in Unicast, Minicast or Hybrid modes (not sent in Multicast only mode)
- They are used to transport a sequence or one or more TLV variables (it's a way of just sending data over the network).
- Are sent to request unicast contracts
- Signaling messages are sent on Port 320

Note: TLV stands for Type/Length/Value variables

Ethernet Header:

- SecureSyncs with a **1204-32** card will report **Spectrac_** “ ” with a MAC address of **00:0C:**
- SecureSync's with a **1204-12** card will report “**Spectrac_**” with a MAC address of “**00:0v**”.
- I believe all Legacy VelaSyncs/Timekeeper master will report “**IntelCor_**”)
- Other masters will report different info.

There are four (4) different types of Signaling messages for Unicast/Minicast/hybrid transmissions (several others exist). These are Unicast negotiation messages (back and forth between Unicast/Minicast/hybrid Master and Unicast/Minicast/hybrid Slaves).

1. Request Unicast Transmission
2. Grant Unicast Transmission
3. Cancel Unicast Transmission
4. Acknowledge cancel unicast transmission

Refer to http://www.shoshin.co.jp/c/endrun/1588ptp/IEEE1588v1_vs_IEEE1588v2.pdf and <https://oroliagroup-portal1.sharepoint.com/Spectracom/Engineering/Projects/GeneralPTP/Shared%20Documents/Standards/IEEE1588-2008V2.pdf>

TLVs are separately (exchanged between PTP master and each PTP client) for each type of PTP packet (such as Sync and delay responses) being exchanged via unicast mode. The flags in the “Grant unicast transmission” tlvs indicate which type PTP packet the TLV is for:

A) The Announce message from Master indicates whether unicast PTP packets are allowed/supported

```
> Frame 24: 110 bytes on wire (880 bits), 110 bytes captured (880)
> Ethernet II, Src: Heineberg_8a:9b:a5 (ec:46:70:8a:9b:a5), Dst: M
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 506
> Internet Protocol Version 4, Src: 10.101.254.54, Dst: 10.101.254
> User Datagram Protocol, Src Port: 320, Dst Port: 320
> Precision Time Protocol (IEEE1588)
  > 0000 ... = transportSpecific: 0x0
  .... 1011 = messageId: Announce Message (0x0)
  0000 ... = Reserved: 0
  .... 0010 = versionPTP: 2
  messageLength: 64
  subdomainNumber: 44
  Reserved: 0
  > Flags: 0x03c
    0... .. = PTP_SECURITY: False
    .0.. .. = PTP_profile Specific 2: False
    ..0. .. = PTP_profile Specific 1: False
    ....1... = PTP_UNICAST: True
    ....0... = PTP_TWO_STEP: False
    ....0... = PTP_ALTERNATE_MASTER: False
    ....1... = FREQUENCY_TRACEABLE: True
    ....1... = TIME_TRACEABLE: True
    ....1... = PTP_TIMESCALE: True
    ....1... = PTP_UTC_REASONABLE: True
    ....0... = PTP_LI_50: False
    ....0... = PTP_LI_61: False
```

PTP Unicast: True = All packets (Announce, Sync, Delay Requests and Delay Responses) are to be sent in Unicast mode. No multicast PTP messages.

B) PTP Slaves send TLVs are sent from Slave to request unicast for each type of PTP packet (Announce, Sync and Delay responses)

1. Example TLV requesting unicast Announce messages


```

    ✓ tlvType: Request unicast transmission (4)
      lengthField: 6
      1011 .... = messageType: Announce Message (0xb)
    ✓ logInterMessagePeriod: 1
      period: every 2 seconds
      rate: 0.5 packets/sec
      durationField: 60 seconds

```

2. Example TLV requesting unicast Sync messages

```

targetPortId: 05555
    ✓ tlvType: Request unicast transmission (4)
      lengthField: 6
      0000 .... = messageType: Sync Message (0x0)
    > logInterMessagePeriod: 0
      durationField: 60 seconds

```

3. Example TLV requesting unicast delay response messages

```

targetPortId: 05555
    ✓ tlvType: Request unicast transmission (4)
      lengthField: 6
      1001 .... = messageType: Delay_Resp Message (0x9)
    ✓ logInterMessagePeriod: 0
      period: every 1 seconds
      rate: 1 packets/sec
      durationField: 60 seconds

```

A single TLV Signalling message used to request unicast for more than one packet type (both PTP Master and PTP Client must support combined TLVs)

- Per Dave Sohn (8 Nov 2022) ptp4l (as used in 2400 SecureSyncs starting in 1.4.1) can send a single TLV message which requests unicast for more than just one type packet
- Example capture below shows a 2400 SecureSync slave sending a single TLV signalling message to its PTP master, requesting both **unicast Syncs** and **unicast Delay Responses** via the same packet.

```

Nov 8, 2022 13:46:52.265500000, 2022-11-08 10:46:52.265500 00 10.15.100.15 10.15.100.13 64 PTPv2 Signalling Message
<
> Frame 88: 186 bytes on wire (840 bits), 186 bytes captured (840 bits)
> Ethernet II, Src: Spectrac_0e:01:20 (00:0c:cc:0e:01:20), Dst: Spectrac_0e:00:f6 (00:0c:cc:0e:00:f6)
> Internet Protocol Version 4, Src: 10.15.100.15, Dst: 10.15.100.13
> User Datagram Protocol, Src Port: 320, Dst Port: 320
> Precision Time Protocol (IEEE1588)
  > 0000 .... = transportSpecific: 0x0
  .... 1100 = messageId: Signalling Message (0xc)
  0000 .... = Reserved: 0
  .... 0010 = versionPTP: 2
  messageLength: 64
  subdomainNumber: 0
  Reserved: 0
  > Flags: 0x0400
  > correction: 0.000000 nanoseconds
  Reserved: 0
  > ClockIdentity: 0x000ccfffeb0120
  SourcePortId: 1
  sequenceId: 1
  control: Other Message (5)
  logMessagePeriod: 127
  targetPortIdentity: 0x000ccfffeb00f6
  targetPortId: 1
  ✓ tlvType: Request unicast transmission (4)
    lengthField: 6
    0000 .... = messageType: Sync Message (0x0)
    > logInterMessagePeriod: 0
      durationField: 600 seconds
  ✓ tlvType: Request unicast transmission (4)
    lengthField: 6
    1001 .... = messageType: Delay_Resp Message (0x9)
    > logInterMessagePeriod: 0
      durationField: 600 seconds

```

C) PTP master then sends TLVs to grant unicast for each type of PTP packet

1. Example TLV granting unicast Announce messages

```

    ✓ tlvType: Grant unicast transmission (5)
      lengthField: 8
      1011 .... = messageType: Announce Message (0xb)
    ✓ logInterMessagePeriod: 1
      period: every 2 seconds
      rate: 0.5 packets/sec
      durationField: 60 seconds
      .... ..1 = renewalInvited: True

```

2. Example TLV granting Sync messages


```

  tlvType: Grant unicast transmission (5)
    lengthField: 8
    0000 .... = messageType: Sync Message (0x0)
  > logInterMessagePeriod: 0
    durationField: 60 seconds
    .... ...1 = renewalInvited: True

```

2. Example TLV granting unicast delay response messages

```

  tlvType: Grant unicast transmission (5)
    lengthField: 8
    1001 .... = messageType: Delay_Resp Message (0x9)
  > logInterMessagePeriod: 0
    period: every 1 seconds
    rate: 1 packets/sec
    durationField: 60 seconds
    .... ...1 = renewalInvited: True

```


Example Signaling message

Filter: ptp

No.	Time	Source	Destination	Protocol	Info
79	48.415232000	192.168.100.49	192.168.99.10	PTPv2	Signalling Message

Frame 126: 96 bytes on wire (768 bits), 96 bytes captured (768 bits)

Ethernet II, Src: Corrigen_7e:d2:08 (00:08:db:7e:d2:08), Dst: Spectrac_08:07:fd (00:0c:ec:08:07:fd)

Internet Protocol, Src: 192.168.100.49 (192.168.100.49), Dst: 192.168.99.10 (192.168.99.10)

User Datagram Protocol, Src Port: ptp-general (320), Dst Port: ptp-general (320)

Source port: ptp-general (320)
Destination port: ptp-general (320)
Length: 62

Checksum: 0x2c72 [correct]
[Good Checksum: True]
[Bad Checksum: False]

Precision Time Protocol (IEEE1588)

0000 = transportSpecific: 0x00

... 1100 = messageId: Signalling Message (0x0c)

... 0010 = versionPTP: 2

messageLength: 54
subdomainNumber: 5

Flags: 0x0600

0... .. = PTP_SECURITY: False
0... .. = PTP profile Specific 2: False
..0... .. = PTP profile Specific 1: False
... 1... .. = PTP_UNICAST: True
... 1... .. = PTP_TWO_STEP: True
... ..0... .. = PTP_ALTERNATE_MASTER: False
... ..0... .. = FREQUENCY_TRACEABLE: False
... ..0... .. = TIME_TRACEABLE: False
... ..0... .. = PTP_TIMESCALE: False
... ..0... .. = PTP_UTC_REASONABLE: False
... ..0... .. = PTP_LI_59: False
... ..0... .. = PTP_LI_61: False

correction: 0.000000 nanoseconds
correction: Ns: 0 nanoseconds
SubNs: 0.000000 nanoseconds
ClockIdentity: 0x0008dbfffe7ed255
SourcePortID: 1
sequenceId: 68
control: Other Message (5)
logMessagePeriod: 127

targetPortIdentity: 0xffffffffffffffff
targetPortId: 65535
tlvType: Request unicast transmission (4)
lengthField: 6

See additional info below

“TLVType” field

- “Request unicast transmission (4)” specifies a specific function.
- Refer to the “tlvType” table further below for specific function.

The value of messageType shall indicate the message type for the unicast message transmission requested. The coding of the enumeration is identical to that used in the messageType field of message headers.



Table 34—tlvType values

tlvType values	Value (hex)	Defined in clause
Reserved	0000	—
Standard TLVs		
MANAGEMENT	0001	15.5.3
MANAGEMENT_ERROR_STATUS	0002	15.5.4
ORGANIZATION_EXTENSION	0003	14.3
Optional unicast message negotiation TLVs		16.1
REQUEST_UNICAST_TRANSMISSION	0004	—
GRANT_UNICAST_TRANSMISSION	0005	—
CANCEL_UNICAST_TRANSMISSION	0006	—
ACKNOWLEDGE_CANCEL_UNICAST_TRANSMISSION	0007	—
Optional path trace mechanism TLV		16.2
PATH_TRACE	0008	—
Optional alternate timescale TLV		16.3
ALTERNATE_TIME_OFFSET_INDICATOR	0009	—
Reserved for standard TLVs	000A – 1FFF	—
Experimental TLVs		14.2
Security TLVs		Annex K
AUTHENTICATION	2000	—
AUTHENTICATION_CHALLENGE	2001	—
SECURITY_ASSOCIATION_UPDATE	2002	—
Cumulative frequency scale factor offset		Annex L
CUM_FREQ_SCALE_FACTOR_OFFSET	2003	—
Reserved for Experimental TLVs	2004 – 3FFF	—
Reserved	4000 – FFFF	—

Experimental TLV values shall be reserved for assignment by the Precise Networked Clock Working Group of the IM/ST Committee; see 14.2.

14.1.2 lengthField (UInteger16)

The value of lengthField is the length of the value field of the TLV in octets; see 5.3.8.

14.1.3 valueField (tlvType specific)

The format and meaning of the valueField member of the TLV is defined in subsequent clauses for each tlvType defined in this standard.

Requests for unicast messages other than Announce, Sync, Delay_Resp, or Pdelay_Resp messages shall always be denied. If unicast transmission is granted for Sync or Pdelay_Resp messages by a two-step clock, then unicast transmission shall also be used for the corresponding Follow_Up and Pdelay_Resp_Follow_Up messages.

“lengthField” (under tlvType)

- “The value of lengthField is the length of the value field of the TLV in octets”
- For Unicast, “6” indicates one TLV. A larger number than “6” indicates multiple TLVs. “The value of the lengthField is 6+N, where N is an even number”

“logInterMessagePeriod” (under tlvType)

- Indicates scheduled periodicity for the message (such as one message every two seconds)

Decoding TLV payloads in the signaling message

```

-
  tlvType: Request unicast transmission (4)
    lengthField: 6
    1011 .... = messageType: Announce Message (0x0b)
  logInterMessagePeriod: 1
    period: every 2 seconds
    rate: 0.5 packets/sec
    durationField: 300 seconds

```

- Wireshark can decode TLV type, but won't decode the payload

Note: both documents referenced in the email below are in: <I:\customer service\PTP\TLVS and signalling messages>

Slightly modified email from Denis Reilly (26 Aug 16)

To begin, TLV's are attached to Signaling messages. The particular type of TLV we are interested in is REQUEST_UNICAST_TRANSMISSION, which is documented in section 16.1.4.1 of IEEE 1588-2008 (attached for your reference and titled "ptpv3 Unicast Req TLV").

Wireshark may decode the TLV type, but will not decode the payload. The payload is 6 bytes, as described below:

The upper 4 bits of the first byte is the Message Type. When a PTP Slave sends this TLV, it is asking for one of three types (as defined in Section 13.3.2.2 of the attached "ptpv2 message types" document):

- **Sync** = Type 0x0
- Delay Response = 0x9
- Announce = 0xB

Some implementations may put more than one TLV in a Signaling message -- for instance, they may request all 3 message types in one signaling message. If this happens, Wireshark will typically only decode the first TLV type, and the others will appear as padding in the packet, so you'll have to decode those by hand.

First, find the signaling message in the packet capture, and click on the "**data**" field.

The "B0" (really just the "B") means it is asking for an announce message. The "01" means it is asking for 1 every 2 seconds (2^1). Then "00 00 01 2c" is the period ($0x12c = 300$)

Announce message (Announce packet)

For a description of the packet, refer to: <http://www.ieee802.org/1/files/public/docs2007/as-garner-protocol-state-machines-frame-formats-0307.pdf>

- Refer to Section 13 of the IEEE1588-2008V2 specs for additional info: [I:\Engineering\Specs and Standards\IEEE \(Institute of Electrical and Electronics Engineers\)](#)
- Sent on Port 320
- Multicast packet periodically sent by selected PTP Master to all PTP clients, so they know who the master is.

Note: The Announce message is usually only sent by the selected best master clock (BMC) on the network. However, all Timekeeper PTP Masters (Such as Legacy VelaSync) send out Announce messages whether or not it's the selected best master.

Contains info such as:

1. Priority values
2. TAI/UTC offset (to allow Slaves to be able to convert the received TAI timescale to UTC timescale)
3. Clock Class (table further below)
4. Clock Quality/ClockVariance/Clock Accuracy (time accuracy) (table further below)
5. timesource (such as **GPS** – or **PTP** when it's a Timekeeper PTP Master)

ptpd.pcap [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Frame	Info
6	2012-02-13 17:55:06.743656	192.168.45.81	224.0.1.129	PTPv2	106	Yes	Announce Message

Frame 6: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)

Ethernet II, Src: Spectracom_08:03:15 (00:0c:ec:08:03:15), Dst: IPv4multicast_00:01:81 (01:00:5e:00:01:81)

Internet Protocol Version 4, Src: 192.168.45.81 (192.168.45.81), Dst: 224.0.1.129 (224.0.1.129)

User Datagram Protocol, Src Port: ptp-general (320), Dst Port: ptp-general (320)

Precision Time Protocol (IEEE1588)

- 0000 = transportSpecific: 0x00
 - 0 = V1 Compatibility: False
 - 1011 = messageId: Announce Message (0x0b)
 - 0010 = versionPTP: 2
 - messageLength: 64
 - subdomainNumber: 0
- flags: 0x003c
 - 0... .. = PTP_SECURITY: False
 - ..0... .. = PTP profile Specific 2: False
 - ...0... .. = PTP profile Specific 1: False
 - 0... .. = PTP_UNICAST: False
 -0... .. = PTP_Two_STEP: False
 -0... .. = PTP_ALTERNATE_MASTER: False
 -1... .. = FREQUENCY_TRACEABLE: True
 -1... .. = TIME_TRACEABLE: True
 -1... .. = PTP_TIMESCALE: True
 -1... .. = PTP_UTC_REASONABLE: True
 -0... .. = PTP_LI_59: False
 -0... .. = PTP_LI_61: False
- correction: 0.000000 nanoseconds
 - correction: Ns: 0 nanoseconds
 - SubNs: 0.000000 nanoseconds
- clockIdentity: 0x000cecfffe080315
- sourcePortID: 1
- sequenceId: 48644
- control: other Message (5)
- logMessagePeriod: 1
- originTimestamp (Seconds): 1329155740
- originTimestamp (nanoseconds): 765322931
- originCurrentUTCoffset: 34
- priority1: 5
- grandmasterClockClass: 6
- grandmasterClockAccuracy: The time is accurate to within 100 ns (0x21)
- grandmasterClockVariance: 22752
- priority2: 128
- grandmasterClockIdentity: 0x000cecfffe080315
- localStepsRemoved: 0
- timeSource: GPS (0x20)

Note: Spectracom SecureSyncs will report "Spectrac" with a MAC address of 00:0v. Other masters will report different info.

