



TYMSERVE™ 2100LD USER GUIDE

*Installing, Configuring, and Operating
the TymServe™ 2100LD Network Time Server*





TYMSERVE™ 2100LD USER GUIDE

*Installing, Configuring, and Operating
the TymServe™ 2100LD Network Time Server*



Legal Notices

Copyright 2002 Datum, Inc. All rights reserved. The distribution and sale of this product and guide are intended for the use of the original purchaser only.

DATUM, INC. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. IN NO EVENT WILL DATUM BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, COVER, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR DOCUMENTATION, EVEN IF DATUM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES ARISING FROM ANY DEFECT OF ERROR IN THIS PUBLICATION.

This product is classified by the U.S. Department of Commerce as Retail Product Encryption Software and is eligible for license exception ENC under sections 740.17 (A)(3) and (A)(4) of the Export Administration Regulations.

TymServe is a trademark of Datum, Inc. U.S. and Foreign Patents Pending. All rights reserved.

Microsoft is a registered trademark of Microsoft Corporation. Microsoft Windows, Microsoft Word, and Active X are trademarks of Microsoft Corporation. Java is a registered trademark of Sun Microsystems, Inc. Federal Express is a registered trademark of Federal Express Corporation. Adobe and Acrobat are registered trademarks of Adobe Systems Incorporated. RSA is a registered trademark of RSA Security, Inc. All other brand or product names are trademarks or registered trademarks of their respective companies or organizations.

This User Guide manual is provided to assist the user in the operation and maintenance of the supplied equipment or software. It is recognized that multiple copies of this manual may be required to support even a single unit and for this reason, permission is hereby granted to reproduce the supplied User Guide for the purpose stated above, provided that this notice is included as part of the copy. Additional copies are also available from Datum eBusiness Solutions for a nominal fee, or from our web site below.

In no case, however, does the supply of this User Guide or the granting of rights to reproduce it, grant any rights to use information contained within to reproduce the supplied equipment or software, either in whole or in part.

The equipment or software described in this manual have been developed solely at the expense of Datum and are proprietary. No unlimited rights in technical data are granted. Limited rights as per DFARS 252.227-7013 shall be effective for 10 years from the copyright date.

Contractor/manufacturer:

Datum eBusiness Solutions
10 Maguire Road, S-120, Lexington, MA 02421-3110 USA
(1)(781)372-3600
www.datum.com

February 2002



TYMSERVE™ 2100LD USER GUIDE

TABLE OF CONTENTS

Chapter 1: TymServe™ 2100 LD Network Time Server Overview 5

- Welcome and Overview 5
- TymServe Components 6
- About Time Synchronization 7
- Unpacking Your TymServe 10

Chapter 2: Installing Your TymServe 2100LD 13

- Quick Initial Setup 14
- Permanent Installation 19
- Configuration Methods 24

Chapter 3: TymServe 2100LD Operation and Time-Related Protocols 27

- TymServe Operation 27
- Time Distribution Model 28
- Time Protocols 29
- NTP Authentication 33

Chapter 4: Command Shell and Command Descriptions 37

- Shell Overview 37
 - Command Description 38
 - Network Directory 40
 - Timing Directory 50
 - Serial Directory 56
 - Utility Directory 57
 - Intrinsic Help 61
-

Chapter 5: SNMP Configuration and Control **65**

SNMP Configuration Overview **65**

Additional Stored MIB Variables **66**

MIB Compilation **66**

Chapter 6: FAQ and Troubleshooting **69**

Frequently Asked Questions **69**

Troubleshooting **73**

Appendix A: Data Sheet Specifications **77**

Appendix B: Input/Output Connectors **79**

TymServe 2100LD: Front and Rear Panels **79**

Pin Descriptions **80**

Appendix C: Firmware Upgrade **83**

Overview **83**

Before You Start the Firmware Upgrade **83**

Troubleshooting **85**

Appendix D: Datum MIB Extension **87**

Overview **87**

Appendix E: Glossary **105**

Time Glossary **105**

Appendix F: Declaration of Conformity **121**

Index **123**

Chapter 1: TymServe™ 2100 LD Network Time Server Overview

In This Chapter

This chapter gives an introduction to the TymServe™ 2100LD Network Time Server, and to various time concepts.

Welcome and Overview

The TymServe is a stand-alone time server that distributes time over a TCP/IP network, including the Internet, using the Network Time Protocol (NTP).

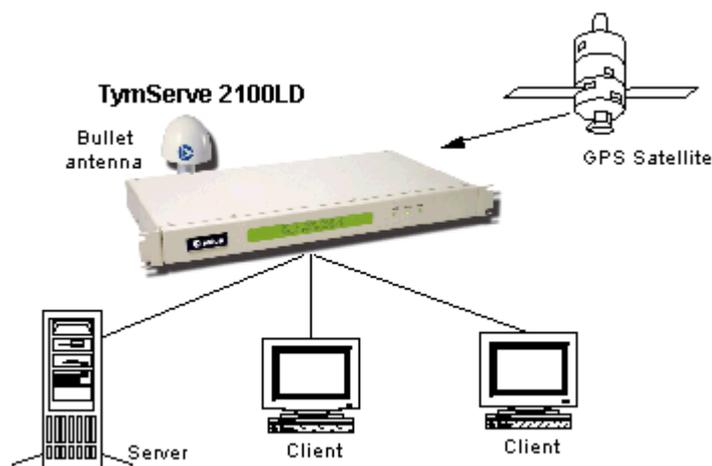


Figure 1-1 TymServe Distributing Time

The TymServe acts as a primary time server that broadcasts or responds to the specific time requests from client computers. In a client/server mode, the NTP client sends a time request packet to the server, the server affixes its current time and returns the packet, and the client software processes the time data to adjust its local clock.

The TymServe’s accuracy—meaning its ability to synchronize time over the network—is typically one to 100 milliseconds, depending on the network installation. The time is obtained directly from the Global Positioning System (GPS) satellite network. The time is adjusted, if necessary, by NIST to the correct international standard time, called Coordinated Universal Time.

TymServe Components

The following section gives an overview of the TymServe components.

