SNMP - Simple Network Management Protocol
(Beta Release Addendum)

SNMP Introduction

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.

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.

TrueTime SNMP Configuration

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 TureTime’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:

Key word (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 coldstart 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 TureTime's SNMP. Answering No will negate the changes.

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

Key word (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 coldstart 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 TureTime's SNMP. Answering No will negate the change.

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

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.

Configuration of SNMP Through the Keypad Interface

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.

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.

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 5 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 a 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.

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)

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.

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

ADDENDUM

MD5 AUTHENTICATION PROTOCOL FOR NTP PACKETS

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.

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 signatures using the key ID specified by the client request. If a packet does not send the correct authentication signature, it is silently dropped. In the near future, dropped authentication packets will be accumulated in an SNMP TrueTime enterprise MIB variable, *ntpMD5AuthFail* (OID address = 1.3.6.1.4.1.1896.2.4.0), that can be queried by an SNMP management station.

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 (a good practice anyway). 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. Further note: Security for any enterprise is normally breached through the lax application of procedures by the people overseeing the enterprise. In other words, a secure network is primarily dependent upon the trustworthiness, diligence, and training of the people operating the enterprise and less so on the equipment.

NTP MD5 KEY MAINTENANCE USING THE TRUETIME KEYPAD INTERFACE

To configure NTP MD5 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 NTP MD5 Auth* prompt is displayed. Press FUNC/ENTR to start configuration for NTP MD5. This takes you to the menu titled *MD5 Main Menu:*. There are three menu choices from this menu: 1) *Modify MD5 keys*, 2) *Output On/off,* and 3) *Back one menu*. Note for all TrueTime menus: the up and down arrow keys scroll through the list of menu items and FUNC/ENTR actuates the selected menu option.

Pressing FUNC/ENTR for the *Modify MD5 keys* option takes you to the menu where you may edit MD5 keys (or view them). *Output On/off* specifies a menu where you can enable NTP MD5 authentication for NTP packets broadcast by the TrueTime time server. Note: At this time, NTP broadcast is not yet available and this menu serves no useful purpose until that time. The *Back one menu* choice returns to the previous menu.

Pressing the *Modify MD5 keys* menu takes you to the *MD5 Edit Menu:*. In this menu you may choose: 1) *Edit a Key*, 2) *Add a Key*, 3) *Delete a Key*, 4) *Delete all Keys*, or 5) *Back one menu*. If you press *Edit a Key*, then you will be able to scroll through the list of all currently entered MD5 keys and up to sixteen key identifiers can be stored in sorted numerical order, plus a *Back one menu* entry that will take you to the *Modify MD5 keys* menu. Pressing FUNC/ENTR on a particular key identifier takes you to the prompt *ENTER MD5 key up to 31 ASCII char*. Pressing FUNC/ENTR again displays the current value of the MD5 key. You may use the up and down arrows to select the character value at a position in the MD5 string and the left and right arrows move to other character positions. Note: It is easier to edit the MD5 keys using the serial command. Pressing FUNC/ENTR accepts any changes and takes you to the *Save key edit?* prompt. Next, use the up and down arrows to select *Yes* or *No* and FUNC/ENTR to activate the command. Note: you can use the edit function to just view MD5 keys and select *No* when asked to save the key changes. Pressing *Yes* or *No* takes you back to the *MD5 Edit a Key:* menu and pressing *Back one menu* takes you back to the *MD5 Edit Menu:.*

In the *MD5 Edit Menu:,* selecting *Add a key* takes you to the menu where you may add a new MD5 key. Your first prompt is *Enter Key ID:* followed by the default value of 0000000001. You may edit the key ID in the range from 1 to 4294967295. Press FUNC/ENTR and when you finish with the key ID, you will see the *MD5 key up to 31 ASCII char* prompt. Press FUNC/ENTR again and you can enter the actual MD5 key as you would in the edit menu. Press FUNC/ENTR when done and you are taken to the prompt *Add this key?.* Select *Yes* or *No* in the same way you did for the edit menu and you can return to the *MD5 Edit Menu:* by pressing the *Back one menu* option. Note: Entering a key identification that is already in use effectively edits that key to the new value. Further note: The key list can have up to 16 MD5 keys.

Back in the *MD5 Edit Menu:* you can select *Delete a key* or *Delete all keys* to remove one or all MD5 keys. These menus operate in a similar fashion as the edit and add menus and they are protected

from accidental entry by yes or no menu confirmations. Further, you will not be allowed to enter these menus if there are no MD5 keys.

