TRUETIME

Model 560-5151
NETWORK TIME SERVER
IRIG-B INPUT

SECTION ONE

1. FUNCTIONAL DESCRIPTION

1.1 PURPOSE OF EQUIPMENT

The TrueTime 560-5151 Network Time Server (NTS) card provides Internet Protocol (IP) network time synchronization over ethernet connected networks, via the Network Time Protocol developed by Dr. David Mills at the University of Delaware. In providing this synchronization, the NTS operates as a “server”. The NTS currently supports version 3.0 of the NTP, RFC 1305 as well as the Simple Network Time Protocol (SNTP), RFC1361. In addition, the NTS will respond to time protocol requests, RFC868. Refer to Appendices A and B for details regarding these protocols. The user interface and ethernet connections are provided via an I/O card installed in the rear slot directly behind the NTS card.

The IRIG-B AM or DC time synchronization source for the NTS card is one of the timing signals distributed via INPUT 1 through INPUT 8 on the Model 56000 backplane. The card is configured at installation by DIP switches to select the signal that will be the Primary and Secondary input.

The Primary and Secondary inputs are monitored for activity. The activity on both inputs is compared to the Delay switch time-out setting (user settable DIP switch) which operates as a watch dog timer. If activity on either the Primary or the Secondary inputs exceeds the delay switch time-out setting, that input is considered bad. NOTE: An input may be considered bad if the minimum input voltage level is not met.

The NTS card can operate without a Fault Monitor CPU card installed in the system. In a system without CPU card, the NTS card will automatically switch to the Secondary input source when the following conditions are met:

1. The Secondary input is good (activity time-out not exceeded).
2. The Primary input is bad (activity time-out exceeded).

The card will not switch to the Secondary input source if it has been detected bad. The card will switch back to the Primary input signal source only after the Primary input has been qualified good (good for 1 to 2 minutes). This feature restores the card to normal operation automatically.

When a CPU card is installed in the system, the NTS card is monitored and can also be controlled by the CPU card. In addition to the NTS on-card automatic Primary to Secondary switch-over, the CPU card also provides Primary to Secondary input switching when the CPU detects a Primary Status Input fault on any card. The CPU control provides what is called a “Bank Switch” meaning that all cards in the system will switch from the Primary to the Secondary signal source <u>and will stay on the Secondary input</u> until the user commands a switch to Primary via the CPU card. The “Bank Switch” allows timing signal inputs on all cards installed in the system to come from one source. The CPU also has the ability (under user control) to force the use of either the Primary or Secondary inputs.

1.2 FAULT LINE TRANSCEIVER FUNCTION

This is a serial half-duplex signaling operation between the 560-5151 card and the Fault Monitor CPU via the active-low FAULT signal line. The Fault Monitor CPU sends control and switching information to the NTS assembly serially. The NTS assembly provides status information serially to the Fault Monitor CPU.

1.3 PRIMARY/ SECONDARY SIGNAL SELECT FUNCTIONS

If the NTS is mapped to the Primary input signal via the Fault Monitor CPU and it detects inactivity on this input, the card will automatically or, under Fault Monitor CPU control, switch to the Secondary input signal. If the NTS card is operating in a system with a Fault Monitor CPU card and the NTS card has switched to the Secondary input source, the NTS card will NOT switch back to the Primary input unless commanded by the user via the Fault Monitor CPU.

1.4 FLYWHEELING PERFORMANCE

During a synchronization input outage, following initial synchronization of the NTS-560 to the input time synchronization source, the timing outputs from the NTS-560 will diverge from the input at the rate of approximately 2 parts in 10^6, if the ambient temperature is maintained within ±3°C.

1.5 PHYSICAL SPECIFICATIONS

Dimensions:	0.8"w X 3.94"h X 8.66"d (2 cm X 10 cm X 22 cm)
Weight:	Approximately ½ pound (¼ kg)

1.6 ENVIRONMENTAL SPECIFICATIONS

Operating Temp:	0° to +50°C
Storage Temp:	-40° to +85°C
Humidity:	Up to 95% max. relative, non-condensing
Cooling Mode:	Convection
Altitude:	10,000 ft. ASL

1.7 POWER REQUIREMENTS

Voltage:	18-72 Vdc
Power:	6 W

1.8 FUNCTIONAL SPECIFICATIONS

1.8.1 TIME SYNCHRONIZATION INPUT

1.8.1.1 INPUT 1 THROUGH 8 (ANALOG MODE)

Analog Input Level:	2-5 Vpp
Impedance:	>20k ohms
Frequency:	1 kHz
Signal Type:	IRIG-B AM

1.8.1.2 INPUT 1 THROUGH 8 (DIGITAL MODE)

Logic Input Levels:	
Low:	-5V <Vin < 1.2V
High:	1.8V < Vin < 5.0V
Impedance:	>20k ohms
Frequency:	1 kHz
Signal Type:	IRIG-B DC

1.8.2 IRIG-B AM ANALOG OUTPUT (OPTION)

Quantity:	2 (via Timing Lines IN3/IN4)
Signal Type:	IRIG-B 122 AM
Amplitude:	5 Vpp High, 1.5 Vpp Low, with no load
Output Impedance:	600 Ohms
Accuracy:	±10 us relative to input

1.8.3 SYNCHRONIZATION PERFORMANCE SPECIFICATIONS

See SECTION FIVE.

1.8.4 CARD COMPATIBILITY

Location:	Slot 1-17 with compatible I/O card in rear slot.
Compatibility:	See Card Compatibility Matrix.

1.9 NETWORK TIME PROTOCOL SPECIFICATIONS

1.9.1 PROTOCOLS

The NTS-560 will respond to time synchronization requests from hosts using these User Datagram Protocol/Internet Protocols (UDP/IP):

NTP Ver. 3.0	UDP Port 123	RFC1305**
SNTP	UDP Port 123	RFC1361
TIME	UDP Port 37	RFC868

Refer to Appendices A and B for detailed information regarding these protocols as implemented by the NTS-560.

** The NTS-560 does not implement the “authenticator field” of the NTP packet as described in Appendix C of RFC1305.

1.9.2 SYNCHRONIZATION SPECIFICATIONS

The NTS-560 hardware is designed specifically to implement the NTP server function. As such it was designed to operate with the TrueTime Mark III real time operating system to minimize the unknown latencies in timestamping the received and transmitted NTP packets. The timestamp accuracy specifications are:

NTP Packet Received Timestamp Accuracy:
±10 μs, relative to synchronization source
NTP Packet Transmitted Timestamp Accuracy:
±10 μs, relative to synchronization source

At these levels of accuracy, the realizable NTP synchronization accuracy of any client host is determined by the quality of the synchronization source and the repeatability of the network and client delays, *not* by the NTS-560 timestamp uncertainty.

1.10 INTERFACE SPECIFICATIONS

1.10.1 ETHERNET INTERFACE

Frame Format:
DIX Ethernet (Ethernet II) or IEEE 802.3 with 802.2 headers
Available Signals (via rear I/O card):

Signal
GND
CI+
DO+
DI+
CI-
DO-
DI-

1.10.2 USER SERIAL I/O INTERFACE

Provides time/day of year through milliseconds, in ASCII characters, output once per second or on request. Also special functions as listed in SECTION THREE.

Serial port parameters (factory-set):

Baud Rate:	300, 600, 1200, 2400, 4800, and 9600 (default)
Data Bits:	7 (default) or 8
Parity:	Even (default), odd or none
Stop Bits:	1 (default) or 2

Use SW1-3 & 4 to select between RS-232 and RS-422 operation:

SW1-3	SW1-4	MODE
ON	OFF	RS-422
OFF	ON	RS-232
ON	ON	NONE
OFF	OFF	NONE

Available signals (via rear I/O card):

RXDIN: RS-232 IN
TXDOUT: RS-232 OUT
RIN+: +RS-422 Input
RIN-: -RS-422 Input
TOUT+: +RS-422 Output
TOUT-: -RS-422 Output

SECTION TWO

2. INSTALLATION AND OPERATION

2.1 HOT SWAPPING

All cards, input cables and output cables are hot swappable. It is not necessary to remove chassis power during insertion or removal. Hot swapping and reference-source changes are abrupt, the effects difficult to characterize; however, the system is designed to protect against permanent effects and minimize temporary effects of these events.

Typically, adjacent-card hot swapping has a negligible effect on the Analog output card. The effect of redundant power supply switch-over is also negligible.

2.2 REMOVAL AND INSTALLATION

CAUTION: Individual components on this card are sensitive to static discharge. Use proper static discharge procedures during removal and installation.

Refer to CARD COMPATIBILITY section prior to installing new card.

To remove card, loosen the captive retaining hardware at the top and bottom of the assembly, then firmly pull on the handle (or on any connector on rear panel adapter cards) at the bottom of the card. Slide the card free of the frame. Refer to the SETUP section for any required switch settings; or, set them identically to the card being replaced. Reinstall the card in the frame by fitting it into the card guides at the top and bottom of the frame and sliding it in slowly, avoiding contact between bottom side of card and adjacent card front panel, until it mates with the connector. Seat card firmly to avoid contact bounce. Secure the retaining screws at the top and bottom of the card assembly.

2.3 SETUP

The setup of the NTS card involves selection of the following DIP switches:

1. 560-5151 Required settings (SW7)
2. Primary input signal switch (SW5)
3. Secondary input signal switch (SW6)
4. Primary input enable switch (SW2)
5. Secondary input enable switch (SW3)
6. Delay switch (activity time-out) (SW4)
7. Analog/Digital timing input switch (SW4)
8. User Port RS-232/422 Switch (SW1)
9. RS-422 Terminator Switch (SW7)
10. GREEN Status Enable Switch (SW1)

2.3.1 REQUIRED SWITCH SETTINGS (SW7-4)

SW7-1, SW7-2, and SW7-4 must be OFF.

2.3.2 PRIMARY TIMING INPUT SOURCE SWITCH (SW5)

Set one SW5 switch to the ON position. The SW5 switch number (1 through 8) corresponds to INPUT 1 through INPUT 8 signals that are distributed on the Model 56000 backplane.

2.3.3 SECONDARY TIMING INPUT SOURCE SWITCH (SW6)

Set one SW6 switch to the ON position. The SW6 switch number (1 through 8) corresponds to INPUT 1 through INPUT 8 signals that are distributed on the Model 56000 backplane.

2.3.4 PRIMARY TIMING INPUT ENABLE SWITCH (SW2)

This switch MUST be set to a binary representation of the Primary input (SW5) setting. This switch is read by the Fault Monitor CPU which can provide status information to the user.

PRIMARY INPUT	**SW2-1**	**SW2-2**	**SW2-3**	**SW2-4**
INHIBIT	OFF	OFF	OFF	OFF
INPUT 1	ON	OFF	OFF	OFF
INPUT 2	OFF	ON	OFF	OFF
INPUT 3	ON	ON	OFF	OFF
INPUT 4	OFF	OFF	ON	OFF
INPUT 5	ON	OFF	ON	OFF
INPUT 6	OFF	ON	ON	OFF
INPUT 7	ON	ON	ON	OFF
INPUT 8	OFF	OFF	OFF	ON

This switch is also used to disable the Primary input. If SW2 switches 1 through 4 are OFF, the card will inhibit operation and fault reporting of the Primary input. Use this setting if the Primary input is not used.

2.3.5 SECONDARY INPUT ENABLE SWITCH (SW3)

This switch MUST be set to a binary representation of the Secondary input (SW6) setting. This switch is read by the Fault Monitor CPU, which can provide status information to the user.

SECONDARY INPUT	**SW3-1**	**SW3-2**	**SW3-3**	**SW3-4**
INHIBIT	OFF	OFF	OFF	OFF
INPUT 1	ON	OFF	OFF	OFF
INPUT 2	OFF	ON	OFF	OFF
INPUT 3	ON	ON	OFF	OFF
INPUT 4	OFF	OFF	ON	OFF
INPUT 5	ON	OFF	ON	OFF
INPUT 6	OFF	ON	ON	OFF
INPUT 7	ON	ON	ON	OFF
INPUT 8	OFF	OFF	OFF	ON

This switch is also used to disable the Secondary input. If SW3 switches 1 through 4 are OFF, the card will inhibit operation and fault reporting of the Secondary input. Use this setting if the Secondary input is not used.