Server

First: About Stratum Levels

Years ago, the telephone industry established hierarchical clock designs and terminology that the Network Time Protocol (IETF RFC 1305) is based upon. These hold that the accuracy of each server is defined by a number called its **stratum**. The highest level is 0; Stratum 0 devices, such as GPS or radio clocks, are connected to a primary time reference, such as the national atomic clock. Each level “away” from this primary time reference adds on another number. The Stratum of a primary server, which gets its time from, for example, a GPS, is assigned as 1. TymServe is such a device.

Devices that get their time from a Stratum 1 primary server via NTP are Stratum 2, Stratum 3, and so forth. A Stratum 2 or 3 Server simultaneously acts as a client, deriving its time via an NTP process with a Stratum 1 (or 2) Server, and acts as a server for clients further down the hierarchy.

Obviously, the further away a network is from the primary source, the higher the possibility of signal degradation because of variations in communication paths and the stability of the local clock.

Table 1-1: Stratum Levels: Summary

Stratum Level	Significance
Stratum 0	A primary time reference sourced from a National Measurement Institute such as NIST or UTC members such as the United States Naval Observatory (USNO)
Stratum 1	Derives its time from a primary time reference (Stratum 0) via GPS, dial-up, or radio clock
Stratum 2...n	A Stratum 2 (and so on) device derives its time from a Stratum 1 server, or other Stratum 2...n device via NTP

For additional details about stratum levels, check these web sites:

- <http://www.ietf.org/rfc/rfc1305.txt>
- <http://www.pasteur.fr/cgi-bin/mfs/01/10xx/1059?460>

TymServe's Server

As stated above, the TymServe is classified as a Stratum 1 Time Server. This means it derives its time from a Primary Time Reference (Stratum 0), such as a GPS satellite or a radio clock synchronized to national standard time.

NOTE: The TymServe is presently not designed to operate as a Stratum 2 (or 3) Server.

Client

Client NTP software varies widely, depending on the type of host and its operating system. Included with your TymServe is Datum's DatumTime™, a shareware program that runs on Win9x, Windows NT, and Win 2000 platforms. Other NTP client software can be used.

Global Positioning System

The U.S. Department of Defense Global Positioning System (GPS) is a constellation of 24 satellites that each orbit twice a day; their orbits are inclined 56 degrees to the equator. These satellites transmit signals that are used by the GPS receivers to very precisely determine the position and time. The GPS receiver in your TymServe tracks the satellites as they pass overhead, and determines the time and position from the satellites' range from the antenna.

The time is expressed as the number of weeks since midnight January 6, 1980 (GPS Week) plus number of seconds in the week. These two values are transmitted as binary integers from the satellites and converted into conventional date or day by the GPS receiver.

The orbits of these satellites and the offset (relative to international standard time, UTC) of their on-board cesium atomic clocks is precisely tracked by the US Air Force control network. Position and time correction information is uplinked from the ground control stations and maintained in the satellites in what is termed *ephemeris tables*, or tables of data that describe the satellite's position when compared to specified coordinates. Each satellite transmission reports the satellite's current position, GPS time, and the offset of the satellite's clock relative to UTC, international standard time.

About Time Synchronization

Time Standards

The international time standard is called Coordinated Universal Time or, more commonly, UTC. The designation "UTC" was chosen as a compromise among all the countries' abbreviations for Coordinated Universal Time. The UTC standard was agreed upon in 1972 by worldwide representatives within the International Telecommunication Union.

Time Synchronization and Business

Reliable time synchronization is essential for doing business today.

Ensuring all components of a network are synchronized to the global UTC time standard is critical for accurate time stamps, operational logs, and security applications. Many complex data processing tasks are dependent upon precise event sequences that are, in turn, dependent upon each sequence having a correct time tag.

By using something other than a dedicated time server, problems can arise, such as:

- Security risks: Users who retrieve time from an outside source, such as the Internet, are going outside your firewall.
- Bandwidth consumption: By attempting to synchronize time by using WAN (wide area network) links, users are consuming expensive bandwidth, which can also degrade time accuracy.
- Lost time: If your network synchronization relies on only one source for time reference, your network can be seriously compromised if that one connection is lost.

So how should you synchronize your network's time?

TymServe Solves the Problem

TymServe sets system time by providing a single, unbiased time reference that draws from multiple sources. All your computer networks are securely synchronized against this time reference. TymServe has the unique advantage of having its own high performance crystal or atomic clock. This way, you make sure NTP clients always receive accurate time, even if the GPS or other external time references become unavailable.

TymServe operates as a Stratum 1 time server, with accuracy to the nearest microsecond relative to UTC as maintained by the U.S. Naval Observatory.

Time is distributed within the network using the Network Time Protocol (NTP), and between multiple sites. The result is that with TymServe, network users can get time without breaching your firewall.

Full specifications are found in *Appendix A*.

Customer Solutions

You have purchased a fine product. You join others who have been using TymServes for log-file synchronization, network component synchronization, and server synchronization. This includes companies in:

- Defense
- Aerospace/aircraft manufacturing
- Health care/hospitals
- Regional telephone systems
- Networking hardware
- Data processing centers
- Internet service providers
- Express mail companies
- Telecommunications
- Software companies
- Banking
- Higher education

About This User Guide

This User Guide is designed for network administrators and others who have at least a basic understanding of network configuration and operation.

Table 1-2: Conventions Used in this Guide

Term	Definition
Bold	Boldface type is used for menu and command names; field, tab, and button labels; and special terms.
Courier	The <code>Courier</code> typeface is used to designate file names and folder names.
<i>Courier Italics</i>	Variables are in <i>Courier Italics</i> .
	The warning symbol alerts the user to information that if improperly used could be harmful to people, equipment, or data.

Additional copies of this *User Guide* are available at <http://www.datum.com/tymserve>, then click on **Download User Guide**.

Technical Support

Technical support for your TymServe is available through Datum Trusted Time Division at (781) 372-3600.

Unpacking Your TymServe

Unpack and inspect each item in the box. If there is any damage, or any items are missing, please contact Datum at (781) 372-3600 or (978) 927-8220 immediately.