Note: "grandmasterClockClass" is set to 6 when Master is in sync (used in BMC)

"GrandmasterClockAccuracy" can be reported as with either 25ns or 100ns (used in BMC)

Note: We set "TimeSource" to "GPS". VelaSync sets it to "PTP"

Applicable Headers/fields for Announce messages (in yellow area above)

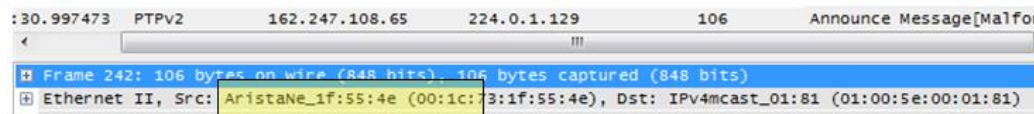
Table 25—Announce message fields

Bits								Octets	Offset
7	6	5	4	3	2	1	0		
header (see 13.3)								34	0
originTimestamp								10	34
currentUtcOffset								2	44
reserved								1	46
grandmasterPriority1								1	47
grandmasterClockQuality								4	48
grandmasterPriority2								1	52
grandmasterIdentity								8	53
stepsRemoved								2	61
timeSource								1	63

Ethernet Header:

- SecureSyncs with a **1204-32** card will report **Spectrac_** “ ” with a MAC address of **00:0C:**
- SecureSync's with a **1204-12** card will report **Spectrac_** with a MAC address of **00:0v**”.
- I believe all **Legacy VelaSyncs/Timekeeper** masters will report **IntelCor_**)
- Other masters will report different info.

For example, if these values aren't indicating the Announce was sent from a SecureSync, the Announce message may be being sent from either a Boundary Clock or a PTP master from another competitor. Below is an example of an announce message being sent from an Arista Network switch (likely acting as a Boundary clock):



Announce message field specifications

Precision Time Protocol header

- The proper **messagelength** field in the PTP header for an Announce message is **“64”** ???

logMessagePeriod:

- In the Announce message, this field indicates the Announce message interval (in seconds) as configured in the PTP Master (such as 1 per second, for example)
- FOR ALL OTHER MESSAGES (including Unicast Sync, Follow-Up, Unicast Delay Response) this field is ignored and should be set to 0x7F / 128

originTimestamp (Timestamp)

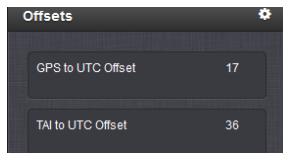
- The value of originTimestamp shall be 0 or an estimate no worse than ± 1 second of the local time of the originating clock when the Announce message was transmitted.

originCurrentUTCOffset

- The value of currentUtcOffset shall be the value of the timePropertiesDS.currentUtcOffset member of the data set.

Notes:

- 1) This value allows PTP slaves to be able to calculate UTC time from the TAI time it's receiving from the PTP Master.
- 2) With the exception of Legacy VelaSyncs/timekeeper (see note below) this value will normally be a value such as "36" (it should be the current "TAI to UTC offset" value. In SecureSync, this current value is reported on the left side of the Management-> Time Management page of the browser, as shown below):



- 3) Legacy VelaSync/Timekeeper PTP Masters send out UTC time by keeping the originCurrentUTCOffset value set to "0", instead.

Priority1

- The value of grandmasterPriority1 shall be the value of the parentDS.grandmasterPriority1 member of the data set.

Note: this field is usually set to 1 on a PTP Master

grandmasterClockClass (ClockQuality)

- The value of **grandmasterClockQuality** shall be the value of the parentDS.grandmasterClockQuality member of the data set.

Note: Normally set to **ClockClass 6** when the PTP Master is in sync.

Table 5—clockClass specifications

clockClass (decimal)	Specification
0	Reserved to enable compatibility with future versions.
1–5	Reserved.
6	Shall designate a clock that is synchronized to a primary reference time source. The timescale distributed shall be PTP. A clockClass 6 clock shall not be a slave to another clock in the domain.
7	Shall designate a clock that has previously been designated as clockClass 6 but that has lost the ability to synchronize to a primary reference time source and is in holdover mode and within holdover specifications. The timescale distributed shall be PTP. A clockClass 7 clock shall not be a slave to another clock in the domain.
8	Reserved.
9–10	Reserved to enable compatibility with future versions.
11–12	Reserved.
13	Shall designate a clock that is synchronized to an application-specific source of time. The timescale distributed shall be ARB. A clockClass 13 clock shall not be a slave to another clock in the domain.
14	Shall designate a clock that has previously been designated as clockClass 13 but that has lost the ability to synchronize to an application-specific source of time and is in holdover mode and within holdover specifications. The timescale distributed shall be ARB. A clockClass 14 clock shall not be a slave to another clock in the domain.
15–51	Reserved.
52	Degradation alternative A for a clock of clockClass 7 that is not within holdover specification. A clock of clockClass 52 shall not be a slave to another clock in the domain.
53–57	Reserved.
58	Degradation alternative A for a clock of clockClass 14 that is not within holdover specification. A clock of clockClass 58 shall not be a slave to another clock in the domain.
59–67	Reserved.
68–122	For use by alternate PTP profiles.
123–127	Reserved.
128–132	Reserved.
133–170	For use by alternate PTP profiles.
171–186	Reserved.
187	Degradation alternative B for a clock of clockClass 7 that is not within holdover specification. A clock of clockClass 187 may be a slave to another clock in the domain.
188–192	Reserved.
193	Degradation alternative B for a clock of clockClass 14 that is not within holdover specification. A clock of clockClass 193 may be a slave to another clock in the domain.
194–215	Reserved.
216–232	For use by alternate PTP profiles.
233–247	Reserved.
248	Default. This clockClass shall be used if none of the other clockClass definitions apply.
249–250	Reserved.
251	Reserved for version 1 compatibility; see Clause 18.
252–254	Reserved.
255	Shall be the clockClass of a slave-only clock; see 9.2.2.

If the inherent characteristics of a clock change such that the clockClass or clockAccuracy designations no longer apply, the clock shall either:

- Upgrade or degrade its clockClass and clockAccuracy in such a way as to correctly specify the current clock characteristics
- Be placed in the FAULTY state

Summary

- **ClockClass = 6:** PTP Master is either synced to an external reference or is “synced to itself”.
- **ClockClass = 7:** PTP Master is in Holdover mode (it was previously synced to an external reference, since last power-up, but has since lost all input references. Holdover mode has not yet timed-out)
- **ClockClass = 52:** in at least versions 1.6.0 and below of the 2400 SecureSyncs, I am seeing ClockClass 52 being reported, when a SecureSync is not in sync and not in Holdover. I am also seeing it reported when a

SecureSync is synced as a stratum 2 server, syncing via NTP input (wasn't sure if this is correct, so I created CAR-2100, Nov 2022 to inquire about it with Engineering. I believe NTP input should be considered a Primary Reference, making it ClockClass 6, but not positive about this).

- **ClockClass = 248:** PTP master may have “Battery Backed Time” enabled to allow Master to sync to itself at startup. Technically, this should be OK for sync, but no guarantees all PTP slaves will accept it for sync??
 - Observed on two v1.5.0 VersaSyncs having Battery Backed Time enabled (synced to RTC at boot)
 - Should switch to ClockClass 6 after selecting a higher priority reference (such as GNSS or IRIG). But testing of v1.5.0 VersaSync doesn't appear to show this happening. Seems like they are remaining at 248 even after switching to GPS. Engineering investigating this.
 - ClockClass 248 (Master synced to itself) is likely to result in (as shown in the PCAP below):
 - ✓ “GrandmasterClockAccuracy” being reported as “Accuracy Unknown”
 - ✓ “TimeSource” being reported as “Internal_oscillator”

```

Nov 15, 2022 09:51:19.09... 2022-11-15 14:51:19... 27 192.168.2.21 224.0.0.1:224 64 PTPv2 Announce Message 248
... 0010 = versionPTP: 2
messageLength: 64
domainNumber: 0
minorSdoId: 0
flags: 0x0008
  0... .. = PTP_SECURITY: False
  .0.. .. = PTP profile Specific 2: False
  ..0. .. = PTP profile Specific 1: False
  ....0.. = PTP_UNICAST: False
  ....0.. = PTP_TWO_STEP: False
  ....0.. = PTP_ALTERNATE_MASTER: False
  ....0.. = SYNCHRONIZATION_UNCERTAIN: False
  ....0.. = FREQUENCY_TRACEABLE: False
  ....0.. = TIME_TRACEABLE: False
  ....1... = PTP_TIMESCALE: True
  ....0.. = PTP_UTC_REASONABLE: False
  ....0.. = PTP_II_59: False
  ....0.. = PTP_II_61: False
> correctionField: 0.000000 nanoseconds
messageTypeSpecific: 0
> ClockIdentity: 0x000cecffe0c0370
SourcePortID: 1
sequenceId: 52833
controlField: Other Message (5)
logMessagePeriod: 1 (2.000000 s)
originTimestamp (seconds): 0
originTimestamp (nanoseconds): 0
originCurrentUTCOffset: 37
priority1: 128
grandmasterClockClass: 248
grandmasterClockAccuracy: Accuracy Unknown (0xfe)
grandmasterClockVariance: 65535
priority2: 128
grandmasterClockIdentity: 0x000cecffe0c0370
localStepsRemoved: 0
TimeSource: INTERNAL_OSCILLATOR (0xa0)
  
```

ARBITRARY (ARB) Clock Classes

- ARB Clock Classes doesn't appear to be available in ptp4l (such as used in 2400 SecureSyncs at versions 1.4.x and above).

Q. what is the difference between the PTP Clock Classes vs ARB clock classes?

A. Per Denis Reilly There is a separate set of clock classes defined in Table 5 of IEEE 1588-2008 for clocks in an "arbitrary" timescale. Instead of using 6/7/52, clocks in the ARB timescale use 13/14/58. So it's just a different clock class mapping that some customers use instead of the more typical mapping for the PTP timescale.

**"GrandmasterClockVariance" (AKA "OffsetScaledLog Variance"-OSLV)

- OSLV (OffsetScaledLog Variance) is a reported estimated variance, as part of the BMCA (Best Master Clock Algorithm)
- Reported in **Announce** messages and in the **Advanced** tab of the 1204-32 browser

Also called/referred to as:

- "GrandmasterClockVariance" in pcap captures
- "Offset Scaled Variance" in 1204-32 web browser and
- "OffsetScaledLogVariance (OSLV)" in PTP Specs

Reported OSLV values with our products

- **SecureSync's 1204-32 card:** Per Denis R "the OSLV value in the 1204-32 card is based on the type of oscillator that is installed in the SecureSync. An OCXO unit will have a different value than a Rb oscillator"

Email from Denis Reilly to Dave Lorah regarding Salesforce Case 202779 (15 Jul 2019) The OSLV value in the 1204-32 card is based on the type of oscillator that is installed in the SecureSync. An OCXO unit will have a different value than a Rb.

The OSLV value is a special calculation in Clause 7.6.3 of 1588-2008 that is based on a scaled computation that is similar to Allan Deviation. It is used in the Best Master Clock algorithm because they felt that if all other things in the BMCA were equal, you would want to listen to the clock that was most stable. The math is a bit tricky but generally speaking, lower values are more stable. We can do this math on SecureSync because we are using the SecureSync's oscillator to directly drive the timestamps.

In practice, very few people pay attention to this because in order for it to matter, the priority1, clock class, and clock accuracy values of two masters have to be the same – this is the 4th tiebreaker in the BMCA.

I think that '0' in the Velasync is a bug. I don't think we calculate the variance in Velasync at all, and if we do not calculate it we are supposed to transmit "0xFFFF" for the OSLV, meaning that if the BMCA gets this far a unit that broadcasts 0xFFFF will always "lose". I think calculating this for Velasync will be tricky because our TSync oscillator does not directly drive the timestamps, so we are better off not calculating it.

I've added [SWI-679](#) to change this behavior so we broadcast 0xFFFF, but I don't view it as a high priority to fix.

- **Legacy 1225 VelaSync (Timekeeper):** Always reported as "0"
- **1232 VelaSyncs**
- **Base 2400 SecureSync:** 22752 ?

“GrandmasterClockAccuracy” (Clock Quality/Clock Accuracy/time accuracy)

- See table further below

7.6.2.5 clockAccuracy

The clockAccuracy characterizes a clock for the purpose of the best master clock (BMC) algorithm. The value of clockAccuracy shall be taken from the enumeration in Table 6. The value of this attribute shall be estimated by the clock to a precision consistent with the value of the selected enumeration, e.g., for 23₁₆ a precision of plus or minus 0.5 μs. This estimate shall be based on the timeSource attribute (7.6.2.6), the elapsed time since last synchronized to this time source, and the holdover specifications of the clock. If the

Note: Normally set to either “the time is accurate to within 25 ns (0x20)” or “the time is accurate to within 100 ns (0x21)” when the PTP Master is in sync.

Table 6 —clockAccuracy enumeration

Value (hex)	Specification
00-1F	Reserved
20	The time is accurate to within 25 ns
21	The time is accurate to within 100 ns
22	The time is accurate to within 250 ns
23	The time is accurate to within 1 μs
24	The time is accurate to within 2.5 μs
25	The time is accurate to within 10 μs
26	The time is accurate to within 25 μs
27	The time is accurate to within 100 μs
28	The time is accurate to within 250 μs
29	The time is accurate to within 1 ms
2A	The time is accurate to within 2.5 ms
2B	The time is accurate to within 10 ms
2C	The time is accurate to within 25 ms
2D	The time is accurate to within 100 ms
2E	The time is accurate to within 250 ms
2F	The time is accurate to within 1 s
30	The time is accurate to within 10 s
31	The time is accurate to >10 s
32-7F	Reserved
80-FD	For use by alternate PTP profiles
FE	Unknown
FF	Reserved

(from Salesforce Case 158356, regarding clockAccuracy values)

A) SecureSyncs

The PTP “ClockAccuracy” value for 1200 **SecureSync** PTP outputs is also the SecureSync’s current TFOM (Time Figure of Merit) value, as reported in both the **Home** page and **Management -> Disciplining** page of the SecureSyncs web browser.

For more information on the SecureSync’s **TFOM** value, please visit the online SecureSync user guide at:
http://manuals.spectracom.com/SS/Content/NC_and_SS/Com/Topics/TIME/TFOM.htm

B) Legacy VelaSyncs (for comparison)

The Clock Accuracy for **Legacy VelaSync**’s PTP outputs is derived from the Legacy VelaSync’s “**Source Accuracy**” value, as reported in **Status** tab of the Timekeeper GUI interface. For more info on Source Accuracies,

refer to the Legacy VelaSync online user guide at the following link
http://manuals.spectracom.com/VS/Content/VS/Topics/TASKS/TK_StatusMon.htm

Note that Legacy VelaSync offer an available configuration to add a minimum “floor” that prevents its Clock Accuracy value from being reported below a minimum value. As the Clock Accuracy value can directly affect the switching back and forth between active masters, over reported accuracies of very little difference between PTP masters, (such as below 10ns for instance) it may be desired to activate this “floor”, otherwise, Legacy VelaSync will report accuracies greater than this floor, resulting in the potential of often changing of which Master is the currently active master, based on minute differences in reported clock accuracies.