2.3.6 DELAY SWITCH (SW4 Switches 1, 2, & 3)

SW4 switches 1 through 3 are used to set the input activity time-out delay. The user should set the delay for a time-out value that is the closest to, but longer than, the period of the input signal. This will provide fault detection in the shortest amount of time (Primary to Secondary switch-over time is minimized).

Example Setting: If the input signal is 1 kHz (1 millisecond period), the appropriate setting would be SW4-1 ON, SW4-2 OFF, SW4-3 OFF --(2.048 millisecond time-out).

DELAY (TIME-OUT)	SW4-1	SW4-2	SW4-3
204.8 microseconds	OFF	OFF	OFF
2.048 milliseconds	ON	OFF	OFF
20.48 milliseconds	OFF	ON	OFF
204.8 milliseconds	ON	ON	OFF
2.048 seconds	OFF	OFF	ON
20.48 seconds	ON	OFF	ON
122.88 seconds	OFF	ON	ON
Infinite	ON	ON	ON

If infinite delay has been selected, Primary and Secondary input fault detection is disabled.

2.3.7 ANALOG/DIGITAL TIMING INPUT SWITCH (SW4-4)

SW4 switch 4 is used to set the NTS for compatibility with an IRIG-B AM or IRIG-B DC time synchronization input:

SW4-4	INPUT COMPATIBILITY
OFF	IRIG-B DC
ON	IRIG-B AM

2.3.8 USER PORT RS-232 / RS-422 SWITCH

Use SW1-3 & 4 to select between RS-232 and RS-422 operation:

SW1-3	SW1-4	MODE
ON	OFF	RS-422
OFF	ON	RS-232
ON	ON	NONE
OFF	OFF	NONE

2.3.9 USER PORT RS-422 TERMINATOR SWITCH (SW7-3)

SW7 switch 3 enables/disables the RS-422 100 ohm termination resistor. If the switch is ON, the terminator is enabled. If it is OFF, the terminator is disabled. The switch should be ON if the

NTS is the last RS-422 device on the RS-422 line. Otherwise, the switch should be OFF.

SW7-3	TERMINATION
OFF	NONE
ON	100 OHMS

2.3.10 GREEN STATUS ENABLE SWITCH (SW1-2)

SW1 switch 2 enables/disables the GREEN condition of the NTS LED during the fully-operation non-fault state of the NTS. This switch has no effect for conditions where the LED is ORANGE.

SW1-2	GREEN
OFF	DISABLED
ON	ENABLED

2.4 STATUS INDICATIONS

All indicators activate briefly following hot-insertion or power-up. The following paragraphs describe operation during steady-state conditions.

2.4.1 P/S STATUS INDICATOR

The P/S indicator provides a visual indication of Primary and Secondary signal loss. If the Primary and Secondary inputs are both lost, the LED will blink at a once per second rate (approx.). A solid ON LED indicates a local power supply failure.

2.4.2 NTS STATUS INDICATOR

The NTS indicator provides a visual indication NTS status:

Blinking Red	Logic Fault
Solid Red:	No time synchronization present
Solid Orange:	Time synchronization present, not locked
Green/Blinking Green:	Fully Operational State

2.4.3 INITIALIZATION FAULT INDICATORS

These are on-card fault indicators which are not externally visible; although, they can be seen by installing the card next to an empty slot. It indicates a failure of the card to initialize properly during power-up. Occasionally, this fault is caused by a temporary condition related to the cycling of power and can be cleared by a power or hot swap cycle. If this is unsuccessful, the card is defective.

2.4.4 DETAILED STATUS VIA CPU

The Fault Monitor CPU has access to detailed 560-5203-1 card status. When the CPU card provides the verbose mode serial report, fault status is available in a 2-byte format, with each binary nibble displayed as a hexadecimal (HEX) character.

The Verbose report displays the Fault status. In this context, a reported fault indicates a problem. The Machine report, when used, reports the current status (settings) of the switches and faults in hexadecimal characters. Together, they pinpoint problems and help the technician view the switch settings on the cards.

2.4.5 VERBOSE REPORTS

The following is an example of a Fault Monitor CPU report in Verbose mode:

TrueTime 56000 Site 01
Automatic Reports **Enabled**
Periodic Reports **Disabled**
Primary Inputs Selected REFA No REFB No REFC Off PRI OK SEC OK TER Off

1. Undefined		OK	Undefined	OK
2. Undefined		OK	Undefined	OK
3. 5151	**LOCAL OSC FAULT**	**0402**	**Undefined**	**OK**
4. Undefined		OK	Undefined	OK

The above sample tells you that:
Automatic reports are enabled and Periodic reports are disabled.
Primary inputs REF A and REF B are not bussing Aux. Ref. REF C is off. Primary and Secondary status inputs OK, Tertiary is OFF.

Numbers 1-4 are slots (not all slots are shown in the example). Slots 1,2,and 4 are undefined (empty) and functional (OK).

Slot 3 is read as follows:
5151 is the abbreviation of the 560-5151 card. The fault reading is 0402.

2.4.6 MACHINE REPORTS

The Fault Monitor CPU has another serial output mode called machine report mode. This mode is usually used with a computer program to interrogate the 56000 system status.
The machine report mode displays hexadecimal (HEX) characters like the verbose mode report.

The following is an example of a Fault Monitor CPU report in Machine Mode:

TrueTime 56000 Site 01
AR1
PR10
P A1 B1 Co P1 S1 To
01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03 00 50 04 02 0251 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
(card slots 05 through 14 HEX not shown)

Example from card slot 3 above:

03 0050 04 02 02 51 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Fault Byte 1 (F1)
Fault Byte 0 (F0)
SW1 Switch Status (S1)
SW2 Switch Status (S0)

Slot 3 shows that the Fault status is 0402 (F1, F0). The Status report read-out is 0251(S1,S0).

2.4.7 REPORT CONVERSIONS

This section deals with how to read and convert the Fault and Status read-outs using various tables and binary conversions. To decipher a Fault Status report, use Fig. A.
For Status reports (S1, S0) use Fig. B.

Fig. A

Spare	Spare	Spare	Spare	Primary Source	Sec.Input Inactive*	Pri.Input Inactive*	PowerCycled	Spare	Spare	Spare	Spare	Spare	Spare	NTS LED=Orange*	NTS LED=Red*
8	**4**	**2**	**1**	**8**	**4**	**2**	**1**	**8**	**4**	**2**	**1**	**8**	**4**	**2**	**1**
2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
0	*0*	*0*	*0*	*0*	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*0*

Upper Byte High Nibble **0** | Upper Byte Low Nibble **4** | Lower Byte High Nibble **0** | Lower Byte Low Nibble **2**

Fault Status F1 Report

Fault Status F0 Report

Key:

Above each 8,4,2,1 is the corresponding fault for that bit. For instance, above the 8 bit in the Upper byte/Low nibble reads Rub. Lockmon, which is the fault .

* = Latched fault bit. Reset via Fault Monitor CPU.

Shaded area

Informational only. The upper row: Bit value hex weights (8,4,2,1) The Lower row corresponds to the hex weight above. For instance, a 7 in a readout equals 111 in binary and 4+2+1 in hex weight.

Each section of 8,4,2,1 is a nibble of either an Upper or Lower byte and separated for easy recognition. Each nibble = 4 bits and each byte = 8 bits. "04" is the F1 report, "02" the F0 report.

Non-shaded area

This area is used according with the report read-out after a report is converted to binary. The 0407 is an example from a report.

Always read the report from Upper (High) byte to Lower (Low) Byte.

Status (S1, S0) Conversion Table **FIG. B**

STATUS REG 0	Bit	Bit Value	Switch	
Low	0	1	Pri. Input Enable SW2-1 ON	
Nibble	1	2	Pri. Input Enable SW2-2 ON	1
Low	2	4	Pri. Input Enable SW2-3 ON	
Byte	3	8	Pri. Input Enable SW2-4 ON	
High	4	1	Sec. Input Enable SW3-1 ON	
Nibble	5	2	Sec. Input Enable SW3-2 ON	5
Low	6	4	Sec. Input Enable SW3-3 ON	
Byte	7	8	Sec. Input Enable SW3-4 ON	
STATUS REG 1				
Low	0	1	NTS Locked	
Nibble	1	2	Green Enable SW1-2 ON	2
High	2	4	Always 0	
Byte	3	8	Always 0	
High	4	1	Delay SW4-1 ON	
Nibble	5	2	Delay SW4-2 ON	
High	6	4	Delay SW4-3 ON	0
Byte	7	8	Analog SW4-4 ON	

BINARY CONVERSION TABLE

Decimal	Displayed in report as	Binary
0	0	0
1	1	1

2	2	10
3	3	11
4	4	100
5	5	101
6	6	110
7	7	111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Binary:
1 = Fault/Switch On
0 = No Fault/Switch Off

Use the Binary Conversion table to convert a read-out from the monitor to binary. For instance, if the report read-out was 3C15, this would be:

11\1100\1\101 in binary.

USING THE FAULT STATUS REPORT (F0, F1)

The hex weight (fault importance) has been assigned 8, 4, 2, 1. Beneath each number is the corresponding fault. Use Fig. A.. The report example read 0402. The 0 is high byte/high nibble, the 4, high byte/low nibble, the 0, low byte/high nibble and 2, low byte/low nibble. Each nibble falls under a section on Fig. A, high to low or left to right.

Look at Fig. A. Below this is a sample read-out. This read-out would appear on the monitor when a Verbose report is requested. In the example, there are no faults in the upper byte/high nibble or in the lower byte/high nibble because both are zero (0). In the upper byte/low nibble, a 4 is reported. Looking directly above this, a 4 bit is easily spotted. The fault is Sec. Input Inactive. However, In the lower byte/low nibble a 2 is reported. This indicates that the NTS LED is orange.

Note that the hex weight assigned totals to 2. If the 2 had been a 6, in binary this is 110. Reading from low bit to high bit, the 1's (i.e., faults) fall under hex weight 4 and 2, which equals a hex weight of 6. Of course, glancing at the lower byte/low nibble, you can quickly see (without converting to binary) that under 4 and 2 (i.e., 6) are NTS LED = Orange and Spare.

Each of the four nibbles is grouped by category for easy visual identification of an offending fault. Each nibble has 15 possible fault combinations. All faults are asserted as a logic 1. The faults are latched on the Oscillator card and must be cleared by the 560-5179-1 Fault Monitor CPU “CL” command

USING THE STATUS REPORT (S1, S0)

The method used for reading the Fault report is the same when reading the Status report. Refer to Fig. B.

Using the read-out, 0251, but because the table is different, the 0 is located at the bottom (high byte). The rest of the numbers follow upward towards the low byte (Status 0). In this case, the 2 falls in the low nibble\lhigh byte section of Status 1. The 5 falls in the high nibble\low byte section of Status 0. Since 5 is not listed, we must convert it to binary, or 101.

1 = Active, a 0 = Not active.

Since we have two 1's , reading from high nibble to low byte (in the Low Byte, Status 0) the current items are active (input from bus IN5):

Sec. Input Enable SW3-1 ON	1
Sec. Input Enable SW3-2	0
Sec. Input Enable SW3-3 ON	1

The 1 is located in the low nibble\low byte section of Status Reg 0. This indicates that Pri. Input Enable SW2-1 ON is active (input from bus IN1).

QUICK REFERENCE SHEET FOR READING FAULT AND STATUS REPORTS

1. Run a report. This is a portion of a sample Machine report.

TrueTime 56000 Site 01
AR1
PR10
P A1 B1 Co P1 S1 To
01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03 00 50 04 02 0251 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
(card slots 05 through 14 HEX not shown)

0507 is the Fault Status read-out
B051 is the Status read-out report

03 0050 04 02 02 51 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Fault Byte 1 (F1)
Fault Byte 0 (F0)
SW1 Switch Status (S1)
SW2 Switch Status (S0)

Slot 3 shows that the Fault status is 0402 (F1, F0). The Status report read-out is 0251(S1,S0).

02 = Fault Status 1 (F1) report
07 = Fault Status 0 (F0) report
02 = Status 1 (S1) report
51 = Status 0 (S0) report

What's in a number?