The following items, pictured on the next page, should be included:

Table 1-3: TS 2100LD and Accessories

For the TymServe 2100LD-GPS
• TymServe 2100LD
• A/C Power Cord with US-style wall plug
• Utility CD (SNMP Customer MIB extension and DatumTime™ SNTTP client software)
• Antenna (Bullet II or optional High Gain)
• Antenna Mast - 40 cm aluminum mast threaded to screw into the bottom of antenna
• Mounting Bracket - for attaching mast to railing
• 50-foot standard RG58 (Belden 8240) or optional RG8 (Belden 9913) coaxial cable
• <i>User Guide</i> (this manual)

Tools Needed for Installation

The TymServe is easy to install. The only tools needed are a medium-sized slot-head (flat-head) screwdriver, and a wrench (1/2”).

Do Not Remove Case Cover

	<p>DANGER! <i>Under no circumstances</i> should you remove the cover of the TymServe. Not only would such an action disable the unit, it is extremely dangerous because of the electrical connections contained inside.</p> <p><i>Do not remove the TymServe cover!</i></p>
-------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Figure 1-2 TS 2100LD Antennas, Cables, and Accessories

Installation

Installation instructions are in [Quick Initial Setup and Permanent Installation: A Preview on page 13](#)

Chapter 2: Installing Your TymServe 2100LD

In This Chapter

This chapter reviews Quick Initial Setup, Permanent Installation, and initial configuration of your TS2100LD.

Quick Initial Setup and Permanent Installation: A Preview

Table 2-1: Quick Initial Setup and Permanent Installation

Description	Quick Initial Setup	Permanent Installation
Installation Type	Place TymServe on the desk close to your desktop or laptop computer	Mount TymServe on 19-inch rack close to TCP/IP network
Antenna	Run it outside the building or set it close to a glass window with a view of the sky	Do a rooftop installation with mast and cable
Setup Computer	Use RS-232 with HyperTerminal in Windows/NT desktop or laptop computer	Use a VT100 ASCII Terminal via serial interface on any compatible host of Telnet Connection after the Quick Initial Setup
Setup Commands	These commands are: IP Address, Net Mask, Default Route, and Time Source	Follow the same steps as Quick Initial Setup, plus set of commands as described in Chapter 4 of this User Guide
Client Synchronization	Use DatumTime™ SNTP client software for Windows/NT. This software is included in the Utility CD provided with TymServe	Use DatumTime utility or download NTP Client software from an NTP Internet Site. This software may require support from your IT group for configuration

Quick Initial Setup

If you want to do a quick install of your TS2100LD in order to verify its operation with known client software, follow these steps before doing the permanent installation.

NOTE: The configuration of network and timing that is performed during the Quick Initial Setup is also required for the Permanent Installation.

Cutting to the Chase: Quick Initial Setup, Easy Steps

1. **Place** the TymServe anywhere convenient, **attach** antenna cable and power input. *Do not* connect the TymServe to your network just yet.
2. **Switch on** the power.
3. Using the computer that manages the TymServe, and the RS-232 cable and HyperTerminal, enter the IP, subnet mask, and gateway addresses that your network administrator has given you.
4. You are finished for now.

Quick Initial Setup, Details:

1. After unpacking the standard antenna, **remove and discard** the rubber washer covering the terminal threads.
2. **Connect** the coaxial antenna cable directly to the bottom of the antenna. If you are using the optional Belden 9913 cable, use the adapter cable. An illustration of cable connections is in Figure 2-1.

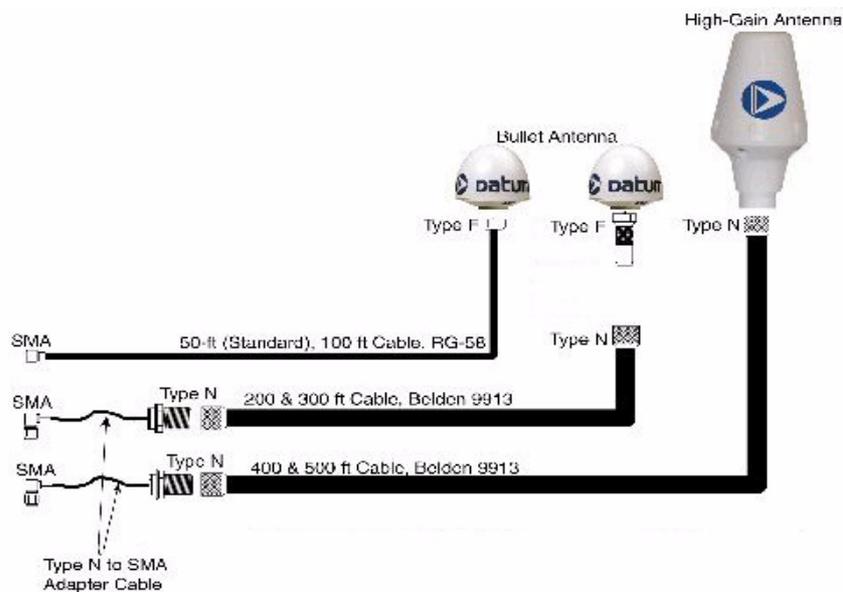


Figure 2-1 Antenna and Cable Options

- Position the antenna outside the building, or inside the building very close to a window with a view of the sky. (If you are using the mast, pass the Type F connector end of the antenna cable through the antenna mast, then connect it with the bottom of the antenna.)

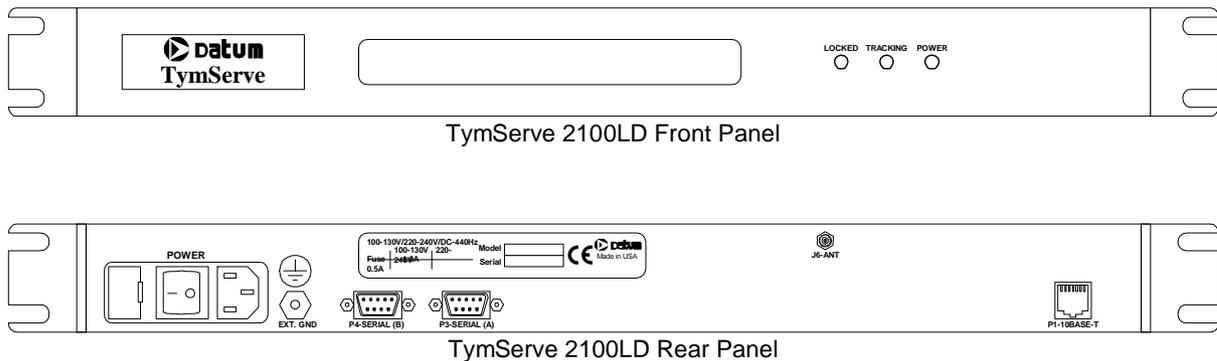


Figure 2-2 Front and Rear Views of TymServe 2100LD

- Connect the other end of the antenna cable to J6 (SMA connector) on the back of the TymServe.
 - Connect the setup computer to P3 Serial Port (A) of the TymServe, with a **straight-through** RS-232 serial cable (a standard serial cable).
- NOTE:** It is very important to use a straight-through antenna. Sample configurations follow later in this chapter.
- Connect the TymServe from the RJ-45 connector to the TCP/IP network through Ethernet 10baseT twisted pair cable. If the connection is made directly to the computer, use cross-over 10baseT cable. Otherwise, use an Ethernet hub for connections.
 - Attach the included power cable and connect to the back of TymServe and turn the power on. The green **Power** light should come on.