The field for this is the “**Limit advertised accuracy**” field. As also excerpted below, refer to the Legacy VelaSync online user guide at the following link for more information on this available/optional field:
http://manuals.spectracom.com/VS/Content/VS/Topics/TK/PTPserv_subtab.htm

Limit advertised accuracy: If set, the server will limit the accuracy advertised in PTP announce messages to be no better than the value provided (in seconds). This is helpful when trying to prevent some clients from switching between grandmasters quickly.

Additional questions also associated with Salesforce Case 158356 (answers from Denis Reilly 22 Mar 18)

Q What criteria would have to be met for the devices to send a clock accuracy of 0x20 and 0x21 then? As an example the GM is reporting 0x20 accuracy at the moment, what value of source accuracy would the GM have to have to amend the clock accuracy it send 0x21 to its clients in an announce message? I would like to know the thresholds for both the vela and sec sync and any other attributes that are used to determine the value of the clock accuracy sent in announce messages.

A In both the SecureSync and Legacy VelaSync, the clock accuracy is a measure of how far the internal system time is from the reference time (usually GPS / GNSS). When they report 0x20, it means that at the time the Announce Message was sent, we estimate there was less than 25 ns error between the internal system time (used to generate PTP hardware timestamps) and the reference time.

Q How often do the vela and secure syncs send announce messages by default

A Legacy VelaSyncs send Multicast Announce message roughly once a second by default. SecureSyncs send Multicast Announce messages every two seconds by default, but that setting is easily changed.

Q The clock accuracy value it sends in the announce message, it this based on the source accuracy at the time of sending? Or does it look over the last X amount of time?

A It is based on the instantaneous source accuracy at the time of sending.

Q What are your recommended settings to deal with accuracy issue explained. Our client has a report that checks for the GM clock accuracy and they keep seeing it change.

A For Timekeeper Legacy VelaSyncs, I would recommend changing the “limit advertised accuracy” field.

Q If I limit the accuracy advertised by the Legacy VelaSync to be 0x20 (time accurate to within 25ns), will this cause any issues if the accuracy is less than this value say to within 100ns? Will it continue to output a signal with announce messages containing info of accuracy to within 25ns even if this is actually not the case?

A That setting simply limits what is advertised in the Announce Messages to prevent clients thrashing from one PTP master to another based on the BMCA (assuming Priority1 and ClockClass are the same). The quality of the time is otherwise unaffected.

25 ns is the lowest advertised accuracy that the 1588 standard supports (See Table 6 of IEEE 1588-2008), so limiting accuracy to 25 ns does nothing. Customers who use this feature usually limit advertised accuracy to 100 ns. Or 250 ns.

If a master's current clock quality is less than 25 ns, but it is broadcasting 100 ns, this setting will may prevent a PTP client from switching to it. But the master's current clock quality may not stay below 25 ns for very long. Customers who activate this setting prefer to have the client keep listening to its current master than have it switch for a short period of time.

(Keep in mind that the other master must also be broadcasting 100 ns and is being selected based on the other BMCA parameters, so it's time is not really “bad”. Switching to a nominally better master for a short period of time can result in worse performance than not switching at all.)

Priority2

- The value of grandmasterPriority2 shall be the value of the parentDS.grandmasterPriority2 member of the data

set.

grandmasterClockIdentity

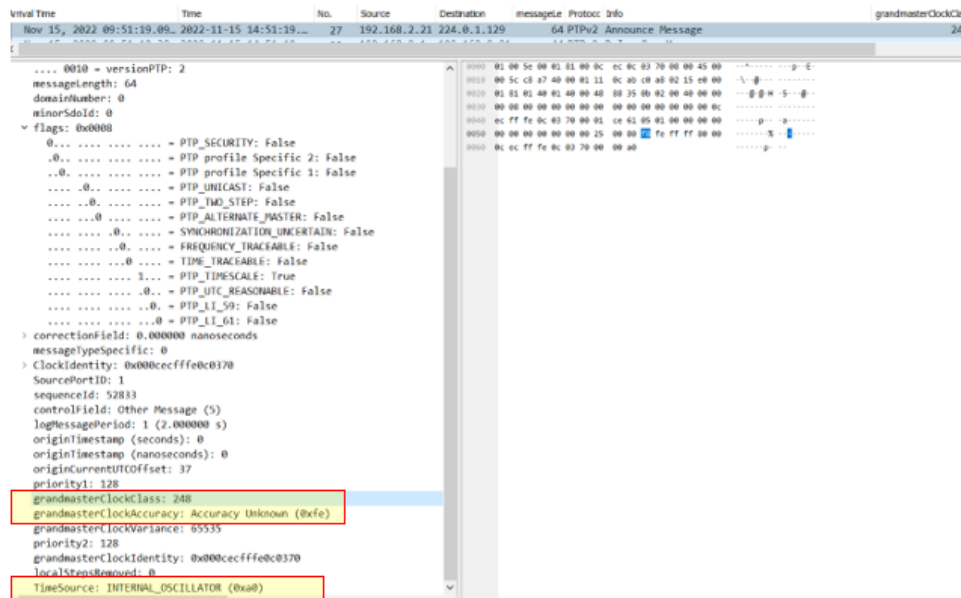
- The value of grandmasterIdentity shall be the value of the parentDS.grandmasterIdentity member of the data set.

localStepsRemoved

- The value of localStepsRemoved shall be the value of currentDS.stepsRemoved of the data set of the clock issuing this message.

TimeSource

- The value of TimeSource shall be the value of the timePropertiesDS.timeSource member of the data set.
 - We normally set this to: **GPS (0x20)**
 - FSMLAB TimeKeeper PTP master (Legacy VelaSync) sets it to: **PTP (0x40)**
 - **TimeSource” being reported as” Internal_oscillator” (not in Sync, and not in Holdover mode)**



- **TimeSource” being reported as” hand_set” (Synced to itself only)**

Best Master Clock algorithm affects Announce messages

- All masters initially listen to the Announce message of all other masters to decide who is best. The best master keeps sending it's announce message. All other masters listen to this announce and compare itself to the best master. They are not supposed to keep sending announce messages if they aren't the best master. But Legacy VelaSync/timekeeper will keep sending announce messages even if it's not the best master on the domain.

Troubleshooting Announce messages

A) No Announce messages or Sync messages being sent from a master

1204-32 and 1204-12 cards: if it's not the only master on network and it's not the best master, syncs and announce messages stop being transmitted, unless it becomes the best master.

Note: Legacy VelaSync continues sending out Announce messages even if it's not the best master.

Sync Messages (Sync Packets)

- For a description of the packet, refer to: <http://www.ieee802.org/1/files/public/docs2007/as-garner-protocol-state-machines-frame-formats-0307.pdf>
- SecureSync with **1204-32** card are reported with: “**spectrac_0a**” followed by MAC address starting with “**00:0C**”
- The MAC address for SecureSync with **1204-12** card begins with “**00:0C**” (doesn’t include **spectrac_**)
- I believe all Legacy VelaSyncs/Timekeeper master will report “**IntelCor_**”
- Sent on Port 319
- Sent from selected PTP master to clients (via unicast or multicast)
- Contains event information.

Example good Sync message (Master in Two-Step mode)

```
[- Precision Time Protocol (IEEE1588)
  [- 0000 .... = transportSpecific: 0x00
    ...0 .... = V1 Compatibility: False
    .... 0000 = messageId: Sync Message (0x00)
    .... 0010 = versionPTP: 2
    messageLength: 44
    subdomainNumber: 0
  [- flags: 0x0200
    0... .... = PTP_SECURITY: False
    .0.. .... = PTP profile specific 2: False
    ..0. .... = PTP profile specific 1: False
    .... .0.. = PTP_UNICAST: False
    .... ..1. = PTP_TWO_STEP: True
    .... ...0 = PTP_ALTERNATE_MASTER: False
    .... .... = FREQUENCY_TRACEABLE: False
    .... ...0 = TIME_TRACEABLE: False
    .... .... 0... = PTP_TIMESCALE: False
    .... .... .0.. = PTP_UTC_REASONABLE: False
    .... .... ..0. = PTP_LI_59: False
    .... .... ...0 = PTP_LI_61: False
  [- correction: 14775.000000 nanoseconds
    correction: Ns: 14775 nanoseconds
    correctionSubNs: 0.000000 nanoseconds
    clockIdentity: 0x001d9cffffebfe8fd
    sourcePortID: 2
    sequenceId: 47957
    control: Sync Message (0)
    logMessagePeriod: 0
    originTimestamp (seconds): 1436270307
    originTimestamp (nanoseconds): 967907700
```


Note that only certain flags apply to Sync messages (shown below in yellow)

No.	Time	Source	Destination	Protocol	Length	Frame	Info
168	2012-02-13 17:55:59.744630	192.168.45.81	224.0.1.129	PTPv2	86	Yes	Sync Message

Frame 168: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)

- Ethernet II, Src: Spectrac_08:03:15 (00:0c:ec:08:03:15), Dst: IPv4mcast_00:01:81 (01:00:5e:00:01:81)
- Internet Protocol Version 4, Src: 192.168.45.81 (192.168.45.81), Dst: 224.0.1.129 (224.0.1.129)
- User Datagram Protocol, Src Port: ptp-event (319), Dst Port: ptp-event (319)
 - Source port: ptp-event (319)
 - Destination port: ptp-event (319)
 - Length: 52
 - Checksum: 0xf7f7 [validation disabled]
- Precision Time Protocol (IEEE1588)
 - 0000 = transportSpecific: 0x00
 - 0000 = messageId: Sync Message (0x00)
 - 0010 = versionPTP: 2
 - messageLength: 44
 - subdomainNumber: 0
 - Flags: 0x0200
 - 0... .. = PTP_SECURITY: False
 - .0... .. = PTP profile specific 2: False
 - ..0... .. = PTP profile specific 1: False
 -0.. .. = PTP_UNICAST: False
 -1. = PTP_TWO_STEP: True
 -0 = PTP_ALTERNATE_MASTER: False
 -0.. .. = FREQUENCY_TRACEABLE: False
 -0 = TIME_TRACEABLE: False
 -0... = PTP_TIMESCALE: False
 -0.. = PTP_UTC_REASONABLE: False
 -0.. = PTP_LI_59: False
 -0 = PTP_LI_61: False
 - correction: 0.000000 nanoseconds
 - ClockIdentity: 0x000cecffffe080315
 - SourcePortID: 1
 - sequenceId: 31805
 - control: Sync Message (0)
 - logMessagePeriod: 0
 - originTimestamp (seconds): 1329155793
 - originTimestamp (nanoseconds): 802224931

Note: Spectracom SecureSyncs will report "Spectrac" with a MAC address of 00:0v. Other masters will report different info.

Correction field: is "0.000000" when Sync packet went through no switches from the Master, or through Ordinary Clocks. A Transparent Clock populates this field with its delay before sending it back out.

(2) OriginTimeStamp fields: Sync timestamp supplied to Slaves. Should never be "0" in a Sync message.

Applicable fields for Sync messages (in yellow area above)

Ethernet Header:

- SecureSync with 1204-32 card are reported with: "spectrac_0a" followed by MAC address starting with "00:0C"
- The MAC address for SecureSync with 1204-12 card begins with "00:0C" (doesn't include spectrac_)
- I believe all Legacy VelaSyncs/Timekeeper masters will report "IntelCor_")

For example, if these values aren't indicating the Announce was sent from a SecureSync, the Announce message may be being sent from either a Boundary Clock or a PTP master from another competitor. Below is an example of an announce message being sent from an Arista Network switch (likely acting as a Boundary clock):

30.997473	PTPv2	162.247.108.65	224.0.1.129	106	Announce Message[Malfor
Frame 242: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)					
Ethernet II, Src: AristaNe_1f:55:4e (00:1c:73:1f:55:4e), Dst: IPv4mcast_01:81 (01:00:5e:00:01:81)					

Precision Time Protocol header

- The proper **messagelength** field in the PTP header for a Sync message is “44”

logMessagePeriod:

In the Sync message, this field indicates the Sync message interval (in seconds) as configured in the PTP Master (such as 1 per second, for example)

Correction field:

Corrections for fractional nanoseconds, residence time and path delay in peer-to-peer transparent clocks, and asymmetry corrections

The Correction Field is the value of the correction measured in nanoseconds and multiplied by 2^{16} . E.g. 2.5 ns is represented as 0x00000000000028000

A value of one in all bits, except the most significant, of the field, shall indicate that the correction is too big to be represented.

All 0s if it didn't go through a transparent clock.

originTimestamp (Timestamp)

- The value of the originTimestamp field shall be as specified in 9.5.9 and 11.3

Flags

AlternateMasterFlag FALSE if the port of the originator is in the MASTER state

unicastFlag

- **TRUE:** if the transport layer protocol address to which this message was sent is a unicast address.
- **FALSE:** if the transport layer protocol address to which this message was sent is a multicast address

twoStepFlag.

- **For a one-step clock**, the value of twoStepFlag shall be **FALSE**.
- **For a two-step clock**, the value of twoStepFlag shall be **TRUE**.

Note: All other flags should be False

Troubleshooting Sync messages

A) No multicast Sync or announce messages being sent from a master

1204-32 and 1204-12 cards: if it's not the only master on network and it's not the best master, syncs and announce messages stop being transmitted, unless it becomes the best master.

Note: Legacy VelaSync continues sending out Announce messages even if it's not the best master.

B) Both OriginTimeStamp fields (at the end of the Sync message) are reporting a value of “0”

- These two fields should never be “0” in a Sync message
- Refer to SF case **118732** for a 1204-32 (SecureSync v5.7.0) exhibiting this condition.
- Refer to SF case **238720** for a 1204-32 (SecureSync v5.8.4) exhibiting this condition (same organization as above)

Follow-up Message:

- For a description of the packet, refer to: <http://www.ieee802.org/1/files/public/docs2007/as-garner-protocol-state-machines-frame-formats-0307.pdf>
- Sent on Port 320
- Sent from selected master, when two-step mode is enabled.
- Contains the time that the Sync message was sent.

Note that only certain flags apply to Follow-up messages (shown below in yellow)

Note: Spectracom SecureSyncs will report “Spectrac” with a MAC address of 00:0v. Other masters will report different info.

0... .. = PTP_SECURITY: False
..0... .. = PTP profile Specific 2: False
...0... .. = PTP profile Specific 1: False
...0... .. = PTP_UNICAST: False
...0... .. = PTP_TWO_STEP: False
...0... .. = PTP_ALTERNATE_MASTER: False
...0... .. = FREQUENCY_TRACEABLE: False
...0... .. = TIME_TRACEABLE: False
...0... .. = PTP_TIMESCALE: False
...0... .. = PTP.UTC_REASONABLE: False
...0... .. = PTP.LI_59: False
...0... .. = PTP.LI_61: False

correction: 0.000000 nanoseconds
correction: Ns: 0 nanoseconds
subNs: 0.000000 nanoseconds
clockIdentity: 0x000cecffe08036b
sourcePortID: 1
sequenceId: 57765
control: Follow_Up Message (2)
logMessagePeriod: 0
preciseOriginTimestamp (seconds): 1391722437
preciseOriginTimestamp (nanoseconds): 226354316

Ethernet Header:

- SecureSync with 1204-32 card are reported with: “**spectrac_0a**” followed by MAC address starting with “**00:0C**”
- The MAC address for SecureSync with 1204-12 card begins with “**00:0C**” (doesn’t include **spectrac_**)
- I believe all **Legacy VelaSyncs/Timekeeper** masters will report “**IntelCor_**”

For example, if these values aren’t indicating the Announce was sent from a SecureSync, the Announce message may be being sent from either a Boundary Clock or a PTP master from another competitor. Below is an example of an announce message being sent from an Arista Network switch (likely acting as a Boundary clock):

30.997473	PTPV2	162.247.108.65	224.0.1.129	106	Announce Message[Malto]
!!!					
Frame 242: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)					
Ethernet II, Src: AristaNe_1f:55:4e (00:1c:73:1f:55:4e), Dst: IPv4mcast_01:81 (01:00:5e:00:01:81)					

“Precision Time Protocol” header

- The proper **messagelength** field in the PTP header for a Follow-up message is “44”

logMessagePeriod:

- In the multicast follow-up message, this field indicates the Sync message interval (in seconds) as configured in the
- PTP Master (such as 1 per second, for example)
- FOR ALL OTHER MESSAGES (including unicast Sync, Follow-Up, Unicast Delay Response) this field is ignored and should be set to 0x7F / 128

PreciseOriginTimestamp (Timestamp)

- The value of the preciseOriginTimestamp shall be as specified in 9.5.10 and 11.3.