0 4 0 7

High Byte High Nibble
High Byte Low Nibble
Low Byte High Nibble
Low Byte Low Nibble

2. When required, convert Decimal to Binary using the Binary Conversion Table.

BINARY CONVERSION TABLE

Decimal	Displayed in report as	Binary
0	0	0
1	1	1
2	2	10
3	3	11
4	4	100
5	5	101
6	6	110
7	7	111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Binary:
1 = Fault/On/Active/Yin
0 = No Fault/Off/Not Active/Yang

SECTION THREE

3. SERIAL I/O INTERFACE

The Serial I/O port can be connected to a terminal or computer. It is configured as a DTE interface and will require a null modem for operation with a terminal or computer.

3.1 SERIAL I/O FUNCTION LIST

Initially at power-up the Serial I/O port outputs time once per second as described in function F08 until it receives a control-C character (HEX 03). Then any of the following commands may be used:

COMMAND	FUNCTION
F01	Time Zone Entry/Request
F02	12/24 Hour Mode
F03	Time/Date Entry/Request
F05	Time Quality Enable/Setup
F08	Continuous Time Once Per Second Enable
F09	Time on Request Enable
F11	Time Output Format Entry/Request
F13	Worst-case Time Error Request
F18	Software Version Request
F36	NTS-100 Configuration Entry/Request
F66	Daylight Savings Enable
F67	Leap Second Information Entry/Request

3.2 SERIAL I/O FUNCTION F01 - TIME ZONE ENTRY/REQUEST

Use Serial I/O Function F01 to select or determine the time zone offset. To request the offset send F01<CR> to the Serial I/O port. The port will respond with the following character string:

F01<SEP><SIGN><HH>:<MM><LT>

where

F	=	ASCII character F.
01	=	function number.
<SEP>	=	one or more separator characters: either space, comma or tab.
<SIGN>	=	either no character or + for positive offsets or - for negative offsets.
<HH>	=	one or two digit hours offset from +12 to -12 hours.
:	=	ASCII character for a colon.
<MM>	=	two-digit minutes offset.
<LT>	=	line terminator, either a carriage return and line feed for output strings or a carriage return only for input strings.

Sample request: F01<CR>
Response: -4:30<CR><LF>

To set the time zone offset send a character string with the following format:

Sample entry: F01 -8:00<CR>
Response: OK<CR><LF>
Sample Request: F01<CR>
Response: -8:00<CR><LF>

3.3 SERIAL I/O FUNCTION F02 - 12/24 HOUR FORMAT ENTRY/REQUEST

Use Serial I/O function F02 to request or set the time display format. To determine the format, send F02<CR> to the Serial I/O port. The port will respond with the following character string:

F02<SEP><HH><LT>

where

F	=	ASCII character F.
02	=	function number.
<SEP>	=	one or more separator characters: either space, comma or tab.
<HH>	=	12 or 24.
<LT>	=	line terminator, either a carriage return and line feed for output strings or a carriage return only for input strings.

Sample request: F02<CR>
Response: F02 12<CR><LT>

To select 24 hour format, send the following character string:

Sample entry: F02 24<CR>
Response: OK<CR><LF>

3.4 SERIAL I/O FUNCTION F03 - TIME/DATE ENTRY/REQUEST

Use Serial I/O function F03 to enter or request time and date. To request time and date send F03<CR> to the Serial I/O port. The port will respond with the ASCII character string:

F03<SEP><TYPE><SEP><mm>/<dd>/<yy><SEP><HH>:<MM>:<SS><LT>

where

F	=	ASCII character F.
03	=	function number.
<SEP>	=	one or more separator characters: either space, comma, or tab.
<TYPE>	=	either LOCAL or UTC.
<mm>	=	one- or two-digit month.
/	=	ASCII character slash.
<dd>	=	one- or two-digit day.
<yy>	=	two-digit year.
<HH>	=	one- or two-digit hours.
:	=	ASCII character for a colon.
<MM>	=	two-digit minutes.
<SS>	=	two-digit seconds.
<LT>	=	line terminator, either a carriage return and line feed for output strings or a carriage return only for input strings.

Sample request: F03<CR>
Response: F03 UTC 01/07/91 02:48:29<CR><LF>

Sample entry: F03 LOCAL<CR>
Response: F03 LOCAL 01/07/91 7:48:29<CR><LF>

Sample request: F03 UTC<CR>
Response: F03 UTC 01/07/91 2:48:29<CR><LF>

To set the time zone offset send a character string with the format above to the Serial I/O port. Either the date MM/DD/YY or the time HH:MM:SS may be omitted if they are replaced with a semicolon (;). Only valid dates are acceptable.

The following entry sets the local date and time:

Sample entry: F03 LOCAL 10/3/03 20:07:04<CR>
Response: OK<CR><LF>

The following entry uses semicolons to omit the time type and date fields, thus setting the UTC time, and leaving the date unchanged.

Sample entry: F03 ;; 3:06:48<CR>
Response: OK<CR><LF>

3.5 SERIAL I/O FUNCTION F05 - TIME QUALITY ENABLE/SETUP

Use function F05 to enable or disable the time quality indicators or to set the four worst-case-error thresholds. The Serial I/O output string indicates the time quality. Refer to "SERIAL I/O FUNCTION F08 - CONTINUOUS TIME ONCE PER SECOND" for a description of the time quality indication in the Serial I/O time output string. As shipped the time quality indicators are enabled and the thresholds are set to 10000ns, 100000ns, 1000000ns, and 10000000ns. The unit will retain the values in use at power-down and use them for subsequent power-ups.

To determine if the indicators are enabled and what the thresholds are, send F05<CR> to the Serial I/O port. The port will respond with the ASCII character string:

F05<SEP><STATE><SEP><FLAG><SEP><FLAG><SEP><FLAG><SEP><FLAG><LT>

where

F	=	ASCII character F.
05	=	function number.
<SEP>	=	one or more separator characters: either space, comma or tab.
<STATE>	=	ON or OFF.
<FLAG>	=	one error threshold in nanoseconds, 1 to 11 digits with or without leading zeros.
<LT>	=	line terminator, either a carriage return and line feed for output strings or a carriage return only for input strings.

Sample request: F05<CR>
Response: F05 ON 00000000100 00000001000 00000010000 00000020000

To enable, disable or set the thresholds of the time quality indicators send a character string with the following format:

Sample: F05 ON 00000000100 00000001000 00000010000 00000020000
Response: OK<CR><LF>

Acceptable threshold value range: 00000000010ns to 40000000000ns.

Sample entry: F05 ON 100 200 500 1000
Response: OK<CR><LF>

Note that although leading zeros are not required for data entry they will be included in any data response.

3.6 SERIAL I/O FUNCTION F08 - CONTINUOUS TIME ONCE PER SECOND ENABLE

Internal time will output once per second at the Serial I/O port if command string F08<CR> is sent to the port. Time-of-year will output once per second after time input via function F03.

Character transmission is continuous with the end of the stop bit of one character coinciding with the beginning of the start bit of the next character. The time output string format may be changed with Serial I/O Function F11. The default output string format is:

<SOH>DDD:HH:MM:SSQ<CR><LF>

where

<SOH>	=	ASCII Start-of-Header character (HEX 01).
<CR>	=	ASCII Carriage Return character (HEX 0D).
<LF>	=	ASCII Line Feed character (HEX 0A).
DDD	=	day-of-year.
HH	=	hours.
MM	=	minutes.
SS	=	seconds.
:	=	colon separator.
Q	=	time quality character.

The time quality character may be a:

SPACE	which indicates a worst-case error less than threshold 1.
.	which indicates a worst-case error greater than or equal to threshold 1.
*	which indicates a worst-case error greater than or equal to threshold 2.
#	which indicates a worst-case error greater than or equal to threshold 3.
?	which indicates a worst-case error greater than or equal to threshold 4.

The time quality character prior to IRIG B lock signal acquisition will be "?". Refer to SERIAL I/O FUNCTION F13 - WORST-CASE-TIME ERROR REQUEST. The carriage return character <CR> start bit begins on the second, +0 to +1 bit time or ±1 ms, which ever is larger. Time will continue to output once per second until the port receives a CONTROL-C character (HEX 03). Until it receives a CONTROL-C the port will ignore all other input.

3.7 SERIAL I/O FUNCTION F09 - TIME ON REQUEST ENABLE

When the Serial I/O port receives the command string F09<CR> it waits for a request in the form of an upper-case ASCII character T to output the time-of-day string. After a T is received, the current time is saved (with a resolution of 1ms) in a buffer and is then transmitted to the port. The port will continue to respond with time-of-day each time it receives a T until this function is canceled by sending a CONTROL-C character

(HEX 03) to the port (all other input will be ignored until then). The default output string is as follows:

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

where

<SOH>	=	ASCII Start-of-Header character (HEX 01)
<CR>	=	ASCII Carriage Return character (HEX 0D)
<LF>	=	ASCII Line Feed character (HEX 0A)
DDD	=	day-of-year
HH	=	hours
MM	=	minutes
SS	=	seconds
mmm	=	milliseconds
:	=	colon separator
Q	=	time quality character -- refer to Function 08 for values

Sample entry:	F09<CR>
Second entry:	T
Response:	<SOH>128:20:30:04.357*<CR><LF>

3.8 SERIAL I/O FUNCTION F11 - TIME OUTPUT FORMAT ENTRY/ REQUEST

Use Serial I/O Function 11 to request or enter the time output string format that is used by Serial I/O Functions F08 and F09.

The format upon power-up will be the format that was in use just before power-down. To request the return of the present format send F11<CR> to the Serial I/O port. The string returned will contain X's in the positions that are omitted in the time output string.

When shipped, the format string will be set to the "null" string, causing the strings of the F08 and F09 outputs to take on their default values.

EXAMPLE F08: <SOH>DDD:HH:MM:SSQ<CR><LF> (Once per second time output mode)

Note: Milliseconds are never present in the output of F08 mode regardless of the format string entered with F11.

EXAMPLE F09: <SOH>DDD:HH:MM:SS.mmmQ<CR><LF> (Time on demand output mode) where

<SOH>	=	ASCII Start-of-Header character (HEX 01)
<CR>	=	ASCII Carriage Return character (HEX 0D)
<LF>	=	ASCII Line Feed character (HEX OA)
DDD	=	day-of-year
HH	=	hours
MM	=	minutes
SS	=	seconds
.	=	ASCII decimal point
mmm	=	milliseconds
:	=	colon separator
Q	=	time quality character position. Characters for this position are: < >, <.>, <*>, <#> and <?>

If non-volatile memory is corrupted the format string will be set to the "null" string.

When the unit returns the current format string in response to "F11<CR>" (as shown in the following example) the first character after the "F11" is always a blank and is not part of the format string but is only a separator.

Sample request: F11<CR>
Response: F11 <CR><LF>

The following text assumes that the format has been previously set to DDD::MMmSSQ.

Sample request: F11<CR>
Response: F11 DDD:XX:MMmSSXXXXQ<CR><LF>

This means that the response from F09 would be:

<SOH>122::24m55*<CR><LF>

To omit a character, other than <SOH> <CR> or <LF>, from the output string send a string of the form.

F11<SEP>DDD:HH:MM:SS.mmmQ<CR>

...with an upper case "X" in place of the character that you wish to omit. The <SOH>, <CR> and <LF> characters in the output strings of F08 and F09 are not subject to control by F11. <SEP> is one character only, either a space, comma or tab. Any character other than an upper case "X" in a numeric position will not affect the output of that position. The colons (:) or decimal point (.), however, may be replaced with any single ASCII character except null (HEX 00), carriage return, or line feed.

Sample entry: F11 XXXXXXXMMMSSS.mmmX<CR>
Response: OK<CR>
F08 string output: <SOH>12M34S<CR><LF>
F09 string output: <SOH>12M34S.567<CR><LF>

The above format means that days hours and the first two colon separators are suppressed and the third and fourth separators are "M" and "S".

Sample entry: F11,HHH;XX;mm:SS,mmmQ<CR>
Response: OK<CR>
F08 string output: <SOH>123;;55:45*<CR><LF>
F09 string output: <SOH>123;;55:45,678*<CR><LF>

The above format means that hours are deleted, the first two separators are semicolons instead of colons and the third separator is a comma instead of a period.

If the format string entered with F11 is terminated early with a carriage return, the remaining characters are enabled and assume their default values.