Next, establish a serial connection between the setup computer and the TymServe:

- On the computer, Click **Start->Accessories->HyperTerminal**
- Double-click `Hypertrm.exe`.
- In the **Connection Description** dialog's **Name** field, enter a name of your choosing.
- Click **OK**.
- In the **Phone Number** dialog's **Connect Using** area, select **com Port number**.
- Click **OK**.

7. In the **Com1 Properties** dialog, enter the following Port Settings information:

Port Setting:	Enter:
Bits per second:	9600
Data bits:	8
Parity:	none
Stop bits:	1
Flow Control:	Xon/Xoff

- 8. Click **OK**.
- 9. The TymServe interface displays (see Figure 2-3).
- 10. Press the **Enter** key twice to see the **?** mark. This indicates that the serial connection with the TymServe is established and the unit is ready for initial configuration.

NOTE: Telnet commands are detailed in Chapter 4 of this *User Guide*.

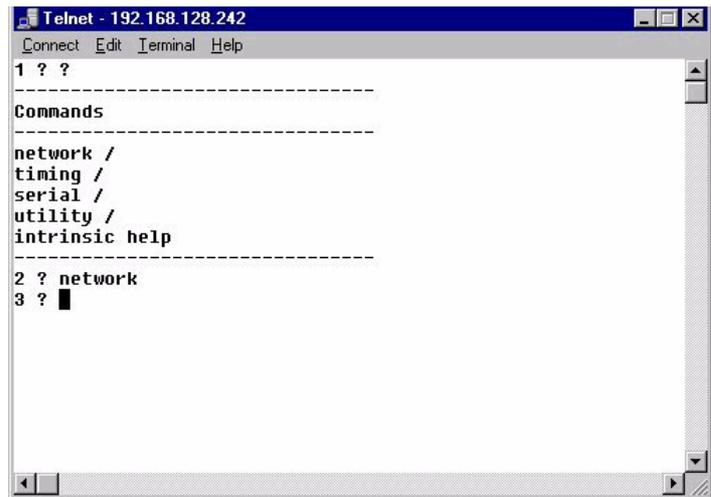


Figure 2-3 (Shell) TymServe Interface

Initial Configuration of the TymServe

Using the interface, configure the following network and timing parameters:

- 1. **Enter** IP address.
- 2. **Enter** Subnet mask.
- 3. **Enter** Default gateway for the devices on a different subnet.
- 4. **Enter** Timing Source: Mode 6

NOTE: Datum recommends that you make a note of these parameters for future reference and for the Permanent Installation.

Acquiring the Satellite Signals

After the initial configuration, the TymServe will seek, or *track*, the satellite signals.

You will know the TymServe is tracking the satellite signal because the **Tracking** light on the front of the TymServe is on. Tracking can take 5-30 minutes.

And after the Tracking light comes on, it may take another 15-30 minutes for the internal oscillator to stabilize. Once it is stabilized, the **Locked** light on the front of the TymServe comes on.

With all three LEDs on—Power, Tracking, Locked—the unit is ready to distribute time.

Testing Functionality

Once the TymServe is tracking, you need to

- Install the Datum Time Utility software, and
- Check the functionality of the Network Time Protocol (NTP).

To check the functionality of the NTP, first check the Ethernet connection between the TymServe and the client computer:

1. Call up the client computer's command prompt.
2. Enter ping command to verify that the TymServe is visible on the network.

Example: ping ip address of the TymServe

3. Press **Enter**

If there is an affirmative response, the TymServe is visible.

NOTE: If there is no response, then troubleshoot and fix the connection problem before checking the functionality of the TymServe on the network.

The DatumTime™ Time Utility

The DatumTime time utility is a handy way of keeping accurate time on your client computer.



Figure 2-4 DatumTime

To install DatumTime, see the following instructions.

To install the DatumTime™ software:

1. On the client computer's hard drive, create a separate directory for DatumTime.
2. Copy the Datumtime.exe file from the utility disk into this directory.
3. Double-click Datumtime.exe. This will install the program onto your computer.
4. Configure the clocks the way you want by clicking on the build tool in the lower right corner of the clock panel.
5. Right-click on the displayed clocks for the menu, and select **Server Options**.
6. Select the **Active Server** you wish to use to obtain your time.
7. Click **OK**.

To synchronize DatumTime:

1. Right-click anywhere on the clock panel to get to the menu. Select **Sync Options** to tell your computer when to automatically get time from the TymServe.
2. Enter the parameters you want.
3. Click **OK**. Now DatumTime will synchronize your time at those intervals.