When you finish with the MD5 key tasks, you may leave the MD5 menus by successively pressing *Back one menu* or by pressing the STATUS key. Note: If you press the STATUS key, make sure that you have confirmed your last operation in the *Yes* or *No* menu appropriate for the operation, otherwise your last operation will have no effect.

NTP MD5 KEY MAINTENANCE USING THE TRUETIME SERIAL INTERFACE

The easiest method to maintain NTP MD5 keys is through the serial interface. This is due to the fact that MD5 keys are alpha/numeric strings and the keypad interface does not allow easy entry of alpha characters. You may add, delete and view the MD5 keys using the serial interface.

To view a 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

To view the 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.

To add a 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

To delete a 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

To delete all NTP MD5 Keys type:

F36 MD:ALL

The unit will respond with:

OK

SECTION XXVII

NTS-XL NETWORK TIME SERVER

SECTION ONE

GENERAL INFORMATION

1-1 INTRODUCTION

1-2 This manual section provides the user of the NTS-XL Network Time Server (87-6003) all of the information necessary to properly install, operate, and utilize its features.

1-3 The information in this manual section includes any normal maintenance and adjustment data that may be required to facilitate field repairs.

1-4 The purpose of the Model NTS-XL is to provide Internet Protocol (IP) network time synchronization, over Ethernet connected networks, via the Network Time Protocol (NTP) developed by Dr. David Mills at the University of Delaware. In providing this synchronization, the NTS-XL operates as a "server". The NTS-XL currently supports version 3.0 of the NTP, RFC 1305 as well as the Simple Network Time Protocol (SNTP), RFC1361. In addition, the NTS-XL will respond to TIME protocol requests, RFC868. Refer to Appendices A and B of this manual section for details regarding these protocols.

1-5 The NTS-XL obtains its timing information from the internal GPS-XL Module.

1-6 through 1-38 reserved.

1-39 INTERNAL TIMING PERFORMANCE SPECIFICATIONS

1-40 The absolute time and frequency characteristics of the NTS-XL are essentially those of the input synchronization source. The relative synchronization characteristics given here reflect the capabilities of the NTS-XL to preserve the time and frequency characteristics of the synchronization source being provided to the NTS-XL.

1-41 NETWORK TIME PROTOCOLS

1-42 The NTS-XL 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 of this manual section for detailed information regarding these protocols as implemented by the NTS-XL.

** The NTS-XL does not implement the "authenticator field" of the NTP packet.

1-43 NETWORK TIME PROTOCOL SYNCHRONIZATION SPECIFICATIONS

1-44 The NTS-XL hardware is designed specifically to implement the NTP server function. As such it was carefully designed to operate with the TrueTime 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-XL timestamp uncertainty.

1-45 INTERFACE SPECIFICATIONS

1-46 Ethernet Interface

Frame Format: DIX Ethernet (Ethernet II) or IEEE 802.3 with 802.2 headers
Connector: AUI, female 15-pin D subminiature

Pin Assignment

Pin	Assignment
1	GND
2	CI+
3	DO+
4	GND
5	DI+
6	GND
7	NC
8	GND
9	CI-
10	DO-
11	GND
12	DI-
13	+12V
14	GND
15	NC

SECTION TWO

INSTALLATION

2-1 OVERVIEW

2-2 The user must provide the NTS-XL with an Ethernet network connection and set-up parameters. The NTS-XL Network Time Server is capable of basic operation without any XL-DC KEYPAD or USER RS-232 connection once the essential network and operating parameters have been entered. The NTS-XL retains all configuration data in Electrically Erasable/Programmable Read Only Memory (EEPROM).

2-3 PROCEDURE

2-4 The NTS-XL plug-in module is mounted in the Model XL-DC provided by TrueTime and therefore obtains its power through the Model XL-DC. It is necessary only to make the network input to the NTS-XL. The network connection is made via the AUI connector and any required Media Access Unit (MAU, also known as a transceiver). Once these connections have been made, turn on the unit and follow the instructions below.

2-5 BASIC QUICK START INSTRUCTIONS

2-6 After powering up the XL-DC, connect a PC or other RS-232 terminal to the XL-DC USER port female DB9 connector. A null modem adapter is required.

2-7 Network configuration information must be sent to the NTS-XL using Serial I/O Function 36. The IP address, subnet mask, default gateway, and network packet type must be entered in order to interface with a network. See Section 3 for a detailed description of Serial I/O Function 36 and Appendix A for details of the NTP packet.

2-9 Verify that the XL-DC is running by starting Serial I/O Function 08, Continuous Time Once per Second. Send the string: F08<CR>. The days through seconds time being generated by the XL-DC will be output from the user port once per second. To stop the continuous output, send a CTRL-C to the USER port. The synchronization source is GPS, so allow at least five minutes for the XL-DC to acquire lock. Once the XL-DC is locked, the ? character in Serial I/O Function 08 will change to a space character.