Sample entry: F11<TAB>XXX|<CR>
Response: OK<CR>
F08 string output: <SOH>|10:45:01*<CR><LF>
F09 string output: <SOH>|10:45:01.234*<CR><LF>

The above format means that days are deleted, the first separator is a vertical bar and all other characters are enabled and assume their default values.

When entering a new format string the character after "F11" is required but is ignored. To enter a "null" format string send "F11" followed by a space, followed by a carriage return.

Sample entry: F11 <CR>
Response: OK<CR>
F08 string output: <SOH>DDD:HH:MM:SSQ<CR><LF>
F09 string output: <SOH>DDD:HH:MM:SS.mmmQ<CR><LF>

The above format means that all characters and separators are enabled and assume their default values.

If the current format string is "null", F11 will return a space character followed by a carriage return.

Sample entry: F11<CR>
Response: F11 <CR>

The format string below explicitly enables all characters and has the same effect as a "null" format string:

Sample entry:	F11 DDD:HH:MM:SS.mmmQ<CR>
Response:	OK<CR>
F08 string output:	<SOH>DDD:HH:MM:SSQ<CR><LF>
F09 string output:	<SOH>DDD:HH:MM:SS.mmmQ<CR><LF>

3.9 SERIAL I/O FUNCTION F13 - WORST-CASE TIME ERROR REQUEST

Use Serial I/O Function F13 to request the estimated worst-case time error. Refer to keypad FUNCTION 13 - WORST-CASE TIME ERROR earlier in this Section for an explanation of worst-case time error. The worst-case time error while the synchronization source input is present and the NTS-100 is locked to it depends upon the type of synchronization source. Refer to SECTION FIVE for the timing accuracy specification for your synchronization source option. Time error begins to accumulate when the NTS-100 loses the synchronization source. The NTS-100 calculates the worst-case time error based on the stability of the time base and the time elapsed since loss of synchronization source. The Serial I/O port will report this calculated error when it receives the string F13<CR> and responds with the following ASCII character string:

F13<SEP><ERROR><CR><LF>

where

F	=	ASCII character F.
13	=	function number.
<SEP>	=	one or more separator characters; either space, comma or tab.
<ERROR>	=	calculated worst-case error in seconds.
<CR>	=	carriage return character.
<LF>	=	line feed character.

Sample request:	F13<CR>
Response:	F13 02.000000000<CR><LF>

3.10 SERIAL I/O FUNCTION F18 - SOFTWARE VERSION REQUEST

Use Serial I/O Function F18 to obtain information about the current version of the software installed in the unit. Send the string:

F18<CR>

The unit will respond with a string no longer that 80 characters, such as:

TrueTime Mk III sys ver 001 NTS V1.000 182-7002v001<CR><LF>

This string indicates that the system software is version 001, the Network Time Server-specific software is version 1.000 and the specific EPROM image is 182-7002, version 001.

3.11 SERIAL I/O FUNCTION F36 - NTS-100 CONFIGURATION ENTRY/ REQUEST

Use Serial I/O Function F36 to obtain information about the current NTS-100 configuration or to change the setup. Changing the network related fields of the configuration will cause a reset of the NTS-100 module.

3.11.1 ETHERNET ADDRESS

The ethernet address is a six byte, hexadecimal value specific to each NTS-100 module. The first three bytes are registered to TrueTime Inc, and the last three bytes are the hex value of the unit's unique number. The ethernet address of the NTS-100 is a fixed address established at the factory. To request the ethernet address of the NTS-100 module, send the string:

F36 EA<CR>

The unit will respond with:

F36 EA:00-A0-69-xx-xx-xx<CR><LF>

where "xx-xx-xx" are the six hex digits of the unit's unique address. Attempts to set this field will be rejected with a syntax error message.

3.11.2 IP ADDRESS

To obtain the IP address of the NTS-100 module, send the string:

F36 IP<CR>

The unit will respond with a string of the form:

F36 IP:nnn.nnn.nnn.nnn<CR><LF>

where "nnn.nnn.nnn.nnn" is the dotted decimal address notation. To set the IP address and restart the NTS-100, send a string of the form:

F36 IP:nnn.nnn.nnn.nnn<CR>

Example: F36 IP:206.54.0.21<CR>

Changing this parameter will cause a software reset of the NTS-100 module.

3.11.3 SUBNET MASK

To return the subnet mask of the NTS-100 module, send the string:

F36 SM<CR>

The unit will respond with:

F36 SM:nnn.nnn.nnn.nnn<CR><LF>

To set the subnet mask and restart the NTS-100, send the string:

F36 SM:nnn.nnn.nnn.nnn<CR>

Example: F36 SM:255.255.255.240<CR>

Changing this parameter will cause a software reset of the NTS-100 module.

3.11.4 DEFAULT GATEWAY

To obtain the default gateway of the NTS-100 module, send the string:

F36 G<CR>

The unit will respond with:

F36 G:nnn.nnn.nnn.nnn<CR><LF>

To set the default gateway and restart the NTS-100, send the string:

F36 G:nnn.nnn.nnn.nnn<CR>

Example: F36 G:206.54.0.17<CR>

Changing this parameter will cause a software reset of the NTS-100 module.

3.11.5 NETWORK PACKET TYPE

To determine the type of network packets being used, send the string:

F36 N<CR>

The unit will respond with one of two strings:

For IEEE 802.3 networks
the unit will respond: F36 N:I<CR><LF>

or

For Ethernet II DIX networks
the unit will respond: F36 N:E<CR><LF>

To set the type of network being used send the appropriate string shown below:

For IEEE 802.3 networks send: F36 N:I<CR>
For Ethernet II DIX networks send: F36 N:E<CR>

Note that this setting affects only the packet type that the NTS-100 will transmit. *The NTS-100 will receive packets of either type, regardless of this setting.*

Changing this parameter will cause a software reset of the NTS-100 module.

3.11.6 COMPLETE NTS-100 NETWORK CONFIGURATION

To review the entire current network configuration of the NTS-100 module, send the string:

F36<CR>

The unit will respond with (example):

F36 IP:206.54.0.21 SM:255.255.255.240 G:206.54.0.17
N:E<CR><LF>

This response indicates the specific IP address, Subnet Mask, Default Gateway, and Network Type of the NTS-100 module. Note that the leading zeros within fields of the dotted decimal addresses are omitted from the IP address, Subnet Mask, and Default Gateway.

To set all settable network parameters and reset the NTS-100 card, send the string (example):

F36 IP:206.54.0.21 SM:255.255.255.240 G:206.54.0.17 N:E<CR>

This example provides the NTS-100 card with an IP address, Subnet Mask, Default Gateway and Network Type. Note that leading zeros may be omitted when entering IP address, Subnet Mask, and Default Gateway. Any field may be omitted and order is not significant. Blanks are allowed on either side of a colon. Any legal command set containing one of the four network parameters will cause a software reset of the NTS-100.

3.11.7 CLOCK TYPE

The synchronization input option determines the clock type. To query the clock type, send the string:

F36 T<CR>

The unit will respond with:

GPS input operation:	F36 T:GPS<CR><LF>
IRIG B input operation:	F36 T:IRIG<CR><LF>
External 1 PPS input operation:	F36 T:1PPS<CR><LF>
For ACTS input operation:	F36 T:ACTS<CR><LF>

Attempts to set this field will be rejected with a syntax error message.

3.11.8 CLOCK ACCURACY

When the synchronization input option of the NTS-100 is either IRIG-B or External 1 PPS, the accuracy of the timing source driving the IRIG-B or External 1 PPS input must be provided to the NTS-100 so that the appropriate fields in the NTP packet may be properly set. To obtain the current setting of the accuracy of the local time source, send the string:

F36 A<CR>

The unit will respond with (example):

F36 A:1.0e-5<CR><LF>

This example illustrates a unit with an accuracy of 10 µs.

To set the accuracy of the NTS-100 module, send the string (example):

F36 A:0.5e-3<CR>

This example illustrates setting the accuracy of the NTS-100 module to 0.5 ms.

When the synchronization input option is GPS, the NTS-100 will automatically make this setting, and operator attempts to set it will be ignored.

3.12 SERIAL I/O FUNCTION F66 - DAYLIGHT SAVINGS ENABLE

Use Serial I/O Function F66 to enable or disable or set the entry or exit times for DST. The initial out-of-the-box default is "Off". The default upon subsequent power-ups will be the selection in use just prior to the previous power-down.

To request the present status of the daylight savings enable, send F66<CR> to the serial port. The port will respond with the ASCII character string:

F66<SEP><STATE><LT>

where

F	=	ASCII character F.
66	=	function number.
<SEP>	=	one or more separator characters: either space, comma or tab.
<STATE>	=	Off or Manual.
<LT> =		line terminator, either a carriage return and line feed for output strings or a carriage return only for input strings.

If the DST function is in Manual, the port will respond with the longer string described below:

Sample request: F66<CR>
Response: F66 OFF<CR><LF>

To alter the state of the daylight savings enable send a character string with the format above to the serial port.

Sample entry: F66<TAB>Off<CR>
Response: OK<CR><LF>

To place the DST function in Manual and set the DST entry and exit times send a continuous string of the form:

F66 MANUAL <IN HOUR><SEP><IN WEEK><SEP><IN DAY><SEP><IN MONTH><OUT HOUR><SEP><OUT WEEK><SEP><OUT DAY><SEP><OUT MONTH><LT>

where

<IN HOUR>	=	time to enter DST in 24-hour format.
<SEP>	=	one or more separator characters, either space comma or tab characters. For output strings this will be a single space character.
<IN WEEK>	=	which week to enter DST, 1, 2, 3, 4 or 0 (for last).
<IN DAY>	=	day of week to enter DST, 1 through 7 where Sunday is 1.
<IN MONTH>	=	month to enter DST, 1 through 12 where 1 is January.
<OUT HOUR>	=	hour to exit DST, in 24 hour format.
<OUT WEEK>	=	which week to exit DST, 1, 2, 3, 4 or 0 (for last).
<OUT DAY>	=	day in to exit DST, 1 through 7 where Sunday is 1.
<OUT MONTH>	=	month to exit DST, 1 through 12 where 1 is January.
<LT >	=	line terminator, a carriage return and line feed for output strings, only a carriage return for input strings.

If desired, any item may be replaced with a semicolon, which will leave its value unchanged. If any of the items in an input string are invalid, an error message will be returned.

Sample Request:	F66<CR>
Response:	F66 MANUAL 02 1 1 04 02 0 1 10
Meaning:	Manual settings are in effect. The entry time is 2 a.m. on the first Sunday of April and the exit time is 2 a.m. on the last Sunday in October.

Sample Entry:	F66 MANUAL ; 0 ; ; ; ; ; ;<CR>
Response:	OK<CR><LF>
Meaning:	DST will now be entered on the last week of the month. All other parameters remain unchanged.

Sample Entry:	F66 MANUAL 4 2 2 3 13 4 6 11<CR>
Response:	OK<CR><LF>
Meaning:	DST will now be entered 04 a.m. on the 2nd Monday in March and exit DST at 1 p.m. on the 4th Friday in November.

3.13 SERIAL I/O FUNCTION F67 - LEAP SECOND INFORMATION

Though strictly they may be performed at two other times during the year, in practice UTC leap second adjustments are only performed on two days of the year: June 30 and December 31. Use serial Function 67 to retrieve/send information regarding upcoming leap seconds. To return the leap second status, send the string:

F67<CR>

The NTS-100 module will return:

F67 06/30/97 +1<CR><LF>

This response indicates a leap second addition during the last minute of June 30, 1996. If there is no leap second pending, the module will return:

F67 none<CR><LF>

To set the leap second information for the next possible adjustment date, send the following strings:

To set a leap second addition for June 30, 1996 send:	F67 06-30-96 +<CR>
To set a leap second subtraction for December 31, 1998 send:	F67 12-31-98 -1<CR>
To clear a leap second setting send:	F67 none<CR>

If a date for a leap second event is sent other than the next possible adjustment date, i.e. June 30 if the current date is in the first half of the year or December 31 if the current date is in the second half of the year, the NTS-100 will return an error message and ignore the information.