Typical Connection for TymServe

The TymServe is most often connected like this:

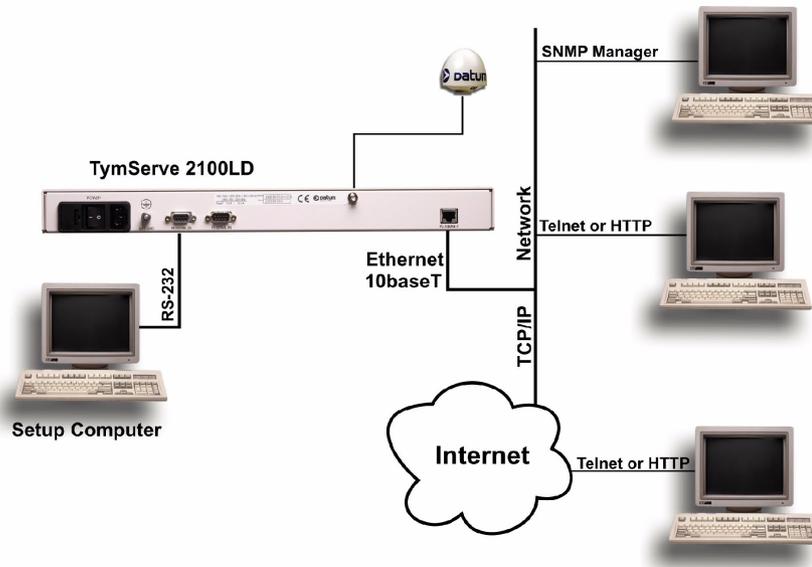


Figure 2-5 Typical Connection for TymServe 2100LD

What's Next

Now that you have completed the Quick Install, and verified the TymServe's operation, continue on to the Permanent Installation.

Permanent Installation

TymServe's Permanent Installation procedure assumes you have completed the Quick Initial Setup, and that you have verified its functionality. The steps for Quick Initial Setup are at the beginning of this chapter of this *User Guide*.

To do the Permanent Installation:

1. **Power off the unit**, then **disconnect** the following from TymServe:
 - Antenna cable
 - RS-232 serial cable
 - 10baseT Ethernet cable
 - Power cable
2. **Install and secure** the TymServe in the rack with the screws.
3. **Connect** the 10baseT twisted pair Ethernet cable from the RJ45 connector of the TymServe to the network.
4. **Install and connect** the antenna, if you have not already done so.
5. **Connect** the GPS antenna cable to the back of the TymServe. For more details on this, please refer to the Antenna and Cable Installation section later in this chapter.
6. After the physical installation, **connect** the TymServe to the A/C power supply.
7. **Turn on** the power. The **Tracking** light will turn on in about 15-30 minutes, and the **Locked** light will turn on when the internal oscillator stabilizes, in another 15-30 minutes.

Now the TymServe is ready to be configured.

NOTE: The TymServe is shipped from the factory with the Dynamic Host Configuration Protocol (DHCP) option turned off. If the IP address is dynamically obtained from the DHCP server, note this address for establishing the Telnet session.

Installing the GPS antenna and lightning arrester

This is the best way to install the GPS antenna with optional lightning arrester:

1. Slide the antenna mounting pole down over the antenna cable that is attached to one side of the lightning arrester, so that the cable passes through the center of the pole.
2. Take the end of the cable that has passed through the pole and screw the antenna onto the cable by turning the antenna.
3. Screw the antenna down on the mounting pole by turning the pole.
4. Use the saddle straps to mount the antenna mast in an area where the antenna has a 30 degree view of the horizon, as measured from the horizon (0 degrees) up to a 30 degree angle.
5. Mount the lightning arrester case onto a grounded object or attach a ground strap to the device.
6. After running the cable from the TymServe location to the lightning arrester, attach the cable to the lightning arrester.

Some suggested TymServe configurations follow.