2-10 Once the XL-DC is running properly, the unit should respond to PING, TIME, and NTP packets. If it does not, check the connection to the network and all Serial I/O Function 36 network configuration parameters.

2-11 QUICK START INSTRUCTIONS FOR MULTIPLE MODULES

2-12 If multiple NTS-XL modules are installed in the XL-DC, repeat steps 2-6 through 2-10 to configure the first NTS-XL module. **Note:** Each NTS-XL module requires a unique IP address and set-up address.

Set up the second card as follows:

1. Change the internal address by moving SW1-1 (DIP switch on PCB) to OFF (i.e., for Port 14 SW1-0 is OFF and SW1-1, 2, 3 are ON).

2. Set up the card via RS 232 by entering the following script (be sure to change the IP address [shown in italics] to the desired address). **Note: The default setting from the vendor is 15 or F** (for Port 15 SW1-0, 1, 2, 3 are ON).

F36 15, IP: *10.1.10.20* SM: 255.255.0.0 G:10.1.10.254

F36 14, IP: *10.1.10.21* SM: 255.255.0.0 G:10.1.10.254

To check the addresses you have entered, type in the following commands:

F36 15

and the display should show `F36 15, IP: 10.1.10.20 SM: 255.255.0.0 G:10.1.10.254`

F36 14

and the display should show `F36 14, IP: 10.1.10.21 SM: 255.255.0.0 G:10.1.10.254`

Note: The lowest address is displayed when only F36 is entered.

3. Test each card using Winsntp, or ping the IP address. Remember to change the IP address in Winsntp to test each card.

2-13 ADDRESS SELECT SWITCH

2-14 Four-position DIP switch SW1 selects the address (0 - 15) of the NTS card. If more than one NTS card is installed, a different address setting must be used for each card. The NTS card shares the same address range as "SmartCard" options. In applications where a "SmartCard" option is also installed in the system, a unique address switch setting for the "SmartCard" is required. In situations where a particular NTS card address is desired, it can be set into the SW1 DIP switch as follows:

SW1-3	SW1-2	SW1-1	SW1-0	Address (Port)	SW1-3	SW1-2	SW1-1	SW1-0	Address (Port)	
OFF	OFF	OFF	OFF	0	ON	OFF	OFF	OFF	8	
OFF	OFF	OFF	ON	1	ON	OFF	OFF	ON	9	
OFF	OFF	ON	OFF	2	ON	OFF	ON	OFF	10	
OFF	OFF	ON	ON	3	ON	OFF	ON	ON	11	
OFF	ON	OFF	OFF	4	ON	ON	OFF	OFF	12	
OFF	ON	OFF	ON	5	ON	ON	OFF	ON	13	
OFF	ON	ON	OFF	6	ON	ON	ON	OFF	14	
OFF	ON	ON	ON	7	ON	ON	ON	ON	15	(Default)

For example, set the NTS card address to 1 (SW1-0 ON, SW1-1, 2, 3 OFF). Setting the card address to 1 will allow a field installation of a "SmartCard", which has a default card address of 0. If more than one NTS card is installed in the system, set the SW1 switch on each of the cards to the next available address. Change addresses to something other than 0, which is reserved.

2-15 NTS KEYPAD SETUP

2-14 The NTS card(s) may be setup with keypad function 36. See Section 3-21 for details on setup for a single card and Section 3-22 for details on setup with two or more cards.

SECTION THREE

OPERATION

3-1 INTRODUCTION

3-2 The NTS-XL Module provides extremely accurate time over an Ethernet connection.

3-6 The NTS-XL module is synchronized by the use of the NAVSTAR Global Positioning System (GPS). This system requires no operator input to maintain accurate UTC time and automatically handles leap second events.

3-7 BASIC OPERATION

3-8 This Section provides a complete description of the basic operation of the NTS-XL.

3-9 NETWORK INTERFACE

3-10 TrueTime's NTS-XL module supports RFC-868, RFC-1305, and RFC-1361. An NTP or SNTP client daemon compatible with the user's computer platform is required for accurate network synchronization. The daemon must be told the NTS-XL IP address.

3-11 START-UP

3-12 On power up, the NTS-XL module will check its EEPROM for valid configuration data. If configuration data is valid and present, then the NTS-XL will attempt to synchronize its internal time to the GPS synchronization source.