Flags

AlternateMasterFlag FALSE if the port of the originator is in the MASTER state.

Note: All other flags should be FALSE

Email from Michel (3 Mar 2014) In 2-Step mode, the t1 timestamps (timestamps of the transmission of the sync packets) shall be got from the follow-up packets, not from the sync packets. The timestamp set in a sync packet is a software timestamp. It is not precise. It shall not be used by the slaves. The precise t1 timestamp (hardware timestamp got from the IEEE1588 Ethernet chip when the sync packet is sent) is set in the follow-up packet.

Delay Request messages

- For a description of the packet, refer to: <http://www.ieee802.org/1/files/public/docs2007/as-garner-protocol-state-machines-frame-formats-0307.pdf>
- Sent on **Port 319**
- Sent from each PTP Slave to the PTP Master
- “**Transportspecific**” fields needs to be “**0x0**” (in order for the 1204-12 card to send a valid delay response containing all the necessary timestamps)

Example of a good Delay Request message

```
▣ Precision Time Protocol (IEEE1588)
  ▣ 0000 .... = transportSpecific: 0x00
    ...0 .... = v1 Compatibility: False
    .... 0001 = messageId: Delay_Req Message (0x01)
    .... 0010 = versionPTP: 2
    messageLength: 44
    subdomainNumber: 0
  ▣ flags: 0x0000
    0... .... = PTP_SECURITY: False
    .0.. .... = PTP profile Specific 2: False
    ..0. .... = PTP profile Specific 1: False
    .... .0.. = PTP_UNICAST: False
    .... ..0. = PTP_TWO_STEP: False
    .... ...0 = PTP_ALTERNATE_MASTER: False
    .... ....0. = FREQUENCY_TRACEABLE: False
    .... .....0 = TIME_TRACEABLE: False
    .... .... 0... = PTP_TIMESCALE: False
    .... .... .0.. = PTP.UTC_REASONABLE: False
    .... .... ..0. = PTP_LI_59: False
    .... .... ...0 = PTP_LI_61: False
  ▣ correction: 59345.000000 nanoseconds
    correction: Ns: 59345 nanoseconds
    correctionSubNs: 0.000000 nanoseconds
    clockIdentity: 0x001d9cffffeblacfe
    sourcePortID: 1
    sequenceId: 15638
    control: Delay_Req Message (1)
    logMessagePeriod: 127
    originTimestamp (seconds): 1436270274
    originTimestamp (nanoseconds): 26902220
```


Note that only certain flags apply to Delay Request messages (shown below in yellow)

Protocol Source Destination Length Info subdomainNumber PTP_TWO_STEP sequenceId grandmasterClockClass preciseOriginTimestamp

PTPV2 10.8.1.37 224.0.1.129 86 Delay_Req Message 0 False 54012

Frame 2463: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)

Ethernet II, Src: SuperMic_62:ee:d6 (00:25:90:62:ee:d6), Dst: IPv4mcast_01:81 (01:00:5e:00:01:81)

Internet Protocol Version 4, Src: 10.8.1.37 (10.8.1.37), Dst: 224.0.1.129 (224.0.1.129)

Version: 4
Header Length: 20 bytes

Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))

Total Length: 72

Identification: 0x0000 (0)

Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Time to live: 1

Protocol: UDP (17)

Header checksum: 0x8ce7 [validation disabled]

Source: 10.8.1.37 (10.8.1.37)

Destination: 224.0.1.129 (224.0.1.129)

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

User Datagram Protocol, Src Port: 319 (319), Dst Port: 319 (319)

Source Port: 319 (319)

Destination Port: 319 (319)

Length: 52

Checksum: 0xb2da [correct]

[Stream index: 21]

Precision Time Protocol (IEEE1588)

0000 ... = transportSpecific: 0x00

...0 ... = V1 Compatibility: False

... 0001 = messageId: Delay_Req Message (0x01)

... 0010 = versionPTP: 2

messageLength: 44

subdomainNumber: 0

flags: 0x000c

0... .. = PTP_SECURITY: False

.0.. .. = PTP profile Specific 2: False

..0. = PTP profile Specific 1: False

....0.. = PTP_UNICAST: False

....0.. = PTP_TWO_STEP: False

....0.. = PTP_ALTERNATE_MASTER: False

....0.. = FREQUENCY_TRACEABLE: False

....0.. = TIME_TRACEABLE: False

....1... .. = PTP_TIMESCALE: True

....1... .. = PTP_UTC_REASONABLE: True

....0.. = PTP_LI_59: False

....0.. = PTP_LI_61: False

correction: 0.000000 nanoseconds

correction: Ns: 0 nanoseconds

correctionSubNs: 0.000000 nanoseconds

ClockIdentity: 0x002590fffe62eed6

SourcePortID: 0

sequenceId: 54013

control: Delay_Req Message (1)

logMessagePeriod: 0

originTimestamp (seconds): 1412306273

originTimestamp (nanoseconds): 707950119

Note: if Delay Request is multicast, verify TTL value is high enough to get packet through all nodes in between.

Note: Needs to be "0x00" in order for a delay response message to be sent, especially with 1204-12 card.

Sa-20

Delay_Req message field specifications

Ethernet Header:

- SecureSyncs with 1204-32 card are reported with: "spectrac_0a" followed by MAC address starting with "00:0C"
- The MAC address for SecureSync with 1204-12 card begins with "00:0C" (doesn't include spectrac_)
- I believe all Legacy VelaSyncs/Timekeeper masters will report "IntelCor_")

Precision Time Protocol header

- The proper **messagelength** field in the PTP header for a Delay Request message is "44"

“originTimestamp (seconds)” and “originTimestamp (nanoseconds)” fields

- The value of the originTimestamp field shall be as specified in 9.5.9 and 11.3

transportSpecific field needs to be 0x0 (Denis said “0x8” is also OK for 1204-32 card, but NOT OK for 1204-12 card (r there will be no delay responses from the SecureSync, or there will the

- The valid values for this field are either 0x0 (for IEEE 1588) or 0x1 (for 802.1as).
- ptpd open source implementation software has a known issue which may send it as 0x8 (instead of 0x0). this prevents the 1204-12 card from sending delay responses. (it doesn't adversely affect 1204-32 cards, which simply ignore this invalid bit

Q from a customer, is this the “Nibble transport = 0x80;”

A Per Denis (6 Nov 2018) Yes, I think so. Here, The transportSpecific field is a nibble (4-bits) but is bits 7-4 of Byte 1 of the common header, with Bits 3-0 being the message type.

So, when you byte-align the field, a transportSpecific value of 0x8 will look like 0x80. Does that make sense?

Table 18—Common message header

Bits								Octets	Offset
7	6	5	4	3	2	1	0		
transportSpecific				messageType				1	0
reserved				versionPTP				1	1
messageLength								2	2
domainNumber								1	4
reserved								1	5
flagField								2	6
correctionField								8	8
reserved								4	16
sourcePortIdentity								10	20
sequenceId								2	30
controlField								1	32
logMessageInterval								1	33

Multiple TLVs No Delay Responses being sent from 1204-12 card

- PTP slave is trying to use Telecom profile (sending multiple TLVs)

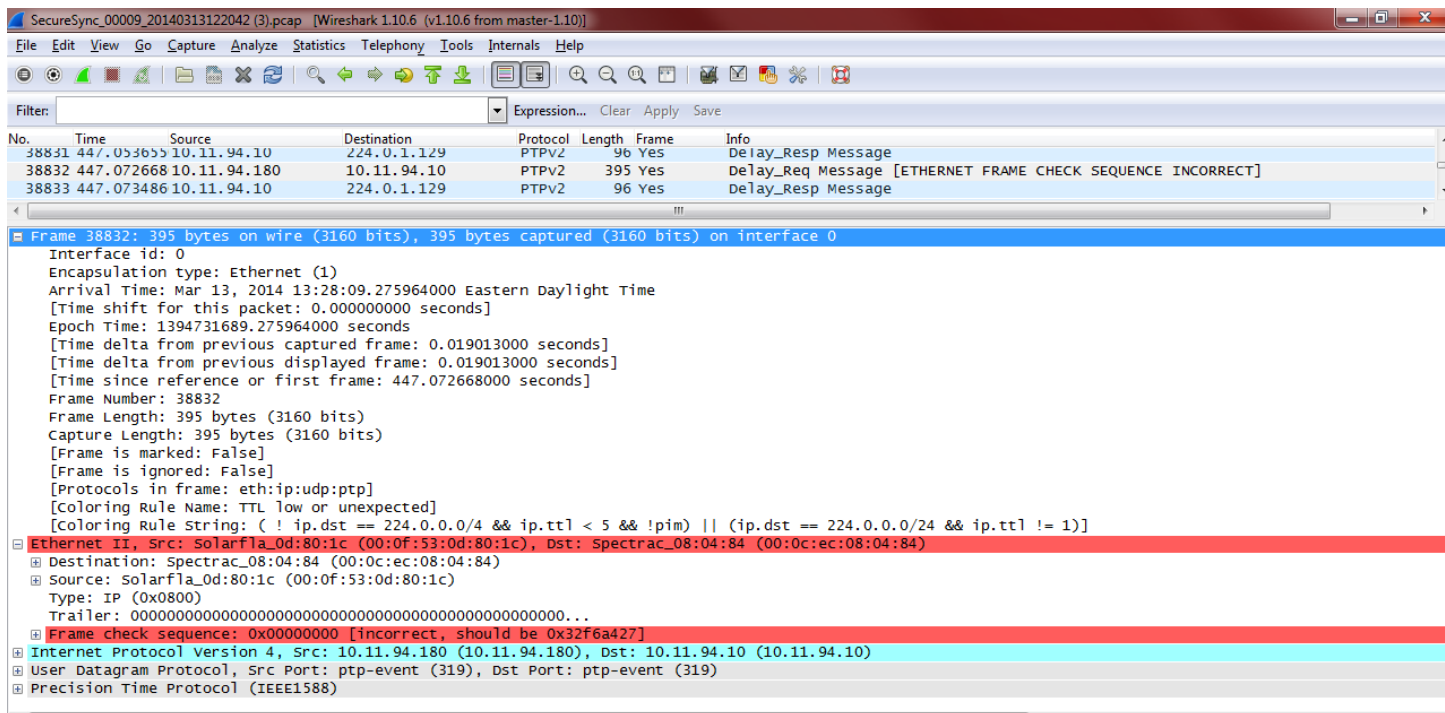
Email from Denis Reilly, 13 Mar 2014) I think Exfo is the client that tries to connect with Multiple TLV's in one message. That's explicitly called out as a possibility in the Telecom profile, but not in the main spec.

The Actarus 1204-12 card does not support this, and the Korusys 1204-32 card does.

As far as I know, there are no plans to put that function into Actarus, because Actarus is not sold as being Telecom-profile compatible. I've copied Laurent and Michel in to confirm.

Delay Requests with Frame Check Sequence (FCS) errors reported in a packet capture

- Refer to http://en.wikipedia.org/wiki/Frame_check_sequence
- Refer to Salesforce cases 13500 and 13751 for Ketchum trading
- Some Solarflare PTP slaves send longer than usual Delay Request packets which wireshark may report as Frame Check Sequence errors.



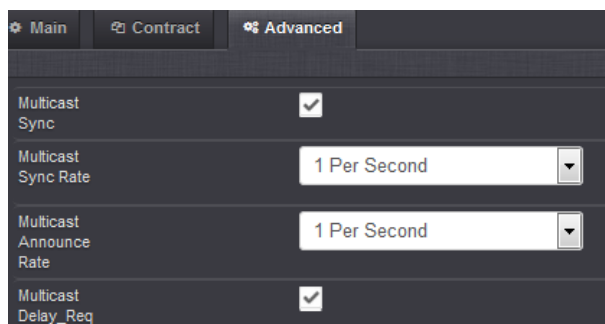
Troubleshooting Delay Requests

Delay request messages ARE present but NO delay responses present

- Is the TTL value in the Delay Request message high enough for them to reach the PTP Master?

A) Specific to 1204-32 card as the PTP Master

- Multicast Sync and Multicast Delay Responses (to multicast Delay Requests are only sent if the “Multicast Sync” and Multicast Delay_Req” checkboxes are selected in the “**Advanced**” tab for the 1204-32 card (Interfaces -> **GB PTP 0** page of the browser) as shown below:



B) Specific to 1204-12 card as the PTP Master (not applicable to 1204-32 card)

1. No Delay response from a 1204-12 card - or the “origintimestamp (nanoseconds)” field is all zeroes - because transportspecific field from Slave is invalid value “0x8” (instead of 0x0)

TransportSpecific field needs to be **0x0** (Denis said “**0x08**” is also OK for 1204-32 card, but not OK for 1204-12 card) or there will be no delay responses from the SecureSync.

- The valid values for this field are either **0x00** (for IEEE 1588) or **0x01** (for 802.1as).
- ptpd client software has a known issue which may send it as 0x08 (instead of 0x00). this prevents the 1204-12 card from sending delay responses. it doesn't adversely affect 1204-32 cards.

Q from a customer, is this the “Nibble transport = 0x80;”

A Per Denis (6 Nov 2018) Yes, I think so. Here, The transportSpecific field is a nibble (4-bits) but is bits 7-4 of Byte 1 of the common header, with Bits 3-0 being the message type.

So, when you byte-align the field, a transportSpecific value of 0x8 will look like 0x80. Does that make sense?



2. No Delay response from a 1204-12 card because of flags being incorrect values

email from Denis (12 Nov 2018) His “Unicast” and “two-step” flags in the Delay Requests are still set to ‘1’. Remember that PHY is fussy about its flags. It may be intentionally throwing out multicast packets if the UNICAST flag in the PTP message is set.

Delay Response messages

- For a description of the packet, refer to: <http://www.ieee802.org/1/files/public/docs2007/as-garner-protocol-state-machines-frame-formats-0307.pdf>
- SecureSync with 1204-32 card are reported with: “spectrac_0a” followed by MAC address starting with “00:0C”
- The MAC address for SecureSync with 1204-12 card begins with “00:0C” (doesn’t include spectrac_)
- I believe all Legacy VelaSyncs/Timekeeper master will report “IntelCor_”
- Port 320
- Sent from PTP Master (multicast or unicast), upon receipt of a Delay Request from each slave.