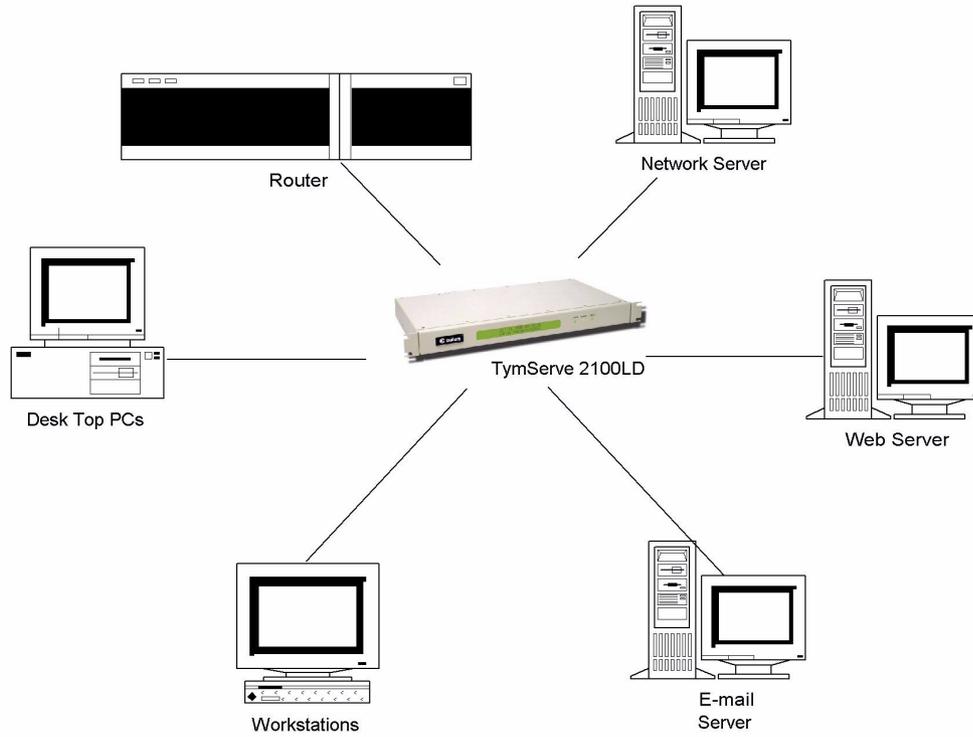


Figure 2-6 TymServe, as Stratum 1, synchronizing all network devices

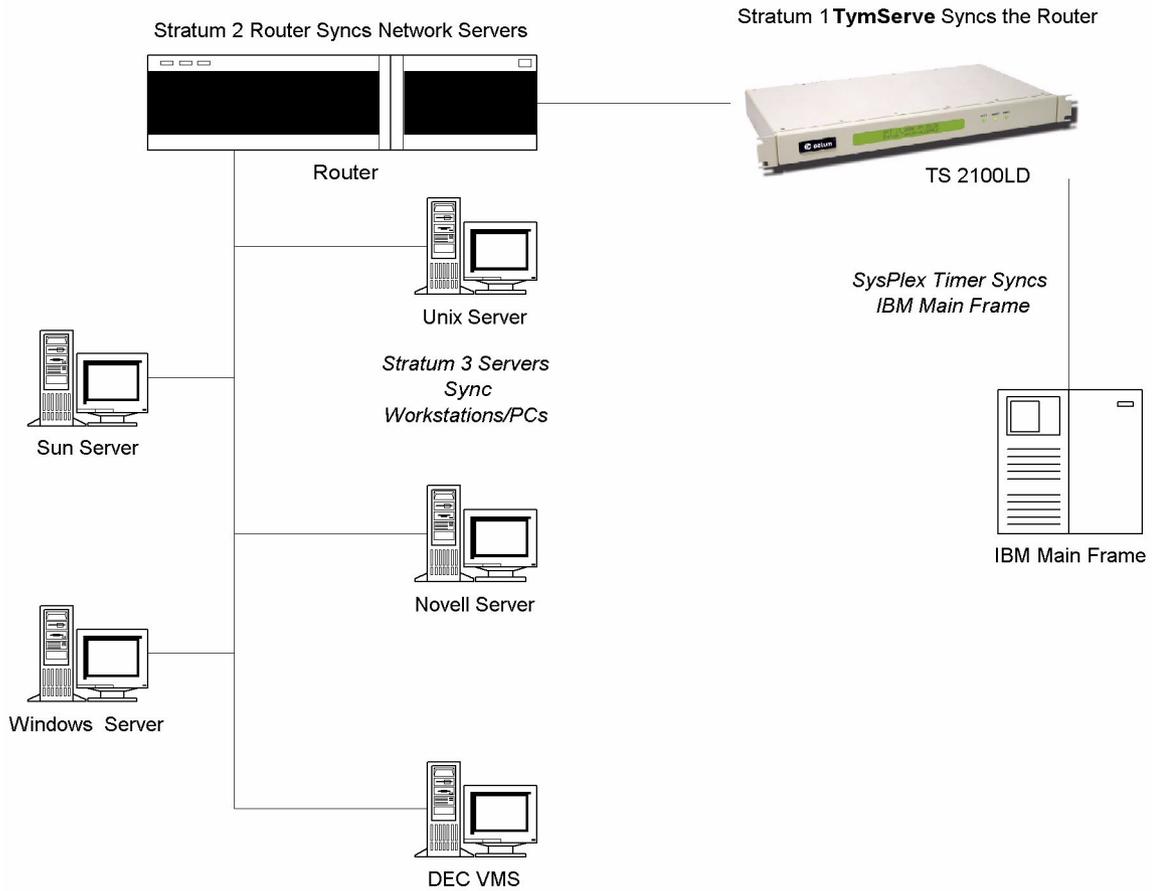


Figure 2-2 TymServe as Stratum 1 device with Stratum 2...n devices

A Word about NTP Client Software

Since this *User Guide* covers only the installation and basic configuration of the TymServe, NTP Client software is not discussed. We recommend you use DatumTime™ Utility, which is included with TymServe. However, you can find information about NTP Client software and its configuration at:

- <http://www.eecis.udel.edu/~ntp>
- <http://www.microsoft.com/NTServer/nts/exec/vendors/freeshare/IClient.asp>

Also, your favorite search engine can turn up other sources.

Antenna Installation: GPS

Antenna placement and cable routing are the most demanding aspects of installing a GPS-based instrument. For more details, please see Datum's *TS 2100LD GPS Installation Guide*.

The bullet antenna provided with the TymServe has a weatherproof housing, suitable for permanent installation in an outdoor location.

NOTE: If the antenna has to be installed in a partially enclosed environment, test it for functionality before you permanently install it.

Best Location

The Global Positioning System (GPS) of 24 satellites are in orbits inclined 56 degrees to the equator, each orbiting the earth twice a day. This angle means that the further north you are in the northern hemisphere, the more probable it is that satellites will be passing to the south of you. And if you are in the southern hemisphere, the satellites will be passing to the north of you. Please consider this as you install your antenna.

The antenna should be located with an unobstructed, clear view of the sky for optimum tracking conditions. The antenna can receive satellite signals through glass, canvas, or thin fiberglass. The satellite signals cannot penetrate foliage, or dense wood or metal structures. The antenna's operation is not affected if it is partially covered with snow, provided the snow is dry and does not form a continuous ice sheet on the surface. The shape of the bullet antenna is designed to prevent accumulation of rain, snow, or ice on its surface.

The GPS transmission is a 1.5 GHz (L1 Band) spread-spectrum signal. Being spread-spectrum means it is relatively immune to interference. But high energy sources, especially those with significant in-band energy, can swamp the receiver's radio frequency (RF) processing circuitry. In addition, it is difficult to operate GPS at power substations or in close proximity to high-voltage 60 Hz sources. Datum offers an optional high gain antenna that is useful in these heavy interference situations. Still, it is best to locate the antenna away from radiating sources so you can avoid degradation in antenna performance.



WARNING: Do not cut the cable to a shorter length. Instead, bundle any excess cable. Correct antenna cable length—even if you do not “use it all”—is critical to proper TymServe operation, which should have a gain within the range of 15dB–25dB.

Outdoors: Install the antenna, using the mast and mounting brackets, with a clear view of the sky, and away from radio frequency interference. It should be mounted vertically, in a location with an unobstructed view of 30° of the horizon. Be sure to position it at least two meters from other active receiving antennas, and shield it from transmitting antennas.

Indoors: Install the antenna by placing it near a window with a clear view of the sky, and away from radio frequency interference. Reflective window coatings will not only reflect sunlight, but the GPS signal as well, so you can expect lower performance if you have reflective or heavy tinting on your office windows.

While Datum does not recommend indoor installations, we understand that this may be the only option available to some customers. In such a case, it is best to temporarily install the antenna along a window to verify performance, before making such a configuration permanent.

Cable Signal Losses

The following table summarizes the calculated signal losses for different types and lengths of cables you can use with the antenna.

NOTE: For reliable operation of the TymServe, the signal level at the input of the TymServe must be between 15dB and 25dB.