3-13 Once the NTS-XL has synchronized to GPS, it will then be ready to respond to any requests that it receives over the network from supported protocols. During interruptions of the synchronization input, the NTS-XL will estimate the quality of the time it is able to provide to clients and update the fields of the NTP packet appropriately. In addition, the time quality character of the Serial I/O Function 08 string and the "worst case time error" reported by Serial I/O Function 13 are also updated during such interruptions. The NTS-XL will provide NTP server operation until the Serial I/O Function 13 "worst case time error" has exceeded the value of the Root Dispersion field set in the NTP packet. See Appendix A for details on this behavior.

3-14 GENERAL OPERATION

3-15 All functions are accessed via the XL-DC USER Serial I/O interface or the KEYPAD.

3-18 FRONT PANEL KEYPAD FUNCTION LIST

3-19 The Serial I/O Function 36 network configuration parameters will be described in this manual section. All other functions listed here can be found in manual section III of the main manual. Any of the following commands may be used:

COMMAND	FUNCTION
F01	Time Zone Entry/Request
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-XL Configuration Entry/Request
F66	Daylight Savings Enable

3-20 KEYPAD FUNCTION F36 - NTS-XL CONFIGURATION ENTRY/REQUEST FOR ONE CARD

3-21 Use Function F36 to set the network parameters of the NTS-XL unit. If multiple NTS-XL units are installed in the XL-DC refer to section 3-22.

Press “FUNC/ENTR”, then “3” ”6”. The display will show:

Display Ethernet
Address

Use the up and down keys to scroll among the major selections for Function F36: Display Ethernet Address, Clock Type, Display/Setup Network Type, Display/Setup Default Gateway, Display/Setup Subnet Mask and Display/Setup IP Address. Pressing "FUNC/ENTR" while the desired action is displayed allows the user to view and/or modify the NTS-XL parameters. (When modifying parameters it is normal that they are displayed slower than usual). At any time a major selection is displayed, the Up and Down arrow keys can be used to move to another major selection. This eliminates the need to view each of the Function F36 parameters if it is only desired to change one parameter.

Pressing "FUNC/ENTR" on “Display Ethernet Address” displays the Ethernet Address of the unit as shown here:

Company:00-A0-69 *(Fixed)*
Unit:00-00-0F *(Example)*

Press "FUNC/ENTR" to move onto the next parameter, or the “STATUS” button to exit function 36 without saving any updated settings.

Pressing "FUNC/ENTR" on “Display/Setup IP Address” allows the user to view and/or change the IP Address of the NTS-XL unit. The format of the IP Address display is shown here:

IP Address:
2255.054.000.034 *(Example)*

The Left and Right arrow keys move the cursor beneath the digits of the address. The Up and Down arrow keys or the number keys can be used to modify the address. Upon completion, use the "FUNC/ENTR" key to enter the address shown and proceed to the next parameter, “CLR” to restore the original setting, or “STATUS” to exit function 36 without saving any updated settings.

Pressing "FUNC/ENTR" on “Display/Setup Subnet Mask” allows the user to view and/or change the Subnet Mask of the NTS-XL unit. The format of the IP Address display is shown here:

Subnet Mask:
255.255.255.240 *(Example)*

The Left and Right arrow keys move the cursor beneath the digits of the mask. The Up and Down arrow keys or the number keys can be used to modify the mask. Upon completion, use the "FUNC/ENTR" key to enter the

mask shown and proceed to the next parameter, “CLR” to restore the original setting, or “STATUS” to exit function 36 without saving any updated settings.

Pressing "FUNC/ENTR" on “Display/Setup Default Gateway” allows the user to view and/or change the Default Gateway of the NTS-XL unit. The format of the Default Gateway display is shown here:

Default Gateway:
255.054.000.033 *(Example)*

The Left and Right arrow keys move the cursor beneath the digits of the address. The Up and Down arrow keys or the number keys can be used to modify the address. Upon completion, use the "FUNC/ENTR" key to enter the address shown and proceed to the next parameter, “CLR” to restore the original setting, or “STATUS” to exit function 36 without saving any updated settings.

Pressing "FUNC/ENTR" on “Display/Setup Network Type” allows the user to view and/or change the Network Type of the NTS-XL unit. The format of the Network Type display is shown here:

Network Type:
Ethernet II DIX *(Example)*

The Up and Down arrow keys toggle the Network Type between “Ethernet II DIX”, and “IEEE 802.3”. When the required type is shown, use the "FUNC/ENTR" key to enter the Network Type and proceed to the next parameter, “CLR” to restore the original setting, or “STATUS” to exit Function F36 without saving any updated settings.