SECTION FOUR

4. MD5 AUTHENTICATION PROTOCOL

4.1 MD5 INTRODUCTION

MD5 is a security protocol that can be used to authenticate NTP client - server communications. TrueTime's version of MD5 is completely compatible with current versions of NTP client software xntpd 3.XX and ntpdate 3.XX furnished by Dr. David Mills at the University of Delaware. MD5 was drafted into a standard by MIT Laboratory for Computer Science and RSA Data Security, Inc. MD5 authentication means the information within the NTP packet is guaranteed to be unaltered and from a user having privileged access. Unlike other cryptographic ciphers, MD5 does not hide the data within the packet. The MD5 authenticated NTP packet is still readable. This means MD5 is faster to generate than other cryptographic protocols, and as Dr. Mills notes, there is no reason to hide the actual time from anyone. Further, MD5 does not suffer from any export restrictions. Think of MD5 as a very sophisticated NTP data checksum that is extremely difficult to reverse generate.

The MD5 cryptographic key identifier and cryptographic message digest are tacked on to the end of a normal NTP packet and the two pieces of information are referred together as an MD5 signature. The key identifier is the first field in the signature and it is a 32 bit integer in the range from 1 to 4294967295 (0xFFFFFFFF). Note: Zero is an illegal value, and for TrueTime setup purposes, 0 internally means the key identification is unused. This number specifies an index into a table of many possible MD5 keys. A key is an ASCII alpha/numeric character string that is from 1 to 31 characters in length. The key is most secure when all 31 characters are filled with numbers and letters chosen at random. The ASCII key string is combined with the NTP packet data and results in a secure message digest. The MD5 message digest is 16 bytes in length and it follows the key identifier in the signature. A server authenticates the NTP packet from a client by looking up the key by reference to the key identifier; generates the MD5 message digest based on the key and the NTP data; and compares the resulting message digest to the client packet's MD5 message digest. If the two compare, a NTP reply packet is generated with a new MD5 signature. If the MD5 message digests do not agree, then the NTP client packet is ignored by the TrueTime server.

For more technical information on MD5 see the MD5 RFC 1321, NTP RFC 1305, and the release notes for NTP client software furnished by Dr. David Mills' web site located at the University of Delaware at http://www.eecis.udel.edu/~ntp, or http://www.eecis.udel.edu/~ntp/software.html.

4.2 TRUETIME NTP MD5 OPERATION

A TrueTime NTP time server can handle both unauthenticated and MD5 authenticated packets at the same time. A packet is assumed to be MD5 authenticated if the total UDP data size of the packet is equal to the size of a normal NTP packet plus the exact size of an MD5 signature. A normal unauthenticated NTP packet is one that has no extra bytes beyond the last NTP timestamp. The procedure used is functionally the one followed by Dr. David Mills' NTP software. Packets without authentication are returned without signatures and packets with authentication are returned with authentication signature using the key ID specified by the client request. If a packet does not send the correct authentication signature, it is silently dropped.

A TrueTime NTS can contain up to 16 MD5 authentication keys. MD5 keys are entered and maintained through the standard TrueTime keypad and serial interfaces. Therefore, for security reasons, the TrueTime time server must be physically isolated from unauthorized users. MD5 keys must be changed on a regular schedule as a further security measure. Persons privileged to carry and maintain keys must have appropriate clearances and be trained for handling secure information. Note: Keys that are no longer trusted (are potentially compromised) must be deleted from the TrueTime MD5 key table.

4.3 SERIAL MD5 KEY CONFIGURATION

You may add, delete, and view the MD5 keys using the serial interface.

4.3.1 VIEW PARTICULAR NTP MD5 KEY TYPE

F36 MV:x

Where x is the key identification number ranging from 1 to 4294967295.

The unit will respond with:

F36 key ID = x, key = ValueOfMD5KeyString

4.3.2 VIEW NEXT NTP MD5 KEY TYPE

F36 MV

The unit will respond with:

F36 key ID = (x+1), key = ValueOfMD5KeyString

Where (x+1) is the next key identification in numerical order from the last serial command that reference a key identification. Note: After booting, the key viewed will be the lowest numbered key identification. If the previous key viewed was at the end of the key identification list it will wrap back to the first key identification.

4.3.3 ADD NTP MD5 KEY TYPE

F36 MS:x ValueOfMD5KeyString

Where x is the key identification number ranging from 1 to 4294967295 and ValueOfMD5KeyString is the MD5 ASCII string key ranging from 1 to 31 characters. Note: It is best to limit the string to alpha/numeric characters only. If other characters are desired, then the restrictions the remote NTP client program places on the string must be considered.

The unit will respond with:

OK

4.3.4 DELETE NTP MD5 KEY TYPE

F36 MD:x

Where x is the key identification number ranging from 1 to 4294967295. The unit will respond with:

OK

4.3.5 DELETE ALL NTP MD5 KEY TYPES

F36 MD:ALL

4.3.6 UNIT RESPONDS

The unit will respond with:

OK

SECTION V

5. IRIG B SYNC INPUT OPTION

5.1 INTRODUCTION

This Section describes setup and operating procedures for using the NTS-100 with IRIG B as the synchronization source.

The NTS-100 IRIG-B Sync Input characteristics are:

Format:	IRIG-B
Input Range:	500 mVpp to 5 Vpp
Input Z:	10K ohms
Accuracy:	±5 µs, with respect to the input code

After making the appropriate input connection and applying power, the Serial I/O port or front panel keypad must be used to continue setup of the NTS-100.

Since IRIG B does not contain year information, the date must be set using Function 03. Function 03 is described in detail in SECTION THREE. To set the date via the Serial I/O port, send the string:

F03 UTC MM/DD/YY ;<CR>

or, to set the date via the front panel keypad:

Press "FUNC/ENTR" “0” “3” "FUNC/ENTR", use the keypad to enter the date, then press "FUNC/ENTR", use the keypad to enter the approximate time, then press "FUNC/ENTR".

Using Serial I/O F03 in this manner does not affect the time. *Only after the date has been entered will the NTS-100 indicate a lock to the incoming IRIG B time code, and respond to NTP packet requests with the Leap Indicator bits set to a value other than 3, the alarm condition*.

Although it is not absolutely necessary to provide leap second information to the NTS-100 with IRIG-B synchronization option, if it is not provided there are two potential drawbacks:

1) The NTS-100 will not place any advance indication in the Leap Indicator field of the NTP packet of an impending leap second event. Refer to Appendix A for details of the NTP packet format.

2) There will be a short period at and following the occurrence of the leap second event during which the NTS-100 time will disagree with the IRIG-B synchronization source (assuming that the IRIG-B source is maintaining strict UTC). This will only persist until the NTS-100

has determined that a valid time step of the input IRIG-B has occurred (a few seconds) and corrects its time to match the IRIG-B source. During this period, NTP packet timestamps created by the NTS-100 will be in error.

During the six months prior to the addition of a new leap second, the USNO will publish to the user community its plan to implement a leap second. Leap seconds are added (or subtracted) only at the end of the days of June 30 and December 31. If the NTS-100 is informed of an impending leap second adjustment at any time during the six months prior to the next leap second adjustment, then it will store that information in its EEPROM. When the time for the leap second adjustment approaches, the NTS-100 will automatically place the appropriate information in the Leap Indicator field of the NTP packet and at the appropriate time will perform the leap second correction to its internal clock. Use Serial I/O Function F67, which is described in detail in SECTION THREE, to provide this information to the NTS-100.

When operating the NTS-100 from an IRIG-B synchronization source, the operator must input information about the clock which is producing the IRIG-B signal. The parameter which is required is entered using the Serial I/O Function F36 and is the “Clock Accuracy” field. This field must specify the accuracy of the clock which is being used to generate the IRIG-B code. Refer to SECTION THREE, Function F36 and Appendix A for more detail on the setting of this parameter.

In addition, if the incoming IRIG-B sync input contains embedded Lock Quality indicators then the operation of the NTS-100 with respect to these must be configured via Function 36:

F36 Keypad Operation:

Pressing "FUNC/ENTR" on “Display/Setup IRIG Lock Quality” enables the user to view and/or change the bit in the IRIG code which determines the status of the NTS-100 lock indicators. The format of the IRIG Lock Quality display is shown here:

IRIG-B Lock
Quality: Lock *(Example)*

Pressing the Up and Down arrows scrolls through the selections for Lock Quality: Lock, TQ1, TQ2, TQ3, TQ4, and None. When the desired selection is displayed, press "FUNC/ENTR" to enter the selection and proceed to the next parameter, “CLR” to restore the original setting, or “STATUS” to exit function 36 without saving any updated settings.

F36 Serial I/O Operation:

The IRIG Lock Quality determines the bit in the incoming IRIG data which the NTS-100 uses to determine whether or not it is receiving valid time. Possible settings are: Lock, TQ1, TQ2, TQ3, TQ4, and None. To determine the current configuration of the NTS-100, send the string:

F36 IQ<CR><LF>

The unit will respond with:

F36 IQ: *setting*

To set the IRIG Lock Quality, send a string of the form:

F36 IQ: *setting*<CR><LF>
Example: F36 IQ: None<CR><LF>

APPENDIX A

NTP V 3.0 DATA FORMAT PER RFC1305

A-1 The layout of the NTP data packet information following the UDP header is shown below.

Leap Indicator	Version Number	Mode	Stratum	Poll	Precision
Synchronizing Distance (Root Delay Version 3)					
Synchronizing Dispersion (Root Dispersion Version 3)					
Reference Clock Identifier					
Reference Timestamp					
Originate Timestamp					
Receive Timestamp					
Transmit Timestamp					
Authenticator					

A-2 Leap Indicator - The leap indicator is a 2 bit code which signals an impending leap second to be added or subtracted in the last minute of the current day. Leap year codes and their corresponding meanings are shown in the table below.

Bit 0	Bit 1	Meaning
0	0	Normal Operation
0	1	61 second last minute
1	0	59 second last minute
1	1	Clock not synchronized

The unsynchronized state is indicated by the NTS-100 whenever the estimated synchronization error is greater than the root dispersion. Such conditions typically occur following turn-on, until synchronization with the external source has been achieved, and whenever the external synchronization input has been removed and the extrapolated time error has exceeded the value of the root dispersion.

A-3 Version Number - The version number is a three bit integer which specifies the NTP version. The NTS-100 will copy this field from the client requesting packet and return it in this field if it is equal to either 2 or 3. NTP version 1.0 packets are not supported.

A-4 Mode - The mode is a three bit integer that determines the functions the NTS-100 module will perform. TrueTime's NTS-100 module operates in mode four or server mode. Mode four operation allows the module to synchronize hosts but will not allow the module to be synchronized by another host.

A-5 Stratum - The stratum is an eight bit integer providing the stratum level of the local time source. TrueTime's NTS-100 module operates in stratum 1, denoting a primary reference.

A-6 Poll Interval - The poll interval is a signed eight bit integer used as the exponent of two to yield in seconds the minimum interval between consecutive messages. For example, a poll interval value of six implies a minimum interval of 64 seconds. The NTS-100 does not alter the setting of this field.

A-7 Precision - The precision is a signed eight bit integer used as the exponent of two to yield in seconds the precision of the local time source and any other hardware affecting the base level "jitter" of the time server. This field is set to approximate the time stamping resolution of the NTS-100 which is 10 µs. So the precision byte is set to -16 which is equivalent to a precision of 15.26 µs.

A-8 Synchronizing Distance (Root Delay Version 3) - The root delay is a signed 32 bit fixed point number representing the predicted round trip delay in seconds to the primary synchronizing source. The fraction point is between bits 15 and 16. This value is set to 0 seconds in TrueTime's NTS-100 module.

A-9 Synchronizing Dispersion (Root Dispersion Version 3) - The root dispersion is a signed 32 bit fixed point number representing the maximum error in seconds relative to the primary synchronizing source. This value is a function of the precision and the quality of the synchronization input option. The user must provide an accuracy input via Serial I/O Function 36 when the synchronization input option is IRIG-B, ACTS or External 1 PPS, since the root primary synchronizing source is not known by the NTS-100 in those cases. When the synchronization input option is GPS, then the NTS-100 will self determine the accuracy. Once the accuracy has been determined, then the NTS-100 sets the root dispersion equal to ten times the square root of the sum of the squares of the precision and the accuracy, except for the ACTS synchronization option, where the root dispersion is set equal to the accuracy.