Table 2-3: GPS Cable Configuration/Signal Losses

Component Description (dB)	Cable Length ¹					
	50 ft ²	100 ft	200 ft	300 ft	400 ft	500 ft
Standard Bullet Antenna (dB)	35	35	35	35		
Hi Gain Antenna (dB)					50	50
Internal GPS Cable (dB)	-0.5	-0.5	-0.5	-0.5	-0.5	-0.5
BNC/N Adapter Cable (dB)		-0.5	-0.5	-0.5	-0.5	-0.5
Bias T (DC Block) (dB)					-1.0	-1.0
Belden 8240 Standard RG 58 (dB)	-9.5					
Belden 9913 Cable (dB)		-5.6	-11.2	-16.8	-22.4	-28.0
Gain at Receiver (dB)	25	28.4	22.8	17.2	25.6	20.0

¹For cable lengths >500 feet, contact Datum ²Standard Cable

Configuration Methods

There are these access methods for configuring the TymServe 2100LD:

- RS-232 Serial Port B
- Telnet
- SNMP

RS-232 Serial Port B

The standard DTE style RS-232, DB9 (female) connector provides the preferred method of initial configuration and setup of the TymServe through a VT100 ASCII terminal using 9600, 8 N, and 1 for communication parameters.

Flow control is accomplished by the use of software Xon/Xoff. This method of access uses the Command Shell explained in [“Shell Overview” on page 37](#) This access method is not password protected.

Telnet Access

To use the Telnet access, first configure the network parameters, such as IP address, mask, default route, through the RS-232 Serial Port B as explained in the initial setup.

To establish a Telnet connection:

1. At the DOS or Windows command prompt, enter `telnet <IP address of the TymServe>`
2. Press **Enter**.

An alternative is to use any of the standard Telnet utilities. Navigating the Telnet command session is identical to the method used by the RS-232 access method.

The figure to the right shows a Telnet session.

The Telnet interface can be password protected. The password can be disabled only through the RS-232 Serial Port. If the user forgets the Telnet password, then it must be changed through the RS-232 port.

Telnet access uses port 23.

The TymServe allows only one Telnet session at a time.

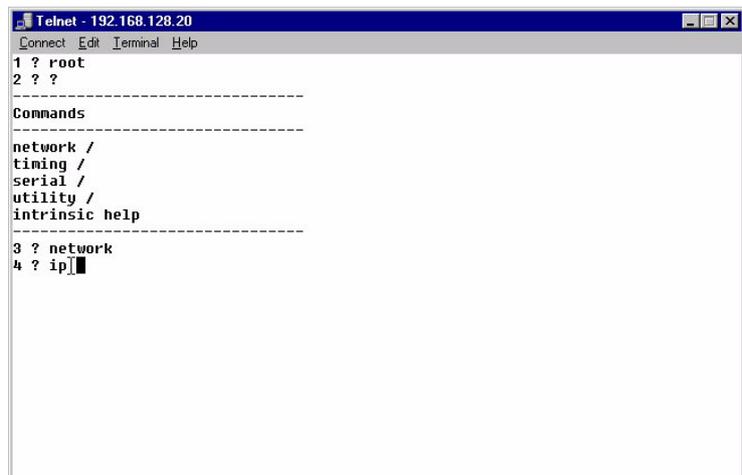


Figure 2-7 Telnet Session in Progress

If the unit is not disconnected properly, the previous Telnet session will be timed out and disconnected after one hour.

To disconnect the Telnet session:

1. In the command line, enter `exit`.
2. Press **Enter**.

The Telnet interface can be further protected by disabling the Telnet Server daemon. Refer to the `auto` and `stop` commands in Chapter 4, [page 38](#), for more details.

SNMP Access

The TymServe provides various remote features like configuration, status, and management control through the Simple Network Management Protocol, SNMP version 1 (RFC1157). In order to use SNMPv1 set and request packets, the network parameters must be configured. Once the network parameters are set, the packets can be sent to configure the operating mode of the unit. For more details about Datum MIB Extension, MIB compilation, and security aspects of SNMP, see [“Chapter 5: SNMP Configuration and Control” on page 65](#), and [“Appendix D: Datum MIB Extension” on page 87](#).

Internet HTTP Access

The basic operating status of the TymServe can be viewed from the HTML custom page over the HTTP protocol, by entering the IP address of the TymServe on the network as shown in the figure here. The status screen also provides the time of the local host.

This access shows the satellites that your TymServe is tracking.

NOTE: For security purposes, there is no management from this screen. Only information is displayed.

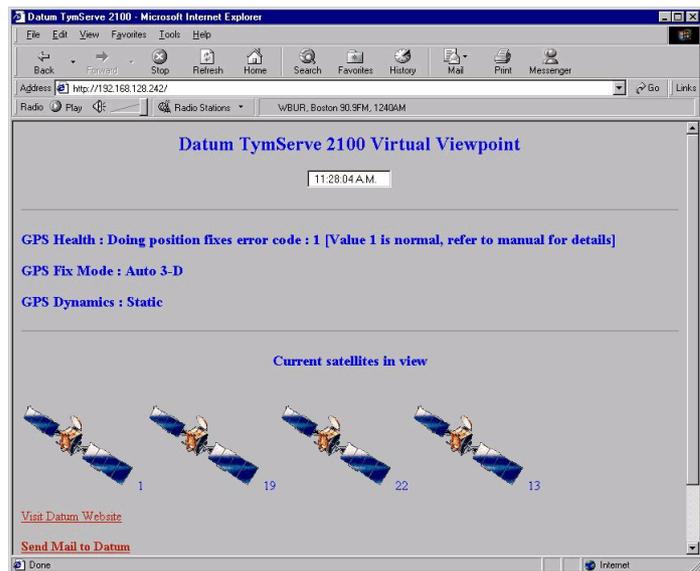


Figure 2-8 Sample Web Page View

Chapter 3: TymServe 2100LD

Operation and Time-Related Protocols

In This Chapter

This chapter describes server operation and time-related protocols.

TymServe Operation

TymServe and Time Distribution

Time is distributed over an IP network by Network Time Protocol (NTP), Simple Network Time Protocol (SNTP), Time Protocol, and Daytime Protocol over TCP/IP or through a Sysplex Timer via Serial Port A.

Once the TymServe is locked with its time source, it will continuously provide time even if the timing signal is lost. When the GPS time signal is lost, the Tracking and Locked lights will turn off, and the unit will run in the Freerun mode, meaning it will maintain the time with its own internal clock. The NTP message returned by the TymServe will indicate—via the Reference Timestamp—when it last obtained time updates from the timing signal.

The TymServe maintains the year value as a four-digit number. It also recognizes leap years.

TymServe and Client Software

Client software should be installed on the client machines before the NTP daemon can maintain the time synchronization with the TymServe.