Pressing "FUNC/ENTR" on “Clock Type” advances the display to the “Display Ethernet Address” display if no modifications were made. If any of the parameters were modified, the NTS-XL queries the user about saving the parameters, and, if necessary, rebooting the NTS-XL unit. The format of the Clock Type display is shown here:

Clock Type:
GPS *(Example)*

Press "FUNC/ENTR" to display the Ethernet Address of the NTS-XL.

3-22 KEYPAD FUNCTION F36 - NTS-XL CONFIGURATION ENTRY/REQUEST FOR TWO OR MORE CARDS

If multiple NTS-XL modules are installed, Function F36 will request the user to select the port for configuration.

Press “FUNC/ENTR”, then “3” ”6”. The display will show:

Select NTP
Port 1 *(Example)*

Use the up and down keys to scroll among the options until the desired port for configuration is displayed. For example, press the up key and the display will show:

Select NTP
Port 2 *(Example)*

Pressing "FUNC/ENTR" on “Select NTP” displays:

Display Ethernet
Address

The remainder of the process matches what is done with one card, so refer back to Section 3-21.

3-23 SERIAL I/O INTERFACE

3-24 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. The default factory settings for the Serial I/O port are:

Baud Rate: 9600
Parity: Even
Data Bits: 7
Stop Bits: 1

3-24 SERIAL I/O FUNCTIONS

3-25 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). The Serial I/O Function F36 network configuration parameters will be described in this manual section. All other Serial I/O Functions listed here can be found in manual Section 3. After a control-C character has been sent, any of the following commands may be used:

COMMAND	FUNCTION
F01	Time Zone Entry/Request
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-XL Configuration Entry/Request
F66	Daylight Savings Enable

3-30 through 3-89 reserved.

3-90 SERIAL I/O FUNCTION F36 - NTS-XL CONFIGURATION ENTRY/REQUEST

3-91 Use Serial I/O Function F36 to obtain information about the current NTS-XL configuration or to change the setup. Changing the network related fields of the configuration will cause a reset of the NTS-XL module.

3-92 **Ethernet Address** - The ethernet address is a six byte, hexadecimal value specific to each NTS-XL 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-XL is a fixed address established at the factory. To request the ethernet address of the NTS-XL 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.

3-93 **IP Address** - To obtain the IP address of the NTS-XL 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-XL, send a string of the form:

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

Ex: F36 IP:206.54.0.21<CR>

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

3-94 **Subnet Mask** - To return the subnet mask of the NTS-XL 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-XL, send the string:

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

Ex: F36 SM:255.255.255.240<CR>

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

3-95 **Default Gateway** - To obtain the default gateway of the NTS-XL 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-XL, send the string:

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

Ex: F36 G:206.54.0.17<CR>

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

3-96 **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 Ethernet II DIX networks the unit will respond: F36 N:E<CR><LF>
or
For IEEE 802.3 networks the unit will respond: F36 N:I<CR><LF>

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

For Ethernet II DIX networks send: F36 N:E<CR> (most Cisco switches require this setting)
For IEEE 802.3 networks send: F36 N:I<CR>

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

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

3-97 Complete NTS-XL Network Configuration - To review the entire current network configuration of the NTS-XL 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-XL 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-XL 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-XL 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-XL.

3-98 **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:

For GPS input operation:	**F36 T:GPS<CR><LF>**
For IRIG B input operation:	F36 T:IRIG<CR><LF>
For 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.

3-100 The GPS system broadcasts information on leap seconds several days prior to the event. Leap seconds are added (or subtracted) only at the end of the days June 30 and December 31. The NTS-XL will automatically place the appropriate information in the Leap Indicator field of the NTP packet on the day of the event. The NTS-XL will also perform the leap second correction at the appropriate time.

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 second 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-XL 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 or whenever the synchronization source (GPS) 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-XL will always set this field equal to 3.

A-4 Mode - The mode is a three bit integer that determines the functions the NTS-XL module will perform. TrueTime's NTS-XL 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-XL 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-XL 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-XL 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-XL 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 synchronization input option is GPS so the NTS-XL will self determine the accuracy. Once the accuracy has been determined, then the NTS-XL sets the root dispersion equal to ten times the square root of the sum of the squares of the precision and 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-XL 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-XL synchronization input option.

Local Source Input	Reference Identifier String
GPS	"GPS"
IRIG B	"IRIG"
1 PPS	"1 PPS"
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-XL 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-XL.

SNTP v 3.0 DATA FORMAT per RFC1361

When the NTS-XL 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-XL will set these 2 bits to either 0 (normal) or 3 (unsynchronized) only

A-3S Version Number - The NTS-XL 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-XL server host

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

A-14S Transmit Timestamp - This field is set to the time that the reply left the NTS-XL 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-XL 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.