A-10 Reference Clock Identifier - The reference clock identifier is a 32 bit code identifying the particular type of timing source. Strata 0 and 1 use a four-octet, left justified, zero-padded ASCII string. TrueTime's NTS-100 module operates as Stratum 1 and uses this four-octet string based on the local time source input as shown in the table below. This setting is determined based on the NTS-100 synchronization input option.

Local Source Input	Reference Identifier String
GPS	"GPS"
IRIG B	"IRIG"
1 PPS	"1PPS"
ACTS	"ACTS"

A-11 Reference Timestamp - The reference timestamp is a 64 bit timestamp format representing the local time at the last update. TrueTime's NTS-100 module's reference timestamp is the last time that a valid synchronization source signal was present.

A-12 Originate Timestamp - The originate timestamp is a 64 bit timestamp format representing the time that the request left the client host.

A-13 Receive Timestamp - The receive timestamp is a 64 bit timestamp format representing the time that the request arrived at the service host.

A-14 Transmit Timestamp - The transmit timestamp is a 64 bit timestamp format representing the time that the reply left the service host.

A-15 Authenticator - This is a 96 bit field containing the authenticator information as described in Appendix C of RFC-1305. This field is not implemented by the NTS-100.

SNTP v 3.0 DATA FORMAT per RFC1361

When the NTS-100 replies to requests from SNTP clients, the packet format is the same as the NTP packet format described above, with these differences:

A-1S Leap Indicator - The NTS-100 will set these 2 bits to either 0 (normal) or 3 (unsynchronized) only

A-3S Version Number - The NTS-100 will copy this field from the client request packet and return it in this field.

A-11S Reference Timestamp - This field is set to the time that the reply left the NTS-100 server host

A-13S Receive Timestamp - This filed is set to the time that the reply left the NTS-100 server host

A-14S Transmit Timestamp - This field is set to the time that the reply left the NTS-100 server host

A-15S Authenticator - This field is not used in SNTP

APPENDIX B

TIME PROTOCOL PER RFC868

B-1 This protocol provides a site-independent, machine readable date and time. The TIME service sends back to the originating source the UTC time in seconds since midnight on January 1, 1900.

B-2 This protocol may be used either above the Transmission Control Protocol (TCP) or above the User Datagram Protocol (UDP). The NTS-100 implements the TIME protocol only above the UDP.

When used via UDP the TIME service works as follows:

Server: Listen on port 37 (45 octal).

Client: Send an empty datagram to port 37.

Server: Send a datagram containing the UTC time as a 32 bit binary number.

Client: Receive the TIME datagram.

The server listens for a datagram on port 37. When a datagram arrives, the server returns a datagram containing the 32-bit time value. If the server is unable to determine the time at its site, it should discard the arriving datagram and make no reply.

B-3 The Time Format

The time is the number of seconds since 00:00 (midnight) 1 January 1900 UTC, such that the time 1 is 12:00:01 am on 1 January 1900 UTC; this base will serve until the year 2036.

APPENDIX C

SIMPLE NETWORK MANAGEMENT PROTOCOL

1.1. SNMP INTRODUCTION

1.1.1. The TrueTime Network Time Server completely supports a SNMP version 1 agent with the MIB II database. SNMP management software allows a network user to remotely monitor and configure an IP (Internet) host that supports a SNMP agent. A SNMP agent is protected from unauthorized use through a security authentication scheme. Further, TrueTime has extended the MIB II database with its own custom enterprise MIB that allows a manager more control than what is specified in the MIB II database.

1.1.2. We assume the reader has an understanding of SNMP because a complete introduction to SNMP would fill many volumes of user manuals. If the reader is unfamiliar with SNMP, pick up a copy of "SNMP, SNMPv2 and CMIP" written by William Stallings and published by Addison-Wesley Publishing Company. This book is considered by the Internet community to be the definitive introduction to SNMP. For more technical references, see RFC 1157 (definition of SNMPv1), RFC 1213 (definition of MIB II) and RFC 1354 (IP Forwarding table addition to MIB II). All RFCs are published with approval by the Internet Activities Board and they are readily found on the Internet by running any search engine and typing in the search field “RFC ####”. Some example WEB locations of search engines are http://search.yahoo.com or http://www.altavista.digital.com.

1.2. SNMP CONFIGURATION

1.2.1. SNMP offers a security authentication scheme that is based on a common password shared by the management station and a group of agents. A group of hosts are known as a community. Any management station or agent can be a member of any combination of communities. Typically a manager will need to change the SNMP community information from TrueTime’s SNMP agent factory defaults for security purposes. However, the factory default SNMP community settings are chosen to make the TrueTime SNMP immediately useable. TrueTime’s SNMP agent recognizes up to five separate SNMP communities. These communities are configured through the serial user port using the F36 string, the front panel keypad, or in the near future remotely using SNMP and TrueTime’s Enterprise MIB. Each community has several configurable parameters that are defined in the following table:

Keyword (as seen from the front panel display)	**Definition**
Community Name	The name of this community. The name is limited to up to 32 ASCII letters, numbers or punctuation letters. This is the name that a management SNMP PDU (packet) specifies. If the community name of an incoming PDU does not match any of the five community names, the packet is ignored and an optional authentication trap message can be generated. See traps below. An empty string field disables the community name.
Trusted IP Address	If the Use Trusted IP flag is set to yes, then this is the table of IP host addresses that this community recognizes as valid SNMP management hosts. Even if the community name of an incoming PDU matches this community, the source IP address must match one of the IP addresses in this table, or the packet is ignored and an optional authentication error trap message is issued. Setting an IP address to all zeros turns off that IP address entry. In addition, this table also serves as the list of hosts that SNMP trap messages are sent to - no matter what the state of Use Trusted IP flag is.
Use Trusted IP	If this flag is set to yes, then the Trusted IP Address table is used in addition to the Community Name for authentication of incoming PDU(s).
R/W Access	For a particular community, the SNMP variables are set to read only, or normal SNMP access. This allows the manager to have a public known community from which anyone may read the SNMP data base and a separate private community that has full normal read and write access to the SNMP database. Note: SNMP MIB II does not define all variables to be writeable. SNMP variables defined by RFC 1213 as read-only remain read-only no matter what the state of this R/W Access flag is.
Trap Enable	When this flag is set to yes, trap messages are issued for this community. Note: this enables/disables all traps (both cold start and authentication).
Trap Port	A trap port other than the normal SNMP trap port of 162 maybe specified. Note: this address must be chosen carefully, or conflicts with other protocols may occur.
Save settings	When any setting is changed, this becomes visible and answering yes immediately saves the changes to TrueTime's SNMP. Answering No will negate the changes.

1.2.2. The following table defines SNMP configurable parameters that are applied globally to all SNMP communities; this menu appears after the last community menu:

Keyword (as seen from the front panel display)	**Definition**
SNMP Global Enable Traps	When set to yes, all authentication failure traps are disabled. This flag overrides the Trap Enable flag set for each community. Note: this directly sets the value of the SNMP variable snmpEnableAuthenTraps.0. Note: the state of this flag has no effect on the issue of cold start trap messages.
Return To Main Menu	This leads back to the main SNMP function window.
Save settings	When SNMP Global Enable Traps is changed, this becomes visible and answering yes immediately saves the change to TrueTime's SNMP. Answering No will negate the change.

1.2.3. The following table summarizes the TrueTime factory default settings for SNMP:

Key word ()	**Definition**
Community 1	
Community Name	public
Trusted IP Address	0.0.0.0, 0.0.0.0, 0.0.0.0, 0.0.0.0
Use Trusted IP	no
R/W Access	read/only
Trap Enable	no
Trap Port	162
Community 2	
Community Name	system
Trusted IP Address	0.0.0.0, 0.0.0.0, 0.0.0.0, 0.0.0.0
Use Trusted IP	no
R/W Access	normal
Trap Enable	no
Trap Port	162
Community 3 to 5	
Community Name	
Trusted IP Address	0.0.0.0, 0.0.0.0, 0.0.0.0, 0.0.0.0
Use Trusted IP	no
R/W Access	read/only
Trap Enable	no
Trap Port	162
SNMP Global Enable Traps	yes

1.2.4. The factory default settings are summarized as follows: community one is called *public* and is set to read-only access for the SNMP MIB; community two is named *system* and it has normal access to the SNMP database; all other communities are disabled. All traps are disabled. Many SNMP management utilities are written with these default assumptions and thus the TrueTime SNMP is immediately useable without configuration.

1.3. NTP PARAMETERS

1.3.1. To configure SNMP from the keypad, press the status function button first and then press FUNC/ENTR 36. This takes you to the network configuration menu. Continue pressing the up-arrow key until the Display/Set SNMP prompt is displayed. Press FUNC/ENTR to start configuration for SNMP. Next, press the up-arrow to select the community that you want to configure. At the proper SNMP Community menu number, pressing the FUNC/ENTR key takes you into that community and you may configure its parameters as described in the above tables. Use the up or down arrow keys to toggle through your settings options. The left and right arrow keys move between digits and letters within an address or a string. Note: because the keypad has only numbers on the front panel, the letters for community names can only be chosen by using the up or down arrow keys and cycling to the letter of your choice. For this reason, it is more efficient to use the serial port, or the TrueTime Enterprise MIB to set the SNMP community name parameters.

1.3.2. You may exit the SNMP configuration when you are back in the Display/Set SNMP window by pressing the up or down arrow keys. Note: if you use the status key to exit the SNMP menu you must do this after you have answered yes in the Save settings menu or you will loose your settings. Once saved, changes to SNMP take place immediately and there is no need to reboot the timeserver.

1.4. Configuring of SNMP Through the Serial Interface

Use Serial I/O Function F36 to obtain information about the current SNMP configuration or to change the setup (there are five possible communities in this unit. In each of the strings listed below x represents the community number 1-5.) To read the current settings for an SNMP community, send the string:

F36Cx<CR>

The unit will respond with a string of the form:

F36 Cx: name UseIP:n R/W:n Trp On:n Trp Prt:n<CR>
where n is 0 for off or 1 for on

Ex: F36 C1: system UseIP:0 R/W:1 Trp On:1 Trp Port:162<CR>
In this example the community name is “system”. The access mode is read/write. Traps are on and the trap port is 162. This community will not use the trusted IP address list.

To read the current list of trusted IP addresses for an SNMP community send a string:

F36CxIP<CR>

The unit will respond with a string of the form:

F36 Cx Trusted Ips: n.n.n.n n.n.n.n n.n.n.n n.n.n.n<CR>
where n.n.n.n is an IP address

Ex: F36 C1 Trusted IPs: 206.54.0.50 206.54.0.51 206.54.0.52 0.0.0.0<CR>
The trusted IP addresses for community number 1 are listed.

1.4.1. READ SNMP CONFIGURATION

Each of the SNMP fields can be read individually. The read commands are listed below.

To read the community name send a string:

F36CxN<CR>

The unit will respond with:

F36 Cx Name:aaaa<CR>
where aaaa is an alphanumeric string up to 32 bytes long

To read a trusted IP address for a community send a string:

F36CxIPy<CR>
where y is a trusted IP address field 1-4

The unit will respond with:

F36 Cx Trusted Ipy: n.n.n.n<CR>
where n.n.n.n is an IP address

To read the use trusted IP addresses (UseIP) setting send a string:

F36CxU<CR>

The unit will respond with:

F36 Cx Use Trusted IP Addresses:n<CR>
where n is 0 for off or 1 for on

To read the trap enable (Trp On) setting send a string:

F36CxT<CR>

The unit will respond with:

F36 Cx Trap Enable:n
where n is 0 for off or 1 for on

To read the trap port (Trp Prt) number send a string:

F36CxTP<CR>

The unit will respond with:

F36 Cx Trap Port: nnnnn<CR>
where nnnnn is the trap port number

To read the access mode (R/W) for a community send a string:

F36CxA<CR>

The unit will respond with:

F36 Cx Normal Access:n
where n is 0 for off (read only) or 1 for on (read/write)

1.4.2. WRITE SNMP CONFIGURATION

The commands to change SNMP community settings are listed below:

To set a community name send a string:

F36CxN: aaaa<CR>
where aaaa is alphanumeric string up to 32 bytes long.

Ex: F36C3N: public<CR>

For community number 3 this sets the name to 'public'.