Note that only certain flags apply to Delay Response messages (shown below in yellow)

10.8.8.101 224.0.1.129 PTPv2 Delay_Resp Message

Frame 15: 96 bytes on wire (768 bits), 96 bytes captured (768 bits)

Ethernet II, Src: AristaNe_14:d5:84 (00:1c:73:14:d5:84), Dst: IPv4mcast_00:01:81 (01:00:5e:00:01:81)

Internet Protocol, Src: 10.8.8.101 (10.8.8.101), Dst: 224.0.1.129 (224.0.1.129)

User Datagram Protocol, Src Port: ptp-general (320), Dst Port: ptp-general (320)

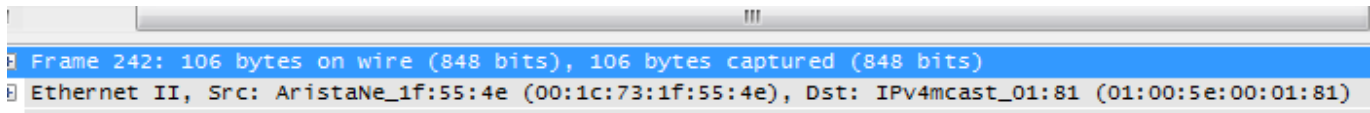
Precision Time Protocol (IEEE1588)

- 0000 = transportSpecific: 0x00
- ...0 = v1 Compatibility: False
- 1001 = messageId: Delay_Resp Message (0x09)
- 0010 = versionPTP: 2
- messageLength: 54
- subdomainNumber: 0
- Flags: 0x0000
 - 0... .. = PTP_SECURITY: False
 - .0.. .. = PTP profile Specific 2: False
 - ..0. = PTP profile Specific 1: False
 -0.. .. = PTP_UNICAST: False
 -0. = PTP_Two_STEP: False
 -0 = PTP_ALTERNATE_MASTER: False
 -0 = FREQUENCY_TRACEABLE: False
 -0 = TIME_TRACEABLE: False
 - 0... = PTP_TIMESCALE: False
 -0.. = PTP_UTC_REASONABLE: False
 -0. = PTP_LI_59: False
 -0 = PTP_LI_61: False
- correction: 0.000000 nanoseconds
- correction: Ns: 0 nanoseconds
- SubNs: 0.000000 nanoseconds
- clockIdentity: 0x000cecffe08036b
- sourcePortID: 1
- sequenceId: 5707
- control: Delay_Resp Message (3)
- logMessagePeriod: 0
- receiveTimestamp (seconds): 1391722240
- receiveTimestamp (nanoseconds): 0
- requestingSourcePortIdentity: 0x000f53fffe0d109d
- requestingSourcePortId: 1

Note: Spectracom SecureSyncs will report “Spectrac” with a MAC address of 00:0v. Other masters will report different info.

“logMessagePeriod field: PTP Master can use this field in the Delay Response message to “suggest” a new rate to the Slave (in the logMessagePeriod field of the Delay Response). If a 1204-12 card (configured as a Slave) recognizes this rate, it will start broadcasting Delay Requests at the new rate.

Ethernet Header:



- SecureSync with **1204-32** card are reported with: “**spectrac_0a**” followed by MAC address starting with “**(00:0C)**”
- The MAC address for SecureSync with **1204-12** card begins with “**00:0C**” (doesn’t include **spectrac_**)
- I believe all Legacy VelaSyncs/Timekeeper master will report “**IntelCor_**”

“Precision Time Protocol (IEEE1588)” header

```
▼ Precision Time Protocol (IEEE1588)
  > 0000 .... = transportSpecific: 0x0
  .... 1001 = messageId: Delay_Resp Message (0x9)
  .... 0010 = versionPTP: 2
  messageLength: 54
  subdomainNumber: 0
  ▼ flags: 0x0000
    0... .. = PTP_SECURITY: False
    .0.. .. = PTP profile Specific 2: False
    ..0. .. = PTP profile Specific 1: False
    .... .0.. .. = PTP_UNICAST: False
    .....0. .... = PTP_TWO_STEP: False
    .....0 .... = PTP_ALTERNATE_MASTER: False
    .....0. .... = FREQUENCY_TRACEABLE: False
    .....0 .... = TIME_TRACEABLE: False
    .....0 .... = PTP_TIMESCALE: False
    .....0.. = PTP_UTC_REASONABLE: False
    .....0. = PTP_LI_59: False
    .....0. = PTP_LI_61: False
  ▼ correction: 0.000000 nanoseconds
    correction: Ns: 0 nanoseconds
    correctionSubNs: 0 nanoseconds
    ClockIdentity: 0x000cecfffe0a16cc
    SourcePortID: 1
    sequenceId: 10424
    control: Delay_Resp Message (3)
    logMessagePeriod: 0
    receiveTimestamp (seconds): 1506000268
    receiveTimestamp (nanoseconds): 234987992
    requestingSourcePortIdentity: 0x444ca8ffffd74d53
    requestingSourcePortId: 45
```

- The proper **messagelength** field in the PTP header for a Delay Response message is “**54**”

“Delay_Resp message field” specifications

- For example, if these values aren’t indicating the Announce was sent from a SecureSync, the Announce message may be being sent from either a Boundary Clock or a PTP master from another competitor. Below is an example of an announce message being sent from an Arista Network switch (likely acting as a Boundary clock):

“**ClockIdentity**” field: with Model 1204-12 PTP card, this is the MAC address.

Note: If this value ends in 80000 (as shown below from a Delay Response message) this indicates the PTP card has lost its MAC address and needs to come back for reprogramming (been observed with 1204-12 but not with 1204-32)

```
▼ flags: 0x0000
+ correction: 0.000000 nanoseconds
ClockIdentity: 0x000cecfffe080000
SourcePortID: 1
```


Email from Denis Reilly (5 March 2014) And see how the Clock ID of the second card ends in 080000? That's bad. That means that the card lost its Serial Number.

It should come back regardless, to be reprogrammed. What S/N cards do they have? Keith, haven't we seen OC12 cards in the field lose their S/Ns before?

logMessagePeriod:

- In the **Multicast Delay Response** message, this field indicates the minimum Delay Request interval message interval (in seconds) as configured in the PTP Master (such as 1 per second, for example). This field allows the Master to "suggest" the Slave set a new rate for Delay request. If the PTP Slave is a 1204-12 card, and once the Slave recognizes this rate, it will start broadcasting at the new rate (note this may not be the case with other PTP Slaves besides the 1204-12 card).
- **FOR ALL OTHER MESSAGES** (including Unicast Sync, FollowUp, Unicast Delay Response this field is ignored and should be set to 0x7F / 128

Esther with Raytheon AMDR reported issue with Delay Request rate changing

When there is a PTP session, and the secure sync is rebooted:

1. The SecureSync resets the delay request sequence ID to start at 1
2. Delay Requests starts being sent twice a second instead of once a second
3. Once the secure sync is fully up, the sequence ID continues, is not reset, and then starts sending every 14 seconds.

Email from Denis (15 Sept 15) As far as the variation in the Delay Request rate is concerned, remember what Michel said a few weeks ago: In Multicast, The OC12 (acting as a PTP Slave) may be set to send Delay Requests at a certain rate, but there is space in the Delay Response packet for the Master to "**suggest**" a new rate to the Slave (in the logMessagePeriod field of the Delay Response). Once the OC12 recognizes this rate, it will start broadcasting at the new rate.

receiveTimestamp (Timestamp)

- The value of the receiveTimestamp shall be as specified in 9.5.12 and 11.3.
- if the ns value is all zeroes, refer to troubleshooting delay responses further below

requestingPortIdentity (PortIdentity)

- The value of the requestingPortIdentity shall be as specified in 11.3.

AlternateMasterFlag (PTP_Alternate_Master)

- **FALSE** if the port of the originator is in the **MASTER** state.
- All other flags should be **FALSE**

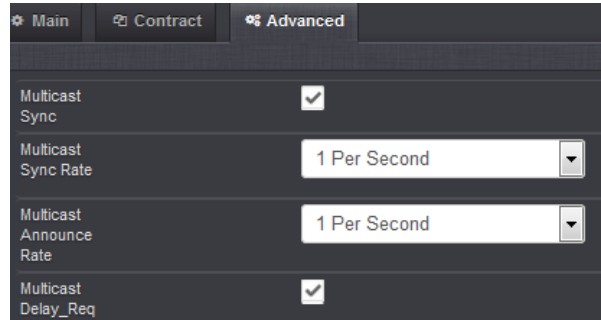
Correction field: An available field for a transparent clock (installed between the master and slave) to report its delay. The PTP master (such as the 1204-12 or 1204-32) does not populate this field, so it will be zeroes if there is no transparent clock in between.

Troubleshooting Delay Responses

A) Delay Request messages ARE present, but NO Delay Responses are present

1. 1204-32 Gb PTP card as the Master

- with Multicast Delay Requests
- Is the TTL value in the Delay Request high enough for them to reach the PTP Master?
- Multicast **Sync** and Multicast **Delay Responses** (to multicast Delay Requests are only sent if the “Multicast Sync” and Multicast Delay_Req” checkboxes are selected in the “**Advanced**” tab for the 1204-32 card (**Interfaces -> GB PTP 0** page of the browser) as shown below:



Setting	Value
Multicast Sync	<input checked="" type="checkbox"/>
Multicast Sync Rate	1 Per Second
Multicast Announce Rate	1 Per Second
Multicast Delay_Req	<input checked="" type="checkbox"/>

3. 1204-12 PTP card as the Master

4. With either Multicast or unicast Delay Requests (sent from the slave)

- Verify the complete validity of the Delay Request flags/fields (refer to “troubleshooting” in the “Delay Request” section of this document for more details)
- With Multicast Delay Requests (sent from the slave)
- Verify the complete validity of the Delay Request flags/fields (refer to “troubleshooting” in the “Delay Request” section of this document for more details)
- Is the TTL (Time to Live” value in the Delay Request high enough for them to reach the PTP Master?
- With unicast Delay Requests (sent from the slave)
- Is the Slave sending the **REQUIRED** (in all software versions) periodic unicast **contract negotiation** requests (TLV signaling messages)?

B) “ReceiveTimestamp (nanoseconds)” field is all 0s, while “ReceiveTimestamp (seconds)” is populated

- likely to only be observed with a 1204-12 card, and likely when interfacing with ptpd slaves (due to a known condition with ptpd)
- The PTP master is supposed to populate both ReceiveTimestamp...” fields
- If the 1204-12 10/100 PTP card (configured as a Master) receives a delay request message having its transportspecific field set to invalid value “**0x8**” (instead of “0x1”), the 1204-12 card’s PHY (it’s time stamper) won’t provide a timestamp to populate this field.
- Though transparent clock “0x8” is invalid, the 1204-32 Gb PTP card ignores this invalid value and still adds a timestamp to both the seconds and nanoseconds fields.

49	12.011824	192.168.0.102	224.0.1.129	PTPv2	96 Delay_Resp Message
50	12.017410	192.168.0.102	224.0.1.129	PTPv2	86 Sync Message
51	12.018297	192.168.0.102	224.0.1.129	PTPv2	86 Follow_Up Message
53	13.018147	192.168.0.102	224.0.1.129	PTPv2	86 Sync Message
54	13.019843	192.168.0.102	224.0.1.129	PTPv2	86 Follow_Up Message
55	13.019935	192.168.0.102	224.0.1.129	PTPv2	106 Announce Message
57	14.019865	192.168.0.102	224.0.1.129	PTPv2	86 Sync Message
58	14.020730	192.168.0.102	224.0.1.129	PTPv2	86 Follow_Up Message
60	15.020558	192.168.0.102	224.0.1.129	PTPv2	86 Sync Message
61	15.021422	192.168.0.102	224.0.1.129	PTPv2	86 Follow_Up Message
62	15.022285	192.168.0.102	224.0.1.129	PTPv2	106 Announce Message
64	16.022249	192.168.0.102	224.0.1.129	PTPv2	86 Sync Message
65	16.023087	192.168.0.102	224.0.1.129	PTPv2	86 Follow_Up Message
67	17.023026	192.168.0.102	224.0.1.129	PTPv2	86 Sync Message
68	17.023891	192.168.0.102	224.0.1.129	PTPv2	86 Follow_Up Message
69	17.024755	192.168.0.102	224.0.1.129	PTPv2	106 Announce Message
70	17.094719	192.168.0.103	224.0.1.129	PTPv2	86 Delay_Req Message
71	17.095765	192.168.0.102	224.0.1.129	PTPv2	96 Delay_Resp Message
73	18.024650	192.168.0.102	224.0.1.129	PTPv2	86 Sync Message
74	18.025514	192.168.0.102	224.0.1.129	PTPv2	86 Follow_Up Message

0000 = transportSpecific: 0x0

.... 1001 = messageId: Delay_Resp Message (0x9)

.... 0010 = versionPTP: 2

messageLength: 54

subdomainNumber: 0

flags: 0x0000

correction: 0.000000 nanoseconds

ClockIdentity: 0x000cecfffe0805e3

SourcePortID: 1

sequenceId: 3

control: Delay_Resp Message (3)

logMessagePeriod: 4

receiveTimestamp (seconds): 1541690624

receiveTimestamp (nanoseconds): 0

requestingSourcePortIdentity: 0x021213ffffe101512

requestingSourcePortId: 1

Peer Delay Request message

- For a description of the packet, refer to: <http://www.ieee802.org/1/files/public/docs2007/as-garner-protocol-state-machines-frame-formats-0307.pdf>

13.9.1 General Pdelay_Req message specifications

The fields of the Pdelay_Req message shall be as specified in Table 29.

Table 29—Pdelay_Req message fields

Bits								Octets	Offset
7	6	5	4	3	2	1	0		
header (see 13.3)								34	0
originTimestamp								10	34
reserved								10	44

NOTE: The reserved field in the Pdelay_Req message is to make the message length match the length of the Pdelay_Resp message. In some networks and bridges, messages with unequal lengths have different transit times that introduce asymmetry errors.

Pdelay_Req message field specifications

originTimestamp (Timestamp)

- The value of the originTimestamp shall be as specified in 11.4.3.

Peer Delay Request/Peer Delay Response (Path_delay_Resp) message

- For a description of the packet, refer to: <http://www.ieee802.org/1/files/public/docs2007/as-garner-protocol-state-machines-frame-formats-0307.pdf>

- Peer Delay Request = Either “Path_delay_Req” or “Pdelay_Req”
- Peer Delay Response = Either “Path_delay_Resp” or “Pdelay_Resp”
- Peer Delay Response Follow Up= Either “Path_delay_Resp_Follow_Up” or “Pdelay_Resp_Follow_Up”

A) General Pdelay_Req message specifications

- Event message (sent on port 319)

3.7 Pdelay_Req message

3.7.1 General Pdelay_Req message specifications

The fields of the Pdelay_Req message shall be as specified in Table 11.

Table 11: Pdelay_Req message fields

17

Bits								Octets	Offset
7	6	5	4	3	2	1	0		
header (section 3.3)								34	0
originTimestamp								10	34
Reserved								10	44

originTimestamp (Timestamp)

The value of the originTimestamp shall be 0.

3.8 Pdelay_Resp message

B) General Pdelay_Resp message specifications

- Event message (sent on port 319)

Event message (sent on port 319)

- The fields of the Pdelay_Resp message shall be as specified in Table 30.

Table 30—Pdelay_Resp message fields

Bits								Octets	Offset
7	6	5	4	3	2	1	0		
header (see 13.3)								34	0
requestReceiptTimestamp								10	34
requestingPortIdentity								10	44

Pdelay_Resp message field specifications

requestReceiptTimestamp (Timestamp)

- The value of the requestReceiptTimestamp shall be as specified in 11.4.3.

C) Peer Delay Response Follow_up

- General message (sent on port 320)
-

3.9 Pdelay_Resp_Follow_Up message

3.9.1 General Pdelay_Resp_Follow_Up message specifications

The fields of the Pdelay_Resp_Follow_Up message shall be as specified in Table 13.

Table 13: Pdelay_Resp_Follow_Up message fields

Bits								Octets	Offset
7	6	5	4	3	2	1	0		
header (section 3.3)								34	0
responseOriginTimestamp								10	34
requestingPortIdentity								10	44

responseOriginTimestamp (Timestamp)

18

The value of the responseOriginTimestamp shall be 0.

requestingPortIdentity (PortIdentity)

The value of the requestingPortIdentity shall be the value of the sourcePortIdentity of the corresponding Pdelay_Req message.

5. References

PTP Management messages

- Management messages are used to access attributes and to generate certain events defined in the IEEE1588 standard.
- PTP management messages are specified in IEEE1588 (Clause 12)
- Many PTP devices have not supported management messages yet

15.4 Management message format

15.4.1 Common fields

The common fields of a management message shall be as specified in Table 37.

Table 37—Management message fields

Bits								Octets	Offset
7	6	5	4	3	2	1	0		
header (see 13.3)								34	0
targetPortIdentity								10	34
startingBoundaryHops								1	44
boundaryHops								1	45
reserved				actionField				1	46
reserved								1	47
managementTLV								M	48

15.4.1.1 domainNumber of the header

The domainNumber of the message common header (see 13.3) of a management message shall specify the target domain.

15.4.1.2 sequenceId of the header

The sequenceId of the message common header (see 13.3) of a response management message shall be set to the sequenceId of the received management message causing the response. Otherwise the sequenceId shall be as specified in 7.3.7.