To set a trusted IP address send a string:

F36CxIPy: n.n.n.n<CR>
where y is trusted ip address field 1-4
n.n.n.n is an ip address

Ex: F36C2IP4: 206.54.0.50

This sets trusted IP address field 4 in community 2 to 206.54.0.50.

To set the use trusted IP (UseIP) flag send a string:

F36CxU: n<CR>
where x is community number 1-5
n is 0 for off or 1 for on

Ex: F36C5U: 0

This says that community 5 will not use trusted IP addresses.

To set the trap enable flag send a string:

F36CxT: n<CR>
where n is 0 for off or 1 for on

Ex: F36C2T: 1

This sets the trap enable flag for community number 2 to on.

To set the trap port send a string:

F36CxTP: nnnnn<CR>
where nnnnn is the trap port number

Ex: F36C1TP: 162

This sets the trap port for community number 1 to 162.

To set the read/write access for a community send a string:

F36CxA: n
where n is 0 for off (read only) or 1 for on (read/write)

Ex: F36C3A: 0

This sets the access for community number 3 to read only.

1.4.3. SNMP GLOBAL ENABLE TRAPS

The SNMP variable snmpEnableAuthenTraps.0 can be changed via the serial port. This flag overrides the Trap Enable flag set for each community. To read the state of this flag send the string:

F36ST<CR>

The unit will respond with:

F36ST:n
where n is 0 for off or 1 for on

To set this variable send the string:

F36ST:n
where n is 0 for off or 1 for on

SNMP TrueTime Enterprise MIB variable definitions (machine-ready file: TrueTime #183-0017)

```
-- The Enterprise
Enterprise                  OBJECT IDENTIFIER ::= { 1.3.6.1.4.1 }

-- TrueTime's Enterprise MIB
TrueTimeEntMIB              OBJECT IDENTIFIER ::= { Enterprise 1896 }

-- groups in TrueTime Enterprise MIB
trapMsg                     OBJECT IDENTIFIER ::= { TrueTimeEntMIB 1 }
ntp                         OBJECT IDENTIFIER ::= { TrueTimeEntMIB 2 }
ntsControl                  OBJECT IDENTIFIER ::= { TrueTimeEntMIB 3 } (Preliminary)
gps                         OBJECT IDENTIFIER ::= { TrueTimeEntMIB 4 }
acts                        OBJECT IDENTIFIER ::= { TrueTimeEntMIB 5 }

-- Display Strings (for compatibility with MIB-II definitions)
DisplayString ::=           OCTET STRING

-- the trapMsg group
```

The Implementation of the trapMsg group is mandatory for all TrueTime network products. The following are the trap messages that are issued by the TrueTime time server. Trap messages are issued for cold starts (reboot or power up), NTP loss of time synchronization and authentication failures for SNMP.

```
trapMsgColdStart OBJECT-TYPE
        SYNTAX          DisplayString (SIZE (0..255))
        ACCESS          read-only
        STATUS          mandatory
        DESCRIPTION     This is an ASCII string sent to UDP port 162 (or user defined) when the
                        TrueTime time server reinitializes. The message is "Cold Start Trap PDU
                        from: ###.###.###.###". Where ###.###.###.### is the doted decimal
                        notation of the IP address of the booting unit.
                        ::= { trapMsg 1 }

trapMsgNtpAlarm OBJECT-TYPE
        SYNTAX          DisplayString (SIZE (0..255))
        ACCESS          read-only
        STATUS          mandatory
        DESCRIPTION     This is an ASCII string sent to UDP port 162 (or user defined) when the
                        TrueTime time server's Leap Indictor is set to 3 (ie ntpSysLeap = 3). This
                        generally means the time server has lost primary time synchronization.
                        This could be due to a line breakage in the timing source, loss of GPS
                        satellites, etc. The message is "NTP Alarm Trap PDU from:
                        ###.###.###.###". Where ###.###.###.### is the doted decimal notation
                        of the IP address of the time server in the alarm state. See ntpSyncLeap
                        and ntpSysLeap.
                        ::= { trapMsg 2 }
```

trapMsgSnmpAuthFail OBJECT-TYPE

SYNTAX	DisplayString (SIZE (0..255))
ACCESS	read-only
STATUS	mandatory
DESCRIPTION	This is an ASCII string sent to UDP port 162 (or user defined) when the TrueTime time server determines the SNMP authentication for a SNMP PDU is in correct. The message is "SNMP Authentication Failure Trap PDU from: ###.###.###.###". Where ###.###.###.### is the doted decimal notation of the IP address of the unit attempting the invalid access.
	::= { trapMsg 3 }

-- the ntp group

The ntp group variables from 1 to 6 are general health variables on the NTP layer and variables 7 to 14 are culled from Dr. Mills' definition of sys variables in RFC 1305. Note: the NTP variables simplify because the TrueTime units are primary time servers. Variables used directly by NTP packets are provided in their raw forms.

ntpInPkts OBJECT-TYPE

SYNTAX	Counter
ACCESS	read-only
STATUS	mandatory
DESCRIPTION	Total number of NTP packets delivered to the NTP application layer from the transport layer.
	::= { ntp 1 }

ntpOutPkts OBJECT-TYPE

SYNTAX	Counter
ACCESS	read-only
STATUS	mandatory
DESCRIPTION	Total number of NTP packets passed from the NTP application layer to the transport layer.
	::= { ntp 2 }

ntpInErrors OBJECT-TYPE

SYNTAX	Counter
ACCESS	read-only
STATUS	mandatory
DESCRIPTION	Total number of NTP packets reject for any reason by NTP application layer.
	::= { ntp 3 }

```
ntpAuthFail OBJECT-TYPE
        SYNTAX          Counter
        ACCESS          read-only
        STATUS          mandatory
        DESCRIPTION     Total number of authentication failures.  This is a subset of ntpInErrors.
                        ::= { ntp 4 }

ntpDesiredAcc OBJECT-TYPE
        SYNTAX          INTEGER { (0..+2147483647) }
        ACCESS          read-only
        STATUS          mandatory
        DESCRIPTION     The desired (worst case time) accuracy in microseconds that the time
                        server will attempt to steer to.  This variable is related to ntpEstError.
                        Should ntpEstError be greater than ntpDesiredAcc, the NTP alarm
                        condition will be set (ntpSysLeap will be equal to 3).  Note:  outgoing NTP
                        packets will have their leap indicator field set to ntpSysLeap.
                        ::= { ntp 5 }

ntpEstErr OBJECT-TYPE
        SYNTAX          INTEGER { (0..+2147483647) }
        ACCESS          read-only
        STATUS          mandatory
        DESCRIPTION     The current estimated (time) error in microseconds of the time server.
                        This variable is related to ntpEstError.  Usually, this value is small and
                        constant for a given type of time server.  However, when primary
                        synchronization is lost, this value will slowly increase with time as the time
                        server's oscillator flywheels away from true time.  Should ntpEstError be
                        greater than ntpDesiredAcc, the NTP alarm condition will be set
                        (ntpSysLeap will be equal to 3).  Note: a primary time server's outgoing
                        NTP packets will have its leap indicator field set to ntpSysLeap.
                        ::= { ntp 6 }

ntpSysLeap OBJECT-TYPE
        SYNTAX          INTEGER {
                                No warning (0),
                                Last minute has 61 seconds (1),
                                Last minute has 59 seconds (2),
                                Alarm condition (clock not synchronized) (3)
                        }
        ACCESS          read-only
        STATUS          mandatory
        DESCRIPTION     This is a status code indicating normal operation, a leap second to be
                        inserted in the last minute of the current day, a leap second to be deleted
                        in the last second of the day or an alarm condition indicating the loss of
                        timing synchronization.  Note:  a primary time server's outgoing NTP
                        packet will have its leap indicator field set to ntpSysLeap.
                        ::= { ntp 7 }
```

```
ntpSysHostMode
        SYNTAX            INTEGER {
                                  reserved (0),
                                  symmetric active (1),
                                  symmetric passive (2),
                                  client (3),
                                  server (4),
                                  broadcast (5),
                                  reserved (6),
                                  reserved (7)
                                  }
        ACCESS            read-write
        STATUS            mandatory
        DESCRIPTION       The value of this variable indicates the mode that the host is operating in.
                            Note:  this is the value of the time server's outgoing NTP packet mode
                           field.
                          ::= { ntp 8 }

ntpSysStratum OBJECT-TYPE
        SYNTAX            INTEGER {
                                  unspecified (0),
                                  primary reference (1),
                                  secondary reference (2..255)
                          }
        ACCESS            read-only
        STATUS            mandatory
        DESCRIPTION       This is an integer that ranges from 1 to 255 indicating the stratum level of
                          the local clock.  Note:  a primary time server sets outgoing NTP packets
                          stratum field and ntpSysStratum to 1.
                          ::= { ntp 9 }

ntpSysPoll OBJECT-TYPE
        SYNTAX            INTEGER { (6..10) }
        ACCESS            read-write
        STATUS            mandatory
        DESCRIPTION       When the time server is in NTP broadcast mode, this is an integer
                          indicating the maximum interval between successive NTP messages, in
                          seconds to the nearest power of two.  For example a value of 6 means
                          2^6 or 64 seconds. Note:  a primary time server's outgoing NTP packet
                          will have its poll field set to ntpSysPoll.  Note:  this field is equal to 0 when
                          not in NTP broadcast mode.  Note, unless this is a time server initiated
                          NTP packet the value of the poll equals the value set in the in coming
                          packet.
                          ::= { ntp 10 }
```

ntpSysPrecision OBJECT-TYPE

SYNTAX	INTEGER { (-127..+127) }
ACCESS	read-only
STATUS	mandatory
DESCRIPTION	This is an integer indicating the ultimate precision of the synchronizing clock, in seconds to the nearest power of two. Note: a primary time server's outgoing NTP packet will have its precision field set to ntpSysPrecision.
	::= { ntp 11 }

ntpSysRootDelay OBJECT-TYPE

SYNTAX	COUNTER { (0..4294967295) }
ACCESS	read-only
STATUS	mandatory
DESCRIPTION	This is a raw 32 bit number representing a signed fixed point 32-bit number indicating the total round-trip delay to the primary synchronization clock source in seconds with the fraction point between bits 15 and 16. Note that this variable can take on both positive and negative values, depending on clock precision and skew. Note: a primary time server's outgoing NTP packet will have its root delay field set to ntpSysRootDelay.
	::= { ntp 12 }

ntpSysRootDisp OBJECT-TYPE

SYNTAX	COUNTER { (0..4294967295) }
ACCESS	read-only
STATUS	mandatory
DESCRIPTION	This is a raw 32 bit number representing a signed 32-bit fixed-point number indicating the maximum error relative to the primary reference source, in seconds with fraction point between bits 15 and 16. Only positive values greater than zero are possible. Note: a primary time server's outgoing NTP packet will have its root dispersion field set to ntpSysRootDisp.
	::= { ntp 13 }

ntpSysRefClockIdent OBJECT-TYPE

SYNTAX	DisplayString (SIZE (0..4))
ACCESS	read-only
STATUS	mandatory
DESCRIPTION	This is a four byte ASCII string identifying the particular reference clock. In the case of stratum 0 (unspecified) or stratum 1 (primary reference), this is a four-octet, left-justified, zero-padded ASCII string. While not enumerated as part of the NTP specification, the following are suggested ASCII identifiers:

Stratum	Code	Meaning
0	DCN	DCN Routing Protocol
0	NIST	NIST Public Modem
0	TSP	TSP Time Protocol
0	DTS	Digital Time Service
1	ATOM	Atomic Clock (calibrated)
1	VLF	VLF Radio (OMEGA, etc.)
1	callsign	Generic Radio
1	LORC	LORAN-C Radionavigation
1	GOES	GOES UHF Environment Satellite
1	GPS	GPS UHF Satellite Positioning
1	ACTS	ACTS Telephone Modem Dial-Up
1	IRIG	Inter-Range Instrumentation Group Signal

Note: for TrueTime time servers only GPS, ACTS and IRIG are presently used. Further, a primary time server's outgoing NTP packet will have its reference identifier field set to ntpSysRefClockIdent.
::= { ntp 14 }

-- the ntsControl group (Preliminary)

This group allows for complete control of TrueTime's products. This group emulates the serial function string commands described in TrueTime's operations manual. To configure the timeserver using the enterprise MIB, use the same syntax as the serial terminal FXX string. Where XX is the function number of the command. As an example, to find the trusted IP hosts for SNMP community one, you would type the following from the management station's command line:

#snmp -c system -h 199.37.0.21 set enterprise.1896.3.1.0 "F36C1IP"<Return key>
#snmp -c system -h 199.37.0.21 get enterprise.1896.3.2.0<Return key>
Response: "F36 C1 Trusted IPs: 199.37.0.26 199.37.0.24 0.0.0.0 0.0.0.0"

The -c command line switch specifies the community name and the -h switch specifies the IP address of the SNMP host agent. Note: the invocation of SNMP will vary from one operating system to the next, but this will give you the idea. Please note: the Enterprise OID addresses; these represent the input and output string buffers in TrueTime's Enterprise MIB and are formally defined below. The first SNMP set command places the function string into the timeserver's command buffer and the following SNMP get command reads the result of the set command. It is important to note that any TrueTime function string parameter can be issued using this method. Also note: that only one function string set may be issued at a time. Do not issue another until the response string is set to something other than an null string. Remember it takes time to process these commands and operating the commands in this fashion ensures that they perform without undesirable effects. Thus, the entire timeserver setup can be done with SNMP. If these commands are issued from a script or batch file, the setup procedure for an entire timeserver is repeatable and automatic. Another advantage of this facility is that the TrueTime Service Department can now help to check the configuration of a timeserver if it is connected to the Internet. As a security precaution, the timeserver can turn on/off the remote configuration feature only through the keypad.

```
ntpControlInput OBJECT-TYPE
        SYNTAX          DisplayString (SIZE (0..255))
        ACCESS          read-write
        STATUS          mandatory
        DESCRIPTION     This variable emulates TrueTime's serial function command strings.  The
                        same commands issued to the serial port can be sent to this string.  Use
                        this variable for SNMP sets of functions strings.  Note:  setting this
                        variable clears ntpControlOutput to the null string.  See ntpControlOutput
                        below.
                        ::= { trapMsg 1 }

ntpControlOutput OBJECT-TYPE
        SYNTAX          DisplayString (SIZE (0..255))
        ACCESS          read-only
        STATUS          mandatory
        DESCRIPTION     This variable emulates TrueTime's serial function command strings.  The
                        same commands issued to the serial port can be sent to this string.  This
                        variable holds the output result string from the last setting of the above
                        ntpControlInput variable.  Use this variable for SNMP gets of function
                        strings.  See ntpControlInpuut above.
                        ::= { trapMsg 2 }
```

-- gps group variables

The GPS group is present in all TrueTime network products. However, only products synchronized by GPS will have meaningful data in this group. This group reports on the number of satellites that are currently tracked, the current GPS tracking mode, the strongest signal strength of the tracked satellites in Trimble units, elevation of the GPS antenna in centimeters and the longitude and latitude of the GPS antenna in normalized binary units that can be easily converted to radians or degrees. GPS is a satellite base time synchronization source and it is the most accurate source of timing for TrueTime's NTS product line.

```
gpsGroupValid OBJECT-TYPE
        SYNTAX          INTEGER { (0..1) }
        ACCESS          read-only
        STATUS          mandatory for GPS capable units
        DESCRIPTION     A test flag indicating if data contained in this SNMP GPS group is valid or
                        not.  This flag equals 1 when GPS is used as the time synchronization
                        source and 0 for all other sources.
                        ::= { gps 1 }

gpsNumTrackSats OBJECT-TYPE
        SYNTAX          INTEGER { (0..8) }
        ACCESS          read-only
        STATUS          mandatory for GPS capable units
        DESCRIPTION     The number of GPS satellites tracked.
                        ::= { gps 2 }
```

```
gpsNumCurrentSats OBJECT-TYPE
        SYNTAX          INTEGER { (0..8) }
        ACCESS          read-only
        STATUS          mandatory for GPS capable units
        DESCRIPTION     Current number of GPS satellites used in position and time fix
                        calculations.  The number of satellites available depends on how long the
                        time server has been up, the time of day and the total amount of clear
                        sky as seen from the GPS antenna.  Because of the high frequency of
                        GPS radio signals, GPS antennas must have unobstructed line of sight
                        from the antenna to the satellite to receive data.
                        ::= { gps 3 }

gpsSatTrackMode OBJECT-TYPE
        SYNTAX          INTEGER {
                                Automatic Mode          (0),
                                Time Mode               (1),
                                Survey Static Mode      (2),
                                Survey Dynamic Mode     (3)
                        }
        ACCESS          read-only
        STATUS          mandatory for GPS capable units
        DESCRIPTION     Mode of operation for satellite tracking.  See section 3.20 of the users
                        manual for a complete description of these modes.  Generally, modes 0
                        and 1 are used for time applications.  Mode 2 is useful for more accurate
                        position information when the unit is stationary, or slowly moving and
                        Mode 3 is for accurate position information when the unit is moving
                        quickly.
                        ::= { gps 4 }

gpsSatMaxSigStrength OBJECT-TYPE
        SYNTAX          INTEGER { ( 0..30) }
        ACCESS          read-only
        STATUS          mandatory for GPS capable units
        DESCRIPTION     Strongest signal strength of all tracking satellites in Trimble linear units.
                        Generally, this number should be 4 or greater for good reception.
                        ::= { gps 5 }

gpsAltitude
        SYNTAX          INTEGER { (-2147483647..+2147483647) }
        ACCESS          read-only
        STATUS          mandatory for GPS capable units
        DESCRIPTION     Altitude of the GPS antenna in centimeters above, or below the WGS-84
                        reference ellipsoid.  The reference ellipsoid is a rotated ellipse that is
                        centered on the Earth's center of mass.  The surface of the ellipsoid is
                        not necessarily the same as sea level.  The ellipsoid surface may be as
                        much as 100 meters different from actual sea level.
                        ::= { gps 6 }
```

gpsLongitude

SYNTAX	INTEGER { (-2147483647..+2147483647) }
ACCESS	read-only
STATUS	mandatory for GPS capable units
DESCRIPTION	Longitude location of GPS antenna where: +2147483647 is maximum east longitude, -2147483647 is maximum west longitude and 0 is Greenwich England. To calculate the longitude in radians use the following formula (gpsLongitude * PI) / ((2^31)-1) = longitude in radians. For degrees: (gpsLongitude * 180) / ((2^31)-1) = longitude in degrees. Note: longitude varies from -PI to +PI in radians and -180 to +180 in degrees.
	::= { gps 7 }

gpsLatitude

SYNTAX	INTEGER { (-2147483647..+2147483647) }
ACCESS	read-only
STATUS	mandatory for GPS capable units
DESCRIPTION	Latitude location of GPS antenna where: +2147483647 is the North Pole, -2147483647 is the South Pole and 0 is the equator. To calculate the latitude in radians use the following formula (gpsLatitude * PI) / (2*((2^31)-1)) = longitude in radians. For degrees: (gpsLatitude * 90) / ((2^31)-1) = latitude in degrees. Note: latitude varies from -PI/2 to +PI/2 in radians and -90 to +90 in degrees.
	::= { gps 8 }

-- acts group variables

The ACTS group is present in all TrueTime network products. However, only products synchronized by ACTS will have meaningful data in this group. This group reports on the number and status of ACTS dial up modem calls. ACTS is a telephone modem dial-up time service that is not as accurate as GPS, but does not suffer from the antenna restrictions of GPS.

actsGroupValid OBJECT-TYPE

SYNTAX	INTEGER { (0..1) }
ACCESS	read-only
STATUS	mandatory for ACTS capable units
DESCRIPTION	A test flag indicating if data contained in this SNMP ACTS group is valid or not. This flag equals 1 when ACTS is used as the time synchronization source and 0 for all other sources.
	::= { acts 1 }

actsBaudRate OBJECT-TYPE

SYNTAX	INTEGER { (300), (1200) }
ACCESS	read-only
STATUS	mandatory for ACTS capable units
DESCRIPTION	Indicates the baud rate setting for the ACTS modem. The ACTS dial-up service accepts 300 or 1200 baud. Note: this is a rare case where faster is not better and 300 baud yields the best time accuracy.
	::= { acts 2 }

```
actsFailRedial OBJECT-TYPE
        SYNTAX          INTEGER { (0..+9999) }
        ACCESS          read-only
        STATUS          mandatory for ACTS capable units
        DESCRIPTION     When the dial-up session fails to connect this is the time in seconds to
                        wait to try again.
                        ::= { acts 3 }

actsMaxCallPeriod OBJECT-TYPE
        SYNTAX          INTEGER { (0..+999) }
        ACCESS          read-only
        STATUS          mandatory for ACTS capable units
        DESCRIPTION     This is the maximum time in hours the ACTS unit will wait between
                        successful calls to the ACTS service.
                        ::= { acts 4 }

actsPhoneNum OBJECT-TYPE
        SYNTAX          DisplayString (SIZE (0..25))
        ACCESS          read-only
        STATUS          mandatory
        DESCRIPTION     This is the phone number of the ACTS dial-up service, including any
                        prefixes needed to reach an outside line or international dialing.  Prefixes
                        are separated by a comma from the main phone number.
                        ::= { acts 5 }

actsNumberOfCalls OBJECT-TYPE
        SYNTAX          COUNTER { (0..4294967295) }
        ACCESS          read-only
        STATUS          mandatory for ACTS capable units
        DESCRIPTION     Number of times the time server has called the ACTS dial-up service -
                        weather the call was successful or not.
                        ::= { acts 6 }

actsGoodCalls OBJECT-TYPE
        SYNTAX          COUNTER { (0..4294967295) }
        ACCESS          read-only
        STATUS          mandatory for ACTS capable units
        DESCRIPTION     Number of times the time server called the ACTS dial-up service and
                        successfully received the time.
                        ::= { acts 7 }

actsBadCalls OBJECT-TYPE
        SYNTAX          COUNTER { (0..4294967295) }
        ACCESS          read-only
        STATUS          mandatory for ACTS capable units
        DESCRIPTION     Number of times the time server called the ACTS dial-up service and
                        something was not right.  This variable is the sum total of all other ACTS
                        failure types.
                        ::= { acts 8 }
```

```
actsFailedInit OBJECT-TYPE
        SYNTAX          COUNTER { (0..4294967295) }
        ACCESS          read-only
        STATUS          mandatory for ACTS capable units
        DESCRIPTION     Time server's internal modem failed to initialize.  If this is excessive, it
                        may indicate a time server hardware failure.
                        ::= { acts 9 }

actsNoDialTone OBJECT-TYPE
        SYNTAX          COUNTER { (0..4294967295) }
        ACCESS          read-only
        STATUS          mandatory for ACTS capable units
        DESCRIPTION     Time server's internal modem found no dial tone.  This may be caused by
                        a broken phone line to the time server.
                        ::= { acts 10 }

actsNoCarrier OBJECT-TYPE
        SYNTAX          COUNTER { (0..4294967295) }
        ACCESS          read-only
        STATUS          mandatory for ACTS capable units
        DESCRIPTION     Time server's internal modem found no carrier.  No modem was found at
                        the other end and maybe the phone number for ACTS is wrong.
                        ::= { acts 11 }

actsBusyLine OBJECT-TYPE
        SYNTAX          COUNTER { (0..4294967295) }
        ACCESS          read-only
        STATUS          mandatory for ACTS capable units
        DESCRIPTION     Time server's internal modem found ACTS line busy.
                        ::= { acts 12 }

actsNoAnswer OBJECT-TYPE
        SYNTAX          COUNTER { (0..4294967295) }
        ACCESS          read-only
        STATUS          mandatory for ACTS capable units
        DESCRIPTION     The remote ACTS mode did not answer the call.
                        ::= { acts 13 }

actsBadReply OBJECT-TYPE
        SYNTAX          COUNTER { (0..4294967295) }
        ACCESS          read-only
        STATUS          mandatory for ACTS capable units
        DESCRIPTION     The syntax of the reply from remote modem was incorrect, possibly due
                        to line noise.
                        ::= { acts 14 }
```

actsNoOnTimeMark OBJECT-TYPE

SYNTAX	COUNTER { (0..4294967295) }
ACCESS	read-only
STATUS	mandatory for ACTS capable units
DESCRIPTION	The reply from remote modem had no on time mark, possibly due to line noise.
	::= { acts 15 }