15.4.1.3 targetPortIdentity (PortIdentity)

The targetPortIdentity field shall be the portIdentity of the port or node on which the management message acts.

NOTE—The port identified by targetPortIdentity is not necessarily the port on which the management message was received.

In the case of a management message transmitted by a clock to a manager, the targetPortIdentity field shall be set to the sourcePortIdentity of the management message to which it is a response.

15.4.1.4 startingBoundaryHops (UInteger8)

The value of the startingBoundaryHops field is implementation-dependent for messages that are not issued in response to a request from another management message. For management messages that are issued in response to a request from another management message, the value of startingBoundaryHops shall be the value computed from the startingBoundaryHops and boundaryHops fields of the requesting message as (startingBoundaryHops minus boundaryHops).

NOTE—When a management message is received, the absolute value of this difference indicates the number of retransmissions by boundary clocks that the message experienced.

15.4.1.5 boundaryHops (UInteger8)

The value of the boundaryHops field indicates the remaining number of successive retransmissions of the management message by boundary clocks receiving the message per 15.3.3. The value of boundaryHops shall be identical to the value of the field startingBoundaryHops when first transmitted by the issuing clock.

15.4.1.6 actionField (Enumeration4)

The value of the actionField shall indicate the action to be taken on receipt of the message as defined in Table 38.

Table 38—Values of the actionField

Action	Action taken	Value (hex)
GET	The management message shall carry a single management TLV. The managementId field of the TLV indicates the specific information that needs to be retrieved. The current values of the data identified by the managementId shall be returned in a management TLV with the actionField value set to RESPONSE. If an error occurs, a management error status TLV shall be returned with the actionField value set to RESPONSE.	0
SET	The management message shall carry a single management TLV. The data in the TLV shall be used to update the current value of the data identified by the managementId field. Attempts to set a static or nonconfigurable value shall return a management error status TLV; see 15.5.4. If the update is successful, a management message with the actionField value set to RESPONSE shall be returned. If an error occurs, a management error status TLV shall be returned with the actionField value set to RESPONSE. If the data identified by the managementId consists of several fields, the update shall be considered as an atomic actionField and the failure to update any item shall be considered an error in the execution of the SET. TLVs with data definitions that mix configurable and nonconfigurable data are not permitted.	1
RESPONSE	The data in the TLV shall be the current values of the data identified by the managementId field of the management message with the GET or SET actionField. The value of the managementId shall be identical to that in the requesting message. If the actionField required by the GET or SET actionFields could not be fully executed, the response shall be a management error status TLV; see 15.5.4.	2
COMMAND	The event indicated by the managementId field shall be initiated. The results of this command shall be acknowledged by a management message with actionField set to ACKNOWLEDGE.	3
ACKNOWLEDGE	An acknowledge management message is a response to a command management message. The value of the managementId shall be identical to that in the command message. If the command could not be executed, the acknowledge message shall be a management error status TLV.	4
Reserved		5-F

Table 40—managementId values

managementId name	managementId value (hex)	Allowed actions	Applies to
Applicable to all node types	0000 – 1FFF		
NULL_MANAGEMENT	0000	GET, SET, COMMAND	port
CLOCK_DESCRIPTION	0001	GET	port
USER_DESCRIPTION	0002	GET, SET	clock
SAVE_IN_NON_VOLATILE_STORAGE	0003	COMMAND	clock
RESET_NON_VOLATILE_STORAGE	0004	COMMAND	clock
INITIALIZE	0005	COMMAND	clock
FAULT_LOG	0006	GET	clock
FAULT_LOG_RESET	0007	COMMAND	clock
Reserved	0008 – 1FFF	—	—
Applicable to ordinary and boundary clocks	2000 – 3FFF		
DEFAULT_DATA_SET	2000	GET	clock
CURRENT_DATA_SET	2001	GET	clock
PARENT_DATA_SET	2002	GET	clock
TIME_PROPERTIES_DATA_SET	2003	GET	clock
PORT_DATA_SET	2004	GET	port
PRIORITY1	2005	GET, SET	clock
PRIORITY2	2006	GET, SET	clock
DOMAIN	2007	GET, SET	clock
SLAVE_ONLY	2008	GET, SET	clock
LOG_ANNOUNCE_INTERVAL	2009	GET, SET	port
ANNOUNCE_RECEIPT_TIMEOUT	200A	GET, SET	port
LOG_SYNC_INTERVAL	200B	GET, SET	port
VERSION_NUMBER	200C	GET, SET	port
ENABLE_PORT	200D	COMMAND	port
DISABLE_PORT	200E	COMMAND	port
TIME	200F	GET, SET	clock
CLOCK_ACCURACY	2010	GET, SET	clock
UTC_PROPERTIES	2011	GET, SET	clock
TRACEABILITY_PROPERTIES	2012	GET, SET	clock
TIMESCALE_PROPERTIES	2013	GET, SET	clock
UNICAST_NEGOTIATION_ENABLE	2014	GET, SET	port
PATH_TRACE_LIST	2015	GET	clock
PATH_TRACE_ENABLE	2016	GET, SET	clock
GRANDMASTER_CLUSTER_TABLE	2017	GET, SET	clock
UNICAST_MASTER_TABLE	2018	GET, SET	port
UNICAST_MASTER_MAX_TABLE_SIZE	2019	GET	port
ACCEPTABLE_MASTER_TABLE	201A	GET, SET	clock
ACCEPTABLE_MASTER_TABLE_ENABLED	201B	GET, SET	port
ACCEPTABLE_MASTER_MAX_TABLE_SIZE	201C	GET	clock
ALTERNATE_MASTER	201D	GET, SET	port
ALTERNATE_TIME_OFFSET_ENABLE	201E	GET, SET	clock
ALTERNATE_TIME_OFFSET_NAME	201F	GET, SET	clock
ALTERNATE_TIME_OFFSET_MAX_KEY	2020	GET	clock
ALTERNATE_TIME_OFFSET_PROPERTIES	2021	GET, SET	clock
Reserved	2022 – 3FFF	—	—
Applicable to transparent clocks	4000 to 5FFF		
TRANSPARENT_CLOCK_DEFAULT_DATA_SET	4000	GET	clock
TRANSPARENT_CLOCK_PORT_DATA_SET	4001	GET	port
PRIMARY_DOMAIN	4002	GET, SET	clock
Reserved	4003 – 5FFF	—	—
Applicable to ordinary, boundary, and transparent clocks	6000 – 7FFF		
DELAY_MECHANISM	6000	GET, SET	port
LOG_MIN_PDELAY_REQ_INTERVAL	6001	GET, SET	port
Reserved	6002 – BFFF	—	—
This range is to be used for implementation-specific identifiers	C000 – DFFF	—	—
This range is to be assigned by an alternate PTP profile	E000 – FFFE	—	—
Reserved	FFFF	—	—

****PTP packet timestamps / structure / Flag fields**

Packet timestamps

Email from Denis Reilly = Packets sent to the general UDP port are not timestamped, packets sent to the event port are. I need to remember this in the future.

Note: Also refer to the SecureSync Option Card info document [EQUIPMENT\SPECTRACOM\EQUIPMENT\SecureSync\Option Cards\SecureSync Option Card information.pdf](#) (in the Sections for Option Cards 1204-12 and 1204-32) for additional info on PTP packet capture analysis.

Packet structure

Note: Refer to Section 13 of the IEEE 1588-2008 spec for information on all of the PTP packet bits

For the latest specs, refer to IEEE-1588-2006V2, at the following link in Sharepoint

<https://oro.liagroup-portal1.sharepoint.com/Spectracom/Engineering/Projects/GeneralPTP/SitePages/Home.aspx?RootFolder=%2FSpectracom%2FEngineering%2FProjects%2FGeneralPTP%2FShared%20Documents%2FStandards&FolderCTID=0x0120001C144F4F864D1D45AC2929A4327F8AB1&View={D793DF9A-1DF4-4C45-BF93-0BA34459C1FE}&InitialTabId=Ribbon%2EDocument&VisibilityContext=WSSTabPersistence>

Refer to sample PTP packets captured with wireshark: [I:\Customer Service\PTP\ptpd.pcap](#)

Note: Example Sections below shown in order of a wireshark packet capture

Ethernet section

```

Ethernet II, Src: Spectrac_08:03:15 (00:0c:ec:08:03:15), Dst: IPv4mcast_00:01:81 (01:00:5e:00:01:81)
  Destination: IPv4mcast_00:01:81 (01:00:5e:00:01:81)
    Address: IPv4mcast_00:01:81 (01:00:5e:00:01:81)
    ....1.... = IG bit: Group address (multicast/broadcast)
    ....0.... = LG bit: Globally unique address (factory default)
  Source: Spectrac_08:03:15 (00:0c:ec:08:03:15)
    Address: Spectrac_08:03:15 (00:0c:ec:08:03:15)
    ....0.... = IG bit: Individual address (unicast)
    ....0.... = LG bit: Globally unique address (factory default)
  Type: IP (0x0800)
```

Internet Protocol section

```

Internet Protocol, Src: 192.168.45.81 (192.168.45.81), Dst: 224.0.1.129 (224.0.1.129)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    ....0.. = ECN-Capable Transport (ECT): 0
    ....0.. = ECN-CE: 0
  Total Length: 72
  Identification: 0xd15b (53595)
  Flags: 0x00
    0... .. = Reserved bit: Not set
    .0... .. = Don't fragment: Not set
    ..0... .. = More fragments: Not set
  Fragment offset: 0
  Time to live: 255
  Protocol: UDP (17)
  Header checksum: 0x1ace [correct]
    [Good: True]
    [Bad: False]
  Source: 192.168.45.81 (192.168.45.81)
  Destination: 224.0.1.129 (224.0.1.129)
```


User Datagram Protocol section

```
[-] User Datagram Protocol, Src Port: ptp-event (319), Dst Port: ptp-event (319)
  Source port: ptp-event (319)
  Destination port: ptp-event (319)
  Length: 52
  [-] Checksum: 0x9f21 [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
```

Flags section (common in all PTP packets):

```
[-] flags: 0x0200
  0... .. = PTP_SECURITY: False
  .0.. .. = PTP profile Specific 2: False
  ..0. .. = PTP profile Specific 1: False
  ....0.. = PTP_UNICAST: False
  ....1. .. = PTP_Two_STEP: True
  ....0 .. = PTP_ALTERNATE_MASTER: False
  ....0. .. = FREQUENCY_TRACEABLE: False
  ....00 .. = TIME_TRACEABLE: False
  ....0... = PTP_TIMESCALE: False
  ....0... = PTP_UTC_REASONABLE: False
  ....0. .. = PTP_LI_59: False
  ....0... = PTP_LI_61: False
```

Correction fields section

```
[-] correction: 0.000000 nanoseconds
  correction: Ns: 0 nanoseconds
  subNs: 0.000000 nanoseconds
  _ _ _ _ _
```

At end of packet

```
ClockIdentity: 0x000cecfffe080315
SourcePortID: 1
sequenceId: 31751
control: Sync Message (0)
logMessagePeriod: 0
originTimestamp (seconds): 1329155739
originTimestamp (nanoseconds): 763582131
```

Mean path delay

- Refer to **“Mean Path Delay”** in the SecureSync Option Card document: <I:\Customer Service\1- Cust Assist documents\SecureSync Option Card information.pdf>

Packet Delay Variation (PDV)

- Apparently, part of the Telecom profile

Q. From Semic to Sylvain regarding 1204-12 Option Card

A Response from Sylvain) 27 Aug 2014)

We don't specify maximum acceptable PDV in our current documentation. However, Telecom standards specify a maximum acceptable PDV in a network (for frequency transfer applications)

Ø Such specification is described in ITU-G.8261.1: « In any 200 s window, at least 1%, with a minimum of 2 packets, should be observed in a cluster comprised between floor delay and floor delay + 150 us »*

*This can be used as a starting point; measuring the PDV requires dedicated measurement equipment.

Distance limitations for PTP networks

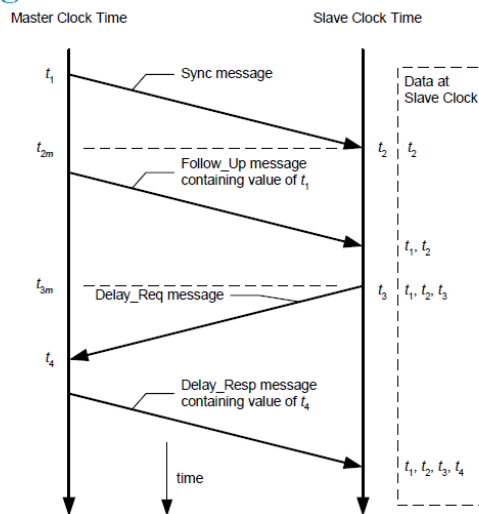
1/19/11 KW- Alan Dodge from JDSU was having trouble with TSync-PTP. Based on their findings, Denis Reilly responded with:

I don't think we should spend too much time looking into this for the customer, because 120M is longer than the 100M cable length spec. The fact that other products work with this long cable is a bit troublesome. I will make a note to test with a 100M cable length. But even if we fail, the solution would likely be with a hardware change, which won't help current customers, and we probably won't even do unless we get a ton of complaints.

Link State Parameter

1/19/11 kw- Email from Denis: The "link state" parameter only means that the Ethernet cable is connected and a network is detected. It does not give any indication of signal integrity. When the link is active, our PTP slave will enter the "listening" state and listen for active masters. If there are signal integrity problems, and our PTP slave cannot receive valid packets from the GrandMaster, it will stay in the Listening state.

Timing diagram



Peer to Peer = Sync, Follow_Up, Delay_Req, Delay_Resp
Sync, Follow_Up, Pdelay_Req, Pdelay_Resp, Pdelay_Resp_Follow_Up

As the PTP protocol was designed with no interoperability with the NTP Service in mind, computers running NTP service should halt NTP service before running PTP service.

PTP PCI Express Card Feature Matrix (Tsync-PTP)		
Vendor	Meinberg (GPS)	Spectracom
	GPS170PEX	TSync-PCIe-PTP
Sync Inputs		
1PPS	NO	YES
AM and DCLS time code inputs	YES	YES
IRIG A, B, IEEE 1344	YES	YES
IRIG E, G, NASA 36, XR3, 2137	YES	YES
Sync Outputs		
1PPS	YES	YES
IRIG B, IEEE 1344	YES	YES
IRIG A, E, G, NASA 36, XR3, 2137	YES	YES
Simultaneous AM and DCLS time code outputs	NO	YES
Timing Functions		
Accuracy	1 microsecond	1 microsecond
Resolution	+/- 20 ns	5 ns
Event Time Capture/Interrupts	2x Event Captures	4x Event Captures
10 MHz sine out	YES	YES
Software and Drivers		
Windows	YES	YES
Solaris	NO	YES
Linux	YES	YES

(Tsync-PTP)

- The PTP module can be configured as either a Master or a Slave.
- The PTP module is installed in place of the GPS receiver.
- The TSync board can't have a both a PTP module and GPS receiver installed. So, when used as a master, the TSync-PCIe board has to use IRIG input from a NetClock/SecureSync or other IRIG generator. The IRIG source can be synced to GPS and output IRIG to the Master, but the Master itself cannot be directly synced to GPS.
- We recommend using a dedicated PTP network for optimum performance, but it can operate on a standard network. However, other packets on the network can degrade the overall performance of PTP.
- We recommend using routers/switches designed for PTP operation to better account for its delays. Using standard switches/routers won't account for its delays.

TAI timescale:

The PTP protocol transmits time in TAI time scale but also provides the UTC to TAI correction factor so slaves can calculate UTC from the received TAI time.

Selecting the TAI timescale is a good decision to prevent leap seconds from occurring on the outputs of the TSync-PCIe boards. Internal to the boards, as long as the PTP Master is synced to an external source that is providing leap second information (such as the SecureSync grandmaster will) changes to both the UTC to GPS and UTC to TAI time correction factors will still occur internal to the PTP master and slaves at the moment a leap second occurs, but the TAI timescale outputs themselves will be seamless at the moment the leap second is asserted (no TAI time jumps will occur).

The PTP master provides the time to the slaves in TAI timescale as well as a TAI to UTC correction factor. When a leap second occurs, the correction factor needs to also change (either automatically or manually) so that the UTC time can be continue to be accurately calculated internal to the TSync boards. If the PTP master knows that the leap second is going to be asserted (such as a SecureSync synced to GPS), it can automatically update the correction value and distribute the new value to all of the slaves.

If the PTP master is not aware that a leap second is pending or has already occurred (and is not manually updated by a user), the correction factor sent to the slaves won't be updated and the worst effect of this is the TAI time is off from UTC

time by exactly the number of leap seconds that have occurred since the TAI correction was manually entered (for example, if one leap second was asserted since TAI was configured, the master and slaves will be exactly one second away from the “real” time). But if you only care about relative time and don’t care about absolute time, this one second time error won’t matter. If you do care about both relative and absolute time, the TAI correction factor needs to be either manually or automatically updated in the PTP master so it can distribute it to the slaves. The SecureSync grandmaster will be able to automate the leap second process with seamless transitions on the outputs.

(Prior to 30 June 2012)

*** TAI offset is equal to the number of UTC leap seconds for GPS correction +19 (There were 19 TAI seconds already when GPS was brought online.

Example (based on 1/14/11 - UT1 is currently 15, plus 19= 34. The TAI offset is 34.

Refer to <http://leapsecond.com/java/gpsclock.htm>

*** TAI offset is equal to the number of UTC leap seconds for GPS correction +19 (There were 19 TAI seconds already when GPS was brought online.

(After 30 June 2012) Example (UT1 is currently 16, plus 19= 35. The TAI offset is 35)

(Before 30 June 2012) Example (UT1 was 15, plus 19= 34. The TAI offset was 34).

Refer to <http://leapsecond.com/java/gpsclock.htm>

Sending PTP through a firewall

Q. Does spectracom have any experience in sending PTP through a non-PTP enabled firewall? Is it a recommended solution?

A (email from Denis Reilly, 28 Sept 15) PTP will “work” through a firewall, but the whole point of a firewall is to inspect packets and determine whether or not they should be let through or not, and that adds latency. We know that variable latency is bad for PTP. If the process of inspecting packets adds variable latency, that will affect performance. So if you want sub-ns performance, I would not recommend it unless you know that the latency through the firewall is very low to begin with (because then the variations in latency will be much smaller).

*****SMPTE profile**

Q (from Keith to Denis Reilly) I just received a call from “Ken” on the West Coast regarding Legacy VelaSync and whether it supported SMPTE time code. He said you were looking into this for him.

I believe, but don’t for certain, that the Legacy VelaSync does not currently support SMPTE. If it doesn’t, he would like to know if there are any plans on adding it (I haven’t heard any plans for this, but again, I can’t say there isn’t).

If Denis can’t confirm that it doesn’t currently support it and whether there are any plans for FSMLabs to support it in the future, I will run this one by FSMLabs to get their input so that you can get back to him.

A Reply from Denis Reilly 20 Jun 16) There are more than one type of SMPTE code, there is the traditional “SMPTE Timecode” which resembles IRIG, but is oriented toward traditional motion picture frame rates.

And there is the newer “SMPTE profile” for PTP, which provides time over a standard Ethernet network.

We don’t support either, but just wanted to point that out.

FAQs for PTP

The advantage of PTP over IRIG:

- Eliminates need to run dedicated coax or twisted pairs for timing signals.
- PTP automatically accounts for cable delays while IRIG requires manual calculation and configuration for cable delays.

Q. The customer supposes to use it as Slave only now. Is there a reduced option w/o many inputs (PTP network input only) at less pricing?

A. **(response from John Fischer)** In the PTP protocol, the complexity is more in the Slave side than in the Master. The Master simply broadcasts the precise time. The Slave receives that time and then must discipline its local oscillator to match to the Master, filtering out VPD noise and accounting for network traffic issues. Also, in a redundant network with multiple Masters, the Slave performs the Best Master Clock algorithm, which chooses the best Master. In most protocols, the Master is the controller, but PTP is somewhat unusual with the Slave doing most of the processing.

Q. Question I posed to Denis about the PTP module port number- - Can a customer inadvertently change the PTP port to a value like 2? And if so, will this completely “break” the PTP messages from being able to go out?

A. **Denis’ answer:** I don’t think customers can change this. There is a knob in the UI for “PTP Port Number”, but I think the knob is there to indicate which port you want to modify, not to modify the port number itself. So even if customers mess with it, I don’t think they can break anything.

PTP Client Software (Windows client software PTP/TimeKeeper/PTPd)

Windows PTP client software

1. FSM TimeKeeper software for Windows (no longer available from us)

- ~~Availability for Windows software started in timekeeper version 7.1.0 (24 Sept 15). Available from Spectracom sometime after Nov, 2015.~~
- ~~Refer to the "Timekeeper" section of the Legacy VelaSyncandGeoCustAssistance doc for details~~

2. Time Machines, Inc. (Utility included in Windows Server 2019 and Windows 10 (v1809))

- <https://timemachinescorp.com/wp-content/uploads/Windows10PTPClient.pdf>

TimeMachines, Inc.
300 S 68th St Place, STE 300
Lincoln, NE 68510

3. Greyware's Domain Time II PTP software for Windows

- Refer to: <https://www.greyware.com/software/domaintime/index.asp>
- Can operate as PTP Client or PTP Master

Email from Jeremy Onyan (8/24/12)

Regarding PTP client for Windows, Dick Fox found this a couple of days ago:

<http://www.greyware.com/software/domaintime/v5/configuration/server/ptp.asp>

Obviously not something we sell, but wanted to put in on the radar since there is in fact a Windows based PTP client SW available.

4. Real Time System PTP software for Windows

Email from Lisa Perdue (31 March 2014) FYI- this software boasts Windows PTP hardware timestamping (with a certain NIC in the PC). The thing is, it doesn't need us at all ☹ (except as the PTP master). But just wanted to share it with you.

http://www.nstarsolutions.com/store/home.php?provider=Real-Time_Systems

Linux PTPD/PTP4L client software

Available programs for Linux

- 1) PTPd (open source software) (See “A” further below)
- 2) PTP4L
- 3) Linux Redhat 6.5 (and higher) distribution (See “B” further below)
- 4) ~~Spectracom TimeKeeper software (See “C” further below)~~ (no longer available from us)

A) PTPd software

- We don't support PTPd software itself.
- PTPd is a free (freeware), open source PTP client software for Linux.
- It is based on IEEE-1588-2002.

We only provide cursory support for this program (such as troubleshooting PTP time stamps being available to the software, for instance). ~~Unlike Timekeeper~~

Email from Denis Reilly: I wanted to let you know that we really can't speak too much about PTPd. We haven't spent much too time using it. We primarily work with our PTP timekeeper software that we offer for purchase. Jeremy can provide you with additional information on this available software (if he hasn't already) if you are interested!

PTPd messages

A) `“(slv) Ignored followup, SequenceID doesn't match with last Sync message”`

Full message: 2014-10-22 10:48:12.794067 ptpd2[3785].md1 (info)(slv) Ignored followup, SequenceID doesn't match with last Sync message

- Refer to sites such as: <http://sourceforge.net/p/ptpd/discussion/469208/thread/451deb55/>

"This can happen if you're using two-step mode and packets got reordered when traversing the network - it might be the case that you received a follow-up before you received the sync it belonged to. However, there was also a sequence number rollover bug that I think manifested itself identically - nothing to worry about, dropping one message will not decrease the performance drastically. If it is the sequence number issue, try version 2.2.2 and or better the current svn trunk."

Issues with PTPd software

A) Issues with Delay requests affecting Delay Response messages sent from the 1204-12 (and 1204-32) card: poor sync issues – due to transportSpecific field set to 0x08 (instead of 0x00).

- Transport specific field in delay request should always be set to **0x00**. However, this issue can change this field to **0x08**, causing 1204-12 card (and 1204-32 card, in at least software versions 5.8.6 and below) to either:
 - **Not** respond with a Delay Response message
 - Or if its Delay response is sent, its **“Receivetimestamp (nanoseconds)”** field will be set to all 0's.

19	1.297827	10.105.116.104	224.0.1.129	PTPv2	Delay_Req Message
20	1.417372	10.105.116.40	224.0.1.129	PTPv2	Delay_Req Message
21	1.534342	10.105.110.119	224.0.1.129	PTPv2	Delay_Req Message
22	1.535567	10.8.8.101	224.0.1.129	PTPv2	Delay_Resp Message
23	1.624829	AristaNe_15:83:7c	PVST+	STP	RST. Root = 32768/1757/00:1c:73:13:46:7a Cost = 4000 P
24	1.653017	10.105.110.117	224.0.1.129	PTPv2	Delay_Req Message
25	1.654241	10.8.8.101	224.0.1.129	PTPv2	Delay_Resp Message
26	1.949183	10.105.116.105	224.0.1.129	PTPv2	Delay_Req Message
27	2.002515	10.8.8.101	224.0.1.129	PTPv2	Sync Message
28	2.003007	10.8.8.101	224.0.1.129	PTPv2	Follow_up Message
29	2.282117	10.105.110.117	224.0.1.129	PTPv2	Delay_Req Message
30	2.283335	10.8.8.101	224.0.1.129	PTPv2	Delay_Resp Message
31	2.292386	10.105.116.40	224.0.1.129	PTPv2	Delay_Req Message
32	2.395442	10.105.110.119	224.0.1.129	PTPv2	Delay_Req Message
33	2.396641	10.8.8.101	224.0.1.129	PTPv2	Delay_Resp Message


```

Frame 19: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: Solarfla_Od:b3:61 (00:0f:53:0d:b3:61), Dst: IPv4mcast_00:01:81 (01:00:5e:00:01:81)
Internet Protocol, Src: 10.105.116.104 (10.105.116.104), Dst: 224.0.1.129 (224.0.1.129)
User Datagram Protocol, Src Port: ptp-event (319), Dst Port: ptp-event (319)
Precision Time Protocol (IEEE1588)
  1000 .... = transportSpecific: 0x08
  .... 0001 = messageId: Delay_Req Message
  .... 0010 = versionPTP: 2
  .....

```

TransportSpecific should be “0x00”. If its “0x8”, the 1204-12 card (as a PTP Master) will send a Delay Response packet with its “**Receivetimestamp (nanoseconds)**” field set to all 0’s. This adversely affect the time sync of the client

Note: Like the 1204-12 PTP card, even the 1204-32 GB PTP Option Card (in at least versions 5.8.6 and below), also ignores Delay Requests having transportspecific value other than 0

Per Denis Reilly (Oct 2019) I finally got some time to test these delay responses, and I was surprised to find out that the -32 card does ignore Delay Requests with the transportSpecific field set to values other than 0x00.

I tested this both with 1.27 and 1.30, both had the same behavior .

See the attached packet capture: the incoming DelayRequest packet from 192.168.1.2 that has transportSpecific set to 0x00 is responded to while the other one is not. (In this capture, I tried 0x01, but 0x08 failed, too.)

So, I suggest that the customer try and modify his code to set transportSpecific to 0x00 and things should work again.

In the meantime, we should decide whether this is a bug or not. Strictly speaking, we are behaving correctly according to the standard. But that may not be the best response from a customer’s perspective.

We have seen this with ptpdV2- Symptoms of this issue include the following:

- PTP clients wavering off the correct time by many microseconds (one customer is seeing~ 50 microseconds of error).
- Either:
 - 1) The corresponding Delay Response message will have its “Receivetimestamp (nanoseconds)” field set to all 0’s, or
 - 2) There may not be a corresponding Delay Response sent from the PTP Master (delay requests, but no delay responses)

➤ To resolve this issue, customers should either:

- 1) Upgrade to a newer version of PTPD and recompile
 - Refer to the following link for more info: <https://sourceforge.net/p/ptpd/bugs/25/>
- 2) potentially replace the discontinued 1204-12 card (with a 1204-32 card, if this functionality gets changed in a post 5.8.6 software update, preventing it from not responding to values other than 0)

Refer to Salesforce cases such as 11043 for specific examples of this happening.

Q. It seems like the Symmetricom units we have implement the delay request-response functionality whereas the Spectracom does not. At this point I am assuming I have not correctly set something up on the Spectracom units. We could use some guidance here.

A. **Email from Denis Reilly:** We've seen something similar in the past. The Delay Request packets have the transportSpecific field set to **0x08**. Our hardware timestamper is expecting the transportSpecific field to be set to **0x00**.

We had seen this in older versions of ptpv2d, but I thought this was fixed in the latest versions, so I am a bit confused. I see that someone has submitted this as a bug for ptpv2d, which is now closed.

http://sourceforge.net/tracker/index.php?func=detail&aid=3471843&group_id=139814&atid=744632

(Note -appears it is now be <https://sourceforge.net/p/ptpd/bugs/25/>.)

Packets in Wireshark say “disregard delayreq because of wrong SeqNo”

Denis Reilly's initial guess (31 July 13) - Multicast Delay Responses meant for other Clients are being received and PTPd not sure how to handle this condition.

Packets in Wireshark say “Ethernet Frame Check Sequence Incorrect”

Email from Denis after reviewing a packet capture from a PTPd client
Why aren't the Frame Check Sequence issues bad?

First, because these are Delay Requests that are actually generating a response. So our Master doesn't mind whatever is going on.

Second, because these packets have extra trailing 0's at the end. (You can see them by expanding “Ethernet II” on one of those packets, and selecting “Trailer”.) My guess is that Wireshark interprets the last 4 bytes at the end of this trailer as the optional Frame Check Sequence block. But it's not – it's just a bunch of 0's – so the Frame Check calculation fails.

B) Linux Redhat 6.5 (and higher) distribution

Q (from John Abdelsater w/Open Access) ASX has noticed the release notes for Redhat Linux 6.5 (we use the 64-bit version). Apparently, this new version of Redhat “natively supports” PTP. From what I see there's a bundled PTP client as well as hardware timestamp support introduced for the most popular Intel and Broadcom NICs.

What do you know of Timekeeper and support for Redhat Linux 6.5, particularly now that Redhat has started to dabble into PTP themselves?

We are having a technology refresh for our Trading systems... we are intending to stick with Timekeeper but I'm wondering if I need to grab the latest release to maintain support with RHEL 6.5.

A First reply from Dennis Reilly (14 Aug 2014)

I took a bit of time this morning to look into this. It looks like RedHat has included the “Linux PTP project” in 6.5. This is an open-source implementation, like ptpd. But it looks like the Linux PTP project has done a bit more recent work in terms of supporting several hardware timestamping NICs, and also in terms of steering the Linux kernel time.

What this means is that we may find more customers in the future using the Linux PTP project/ptp4l/phc as their open-source implementation of choice instead of ptpd. We probably ought to get familiar with it.

I will check with Cort to see whether there is a Timekeeper version he recommends with RedHat 6.5.

Second reply from Denis Reilly (14 Aug 2014)

I've verified with Cort that the Linux PTP support in RedHat 6.5 isn't really anything “built-in”. What it means is that

that version of RedHat includes those Open-Source packages from the Linux PTP project. (It also probably includes some newer bits in the Kernel, but Tk can work with these, too.) Remember that RedHat is a paid distribution that provides enterprise-level support. By including this in their distribution RedHat will probably support customers who try to use this.

There are no issues with using Timekeeper on RedHat 6.5 or later related to this. You simply use one or the other to process PTP packets and control the kernel time. In fact, according to RedHat's documentation, this isn't even installed by default. So, nothing at all should change.

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/s1-Using_PTP.html

So, if they are currently using a reasonably current version of Timekeeper, they shouldn't have to upgrade just for RedHat 6.5. (But they may want to find there are other improvements to Tk they are interested in.)

C) Timekeeper software from FSM Labs (NTP/PTP sync software for Linux)

- **Note:** For info on Timekeeper software, refer to the "Timekeeper section" in the document: [..\Legacy VelaSyncAndGeoCustAssist.pdf](#)
- **Note:** we no longer offer this FSM software!!

PTP Slave manufacturers/Models

****SolarFlare network adapters**

Location: United Kingdom

Websites

Main: <http://www.solarflare.com/>

Support: <https://support.solarflare.com/>

Tech Support Contact

Solarflare contact – Eddie Thomson – ethomson@solarflare.com

Solarflare manuals/documents:

https://support.solarflare.com/index.php?option=com_cognidox&view=categories&Itemid=11

Solarflare firmware (SFPTPD)

SolarFlare customizes PTPd and calls it **SFPTPD** software

Models/Products <http://www.solarflare.com/Products-Overview-Onload-Performant>

Models begin with “SFN” such as SFN6832F for example

Solarflare 5322 PTP Slave board has high offsets and jitter

refer to Salesforce case 4860

Eric Aversa was having trouble with high offsets and jitter between a SecureSync-PTP master and their PTP slaves. They contacted solarflare and got a software update that fixed this issue.

Frame Check Sequence (FCS) errors in a packet capture

Refer to http://en.wikipedia.org/wiki/Frame_check_sequence

Some Solarflare PTP slaves send longer than usual Delay Request packets which Wireshark may report as Frame Check Sequence errors.

****Exfo PTP slaves**

Not recommended to use TSync-PTP boards with these PTP Slaves, as they apparently require Telecom Profile.

No Delay Responses being sent from 1204-12 card

PTP slave is trying to use Telecom profile (sending multiple TLVs)

Email from Denis Reilly, 13 Mar 2014 I think Exfo is the client that tries to connect with Multiple TLV's in one message. That's explicitly called out as a possibility in the Telecom profile, but not in the main spec.

The Actarus 1204-12 card does not support this, and the Korusys 1204-32 card does.

As far as I know, there are no plans to put that function into Actarus, because Actarus is not sold as being Telecom-profile compatible. I've copied Laurent and Michel in to confirm.

Specific network/PTP switch/Boundary Clock info

**Layer 2 / Layer 3

Q. Does the SecureSync support one-step, two-step, layer 2 multicast, layer 3 multicast, peer-to-peer, layer 3 unicast all combinations? Can I configure any combination if I need?

A. Reply from Denis Reilly 6 May 13) all the above, in any combination that makes sense.

**PTP network switch recommendations

Q. Can you tell me which network switches with PTP you recommend??

A Reply from Denis Reilly (7 May 13) It depends on how good their accuracy needs to be.

As good as NTP? The switch probably doesn't matter. Microseconds? They probably want a switch with a boundary or transparent clock in them, like the Cisco Nexus 3000's. Under 1 microsecond? Now they are into the low-latency switches, like Arista.

**Model 7705 router

Email from Denis Reilly (16 Sept 2013) I am having trouble finding information on this router, but I did find this test report:

http://www.ixiacom.com/pdfs/library/case_studies/ALU-1588v2-Test.pdf

which makes the claim that the router can operate as a Boundary Clock or Transparent Clock.

Response from customer - Almost all the routers that we use are 7705 (SAR8, SARF and SARM), some of them are 7750-SRc12, 7750-SR7 and 7750-SR12.

**Arista switches/boundary clocks

Arista Networks Tech Support: support@aristanetworks.com

Email from Sam Otto (18 Jul 2013) Regarding a switch in the PTP lab: The Arista switch is now configured and working with both NTP and PTP.

Please review the updated wiki and feel free to send me your recommendations, you may update as you see fit.

http://10.30.1.20/DevWiki/index.php?title=Rochester_Networking_Test_Bed#PTP_Interface_Configurations

*****NOTE:** Something to be aware of because our current PTP Modules are 10/100 their respective Ethernet ports on the switch require the following command, "**speed forced 100full**". This is how Nick from Arista hacked the switch to work with our product.

Arista Boundary clock

- Refer to <http://www.arista.com/docs/Manuals/ConfigGuide.pdf> (Chapter 5.3.2 provides info on PTP)

8725 Arista switch / Myricom link flap issue

(this info provided to us from Joe Laiback with Schoenfeld tools)

From: Stuart Livings, Arista Technical Solutions Engineer

Hi Joe,

We've spent some time investigating this further here at Arista and we've got some more thoughts on this issue.

The 7148SX is different from the 7150S in that the PHYs on the 7148SX are tuned to give the best possible signal at the remote end of the cable, even at the cost of signal level. The 7150S is tuned to give a particular quality and signal level at the local end of the cable.

Our current speculation is that this tuning of the 7148SX and the tuning of the Myricom interface are mutually exclusive. We believe the first test suite to run in the lab environment should be to disable this tuning characteristic of the 7148SX and retest without the Myricom

driver tweak.

The command in question is set per physical interface and takes the form 'tx-preemphasis standard'. When entered, the 7148SX will return the parameters as above. This command will have no effect on the 7150S.

As part of this test we should prove and counter-prove each test and ensure that we understand the effect of each individual setting. We should make sure each test is documented with all of the test data requested in the earlier email.

Please let us know if there is anything further we can be doing to assist you in the interim.

****Hirschmann switch**

Q. How do you compare the Arista low latency switch to a real PTP switch similar to the Hirschmann? <http://www.e-catalog.beldensolutions.com/link/57078-24455-49846-49997-82828-173144-173174/en/MAR1040-4C4C4C4C9999SM9HPHH07.0./0>

A **Reply from Sam Otto (7 May 13)** I have not heard of the Hirschmann switch until now, thank you for the link. I know that Arista has performed extensive amount of time testing their switch's with various PTP Master and Slave devices. For example, we worked with during the PTP Plug Fest last fall in San Francisco and they are currently performing additional testing with our SecureSyncs.

****Nexus switch**

Nexus 3000 series

(email from Denis Reilly)

Here is a Cisco configuration PTP link for the Nexus 3000 series.

http://www.cisco.com/en/US/docs/switches/datacenter/nexus3000/sw/system_mgmt/503_U3_1/b_Cisco_n3k_System_Mgmt_Config_503_U3_1_chapter_0101.pdf

Simple connectivity diag attached as well

Here are the commands configured on the Nexus 3548 switch which doesn't show the default parameters

```
ukld400-004-n35# sh runn | i ptp
feature ptp
ptp source 10.210.114.11
```

```
Interface Eth1/41
description ** link to ukld400-001-c49 vlan873 ptp **
ptp
ptp vlan 873
ukld400-004-n35#
```

Some show commands output

```
ukld400-004-n35# show ptp brief
```

PTP port status

```
-----
Port      State
-----
```

```
Eth1/41   Master
ukld400-004-n35#
```

```
ukld400-004-n35# show ptp clock
```


PTP Device Type: Boundary clock
Clock Identity : 60:73:5c:ff:fe:62:3f:7c
Clock Domain: 0
Number of PTP ports: 1
Priority1 : 255
Priority2 : 255
Clock Quality:
 Class : 248
 Accuracy : 254
 Offset (log variance) : 65535
Offset From Master : 0
Mean Path Delay : 0
Steps removed : 0
Local clock time:Thu May 2 11:38:22 2013
ukld400-004-n35#

ukld400-004-n35# show ptp parent

PTP PARENT PROPERTIES

Parent Clock:
Parent Clock Identity: 60:73:5c:ff:fe:62:3f:7c
Parent Port Number: 0
Observed Parent Offset (log variance): N/A
Observed Parent Clock Phase Change Rate: N/A

Grandmaster Clock:
Grandmaster Clock Identity: 60:73:5c:ff:fe:62:3f:7c
Grandmaster Clock Quality:
 Class: 248
 Accuracy: 254
 Offset (log variance): 65535
 Priority1: 255
 Priority2: 255
ukld400-004-n35#

ukld400-004-n35# show ptp port int e1/41
PTP Port Dataset: Eth1/41
Port identity: clock identity: 60:73:5c:ff:fe:62:3f:7c
Port identity: port number: 40
PTP version: 2
Port state: Master
VLAN info: 873
Delay request interval(log mean): 0
Announce receipt time out: 3
Peer mean path delay: 0
Announce interval(log mean): 1
Sync interval(log mean): -2
Delay Mechanism: End to End
ukld400-004-n35#

ukld400-004-n35# show ptp clocks foreign-masters-record

P1=Priority1, P2=Priority2, C=Class, A=Accuracy,
OSLV=Offset-Scaled-Log-Variance, SR=Steps-Removed
GM=Is grandmaster

Interface	Clock-ID	P1	P2	C	A	OSLV	SR
-----------	----------	----	----	---	---	------	----

ukld400-004-n35#

5 millisecond bug in Nexus 3000 code (May 2013)

email from Paul Panzl [<mailto:ppanzl@cisco.com>] to Sam Otto (may 2013)

do you have a cisco.com userid? if not do you have an FTP server where I can drop code. Problem is there is still one outstanding bug in nexus 3000 PTP code, even in the daily engineering builds I'm getting.

the bug causes a 5 millisecond correction on downstream devices when the nexus 3000 is under load. data plane + control plane traffic.

Plus another feature of the nexus 3000 requires (has to do with our oscillator and timestamp counter implementation - very sore point for me)

GM to nexus 3000 and nexus 3000 to nexus 3000 links require sync -3, yes ouch -3. basically any upstream device connected to a nexus 3000 must have a sync int of -3 on the ports facing the nexus 3000.

my upstream nexus 3548 to nexus 3000 configs. you do not need port channels or trunks to use ptp, this is just the current test config for me.

```
interface Ethernet1/30
description to N3K-7
ptp
ptp vlan 401
ptp delay-request minimum interval -1
ptp sync interval -3
switchport mode trunk
switchport trunk native vlan 401
switchport trunk allowed vlan 401
channel-group 13 mode active
no shutdown
```

and the corresponding port on my nexus 3000

```
interface Ethernet1/24
description N3548-1 Port 1/30
ptp
ptp vlan 401
switchport mode trunk
switchport trunk native vlan 401
switchport trunk allowed vlan 401
duplex full
channel-group 13 mode active
no shutdown
```

to enable ptp on the nexus 3000s you need

feature ptp

```
ptp source 169.124.196.215 (whichever IP fits your network needs. PTP frames will be sourced with this IP address)
ptp priority1 128
ptp priority2 128
```

nexus 3000s config for server facing ports

```
interface Ethernet1/1
```



```
description to ptp-s12 - DO NOT SHUT THIS PORT
ptp
ptp vlan 401
ptp sync interval 0
switchport access vlan 401
no shutdown
```

```
interface Ethernet1/2
description to ptp-s7
ptp
ptp vlan 401
ptp sync interval 0
switchport access vlan 401
no shutdown
```

```
interface Ethernet1/3
description to ptp-s8
ptp
ptp vlan 401
ptp sync interval 0
switchport access vlan 401
speed 1000
duplex full
no negotiate auto
no shutdown
```

```
interface Ethernet1/4
description to ptp-s13
ptp
ptp vlan 401
ptp sync interval 0
switchport access vlan 401
speed 1000
duplex full
no negotiate auto
no shutdown
```

****Alcatel 7705 Router**

Email Dave Lorah sent to kcrow@ask4cii.com (30 July 2013)

I did a little hunting this morning and found an online manual for the Alcatel 7705 Router.

In the PTP section of the manual I read that this router uses a IPv4 Unicast PTP message and according to this 2009 manual it uses a 1 step only mode. This may have been changed in newer versions of the product but I cannot tell for sure. So try setting the One Step Mode to ENABLED first.

So it would make sense to try setting the SecureSync up for a Unicast PTP. I have attached a nice app note that covers the setup of Unicast in the SecureSync.

Monitoring PTP performance/operation

Question: I would like to ask you about PTP. We have enabled both PTP unicast and multicast and want to monitor the status of PTP (such as traffic volume, a number of PTP clients, stability of PTP, and so on). How can we do that?

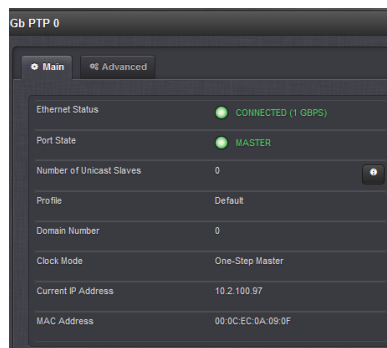
- is there a way to check it via snmp polling from such tools as OpenNMS or Cacti?
- any CLI command to check it?
- anything in GUI that is available for us to check the status of PTP? I know you have this page shown as below, but I am looking for more than that.

Various methods to monitor PTP performance/operation (some are free/ other have costs associated)

A) Free monitoring capabilities

1. The browser “Status” page for the applicable PTP Option Cards

- For example- from the 1204-32 Gb PTP card



2. Use a packet capture tool (wireshark or tcpdump, for examples) to review the PTP Announce messages sent from the PTP Master

3. Via SNMP using the newer PTP Mib file for 1204-32 card

- New SNMP MIB Added in update version 5.6.0 for the 1204-32 card
- As of at least v5.6.0, this is a read-only file for performing just “Gets” (no Sets or Traps available)
- Can read values directly from the 1204-32 card, such as configs (network, and PTP settings) along with port state, PTP Clock Class, Clock **Accuracy**.

4. “OnTime Networks” program called “PTPBrower” (apparently, freeware as of at least May, 2017)

- Freeware program
- Snoops PTP Announce messages
- <http://ontimenet.com/products-system-tools-ptpbrowser/>
- C:/Program Files (x86)/OnTime

B) Purchased PTP monitoring software/capabilities

1) Our SWIFT software (once available)

2) Meinberg software (from our competitor so we don't want to recommend)

Email from Denis- Meinberg has good PTP monitoring software for sale, but I wouldn't recommend them. ☹

3) FSMLabs Timekeeper software and the associated FINRA statistics package.

4) Cacti and OpenNMS network management programa

Email from Denis- Cacti and OpenNMS are "network management systems" that will query devices on your network and present the data all in one place. But they're meant to answer questions like "how much traffic is going through that router" and "Is my web server being attacked by a DDOS". They may have NTP monitoring support, since lots of people run NTP and it's been around for so long, but I don't think they will have PTP support.

11) IXXAT "1588 PTP Manager" program (Tool for monitoring and configuration of IEEE 1588-2008 PTP networks)

- <https://www.ixxat.com/products/products-industrial/time-synchronization/ieee-1588-ntp-manager>
- From IXXAT/HMS industrial Networks, inc
- As of at least May, 2017, don't know anything more than what's on the website linked above
- Free demo software available at link above

The PTP Manager allows monitoring, configuration and testing of an IEEE 1588-2008 network. The configuration of all detected PTP clocks can be simply viewed and modified by using the PTP manager. It supports all features of Ordinary, Boundary and Transparent Clocks, including fault logs and the Unicast Master Table. Complex configurations are not necessary, because only the desired network card of the Host PC has to be selected. Automatic display of network hierarchy

The PTP clocks within a network are automatically detected and listed by the PTP Manager. In addition, the PTP Manager recognizes the master/slave relationship and displays this in tree view.

Presentation of synchronization data as graph

For convenient monitoring of the synchronization between master and slave, the PTP Manager can display the "One Way Delay", "Offset from Master" and "Observed drift" as graphs over the time. The measured values can be exported as CSV file. The graph-view can be set either to auto zoom or to manual zoom.

Schweitzer Engineering Laboratories (SEL) equipment (Orolia Competitor)

<https://selinc.com/>

- Schweitzer Engineering Laboratories (SEL) is apparently a direct competitor of Orolia
- They apparently make satellite-based NTP/PTP Servers and IRIG distribution units that are used to sync their other SCADA network type devices, Protection Relays, Real Time Automation Controllers (RTAC), display clocks, etc.
- All their products appear to have “SEL-“ Model Numbers
 - Refer to sites such as: <https://cms-cdn.selinc.com/assets/Literature/Publications/Product%20Catalogs/Catalog%20Sections/SEL%20Precise%20Time.pdf?v=20210112-191149>

“Mutual customer” desire for our SecureSync to sync their other SEL devices (via NTP)

- Refer to Salesforce Case 262248

I am working on a project where we are using an Orolia to broadcast time using NTP over a Ciena Network to different SEL Schweitzer RTUs and protection relays. I have programmed the Orolia according to the information provided in the User Manual. However, we still don't have time sync to our devices. Is there any documentation or recommendation on how to set up the Orolia to serve as an NTP server for this device?