The clients that need to be synchronized should be running a copy of the public domain NTP daemon or other equivalent client software. If an NTP daemon is not available on your system, you can obtain a copy of RFC 1119 from the Network Information Center (NIC) via FTP, in order to implement an NTP daemon for your system. Details of the NTP protocol and synchronization techniques are not discussed in this *User Guide*, but can be found at:

- <http://www.ietf.org/rfc/rfc1305.txt>
- <http://www.pasteur.fr/cgi-bin/mfs/01/10xx/1059?460#mfs>

TymServe and the Global Positioning System

The Global Positioning System (GPS) receiver in your TymServe tracks the 24 GPS satellites as they pass overhead during the day.

The TymServe also determines the range of the satellite in relation to its antenna. There are four unknowns about location of the satellite, and what they roughly represent, are:

- x, or latitude
- y, or longitude
- z, or altitude
- t, or time

Knowing the range from one satellite places you on a sphere. Two satellites show the intersection of two spheres, roughly a circle. Three satellites show two points. And four satellites show the complete four-variable solution.

However, once x, y, and z are known, only one satellite is needed to solve for time (t). This is due to one of the following: either the receiver has tracked at least four satellites and has positioned itself, or the user has entered a known position into the TymServe.

Thus the TymServe antenna still works—and TymServe can still source time—in areas with a somewhat restricted view of the sky, such as in cities.

Time Distribution Model

Network time distribution systems usually use a hierarchical time distribution model, as illustrated in Figure 3-1.

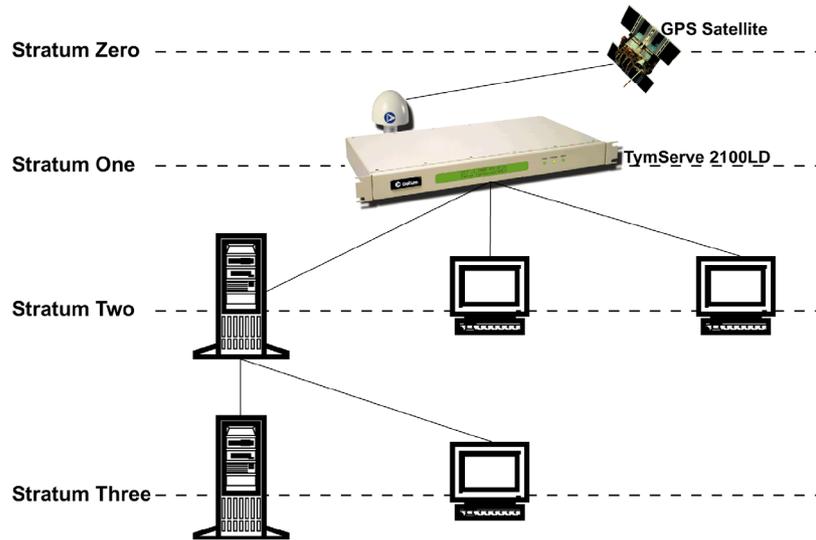


Figure 3-1 Time Distribution Hierarchy

In hierarchical systems, the primary time source clocks are considered Stratum 0 (zero) which includes GPS satellites and time sources at the United States Naval Observatory (USNO), National Institute of Standards and Technology (NIST), or other national time standards organizations.

The TymServe acts as a Stratum 1 time server that derives its time from the GPS satellites and distributes this time through TCP/IP network or Sysplex Timer to the computers. The client computers may act as Stratum 2 time servers and distribute time to Stratum 3 computers as shown in Figure 3-1.

Time Protocols

Time Protocol (RFC 868)

This protocol provides a site-independent, machine-readable date and time. The time service on the TymServe responds to the originating source with the time in seconds since midnight of January 1, 1900. The time is the *number of seconds* since 00:00 (midnight) January 1, 1900 GMT. So the time “1” is 12:00:01 A.M. on January 1, 1900 GMT. This base will serve until the year 2036.

If the server is unable to determine the time, it either refuses the connection or it closes the connection without sending any response.

When used over the Transmission Control Protocol (TCP), the TymServe listens for a connection on port 37; once the connection is established, the server returns a 32-bit time

value and closes the connection. When used over the User Datagram Protocol (UDP), the TymServe listens for a datagram on port 37. When a datagram arrives, the TymServe returns a datagram containing the 32-bit time value.

Daytime Protocol (RFC 867)

The Daytime protocol sends the current date and time as a character string without regard to the input.

When used over TCP, the TymServe listens for a connection on port 13; once a connection is established the current date and time is sent out as an ASCII character string. The service closes the connection after sending the quote.

When used over UDP, the TymServe listens for a datagram on port 13. TymServe responds to the UDP request with the current date and time as an ASCII character string.

Simple Network Time Protocol (RFC 1361/2030)

Simple Network Time Protocol (SNTP) is a simplified access protocol for servers and clients using NTP as it is now used on the Internet. The access paradigm is identical to the UDP/Time client implementation. SNTP is also designed to operate on a dedicated server configuration, including an integrated radio clock. SNTP uses the standard NTP time stamp format described in RFC 1305 and previous versions of that document. NTP stamps are represented as a 64-bit unsigned, fixed-point number, in seconds relative to 0^h on January 1, 1900.

Network Time Protocol (RFC 1305 and RFC 1119)

The Network Time Protocol (NTP) is used to synchronize computer clocks in the TCP/IP computer network. It provides a comprehensive mechanism for accessing national time and frequency distribution services, for organizing the time-synchronization subnet, and for adjusting the local clocks. NTP provides accuracy of 1-10 milliseconds (ms), depending on the jitter characteristics of the synchronization source and network paths. NTP is a client of the User Datagram Protocol (UDP), which itself is a client of the Internet Protocol (IP).

Some definitions follow. For more terms, see [“Appendix E: Glossary”](#) on page 105 of this *User Guide*.

NTP Data Format

The format of the NTP message data area, which immediately follows the UDP header, is shown in Figure 3-2. NTP time stamps are represented as a 64 bit unsigned fixed-point number, in seconds relative to 0^h on 1 January 1900. The integer portion is in the first 32 bits and the fraction portion is in the last 32 bits.

Table 3-2: NTP Message Data

0	8	16	24	31
LI	VN	MODE	Stratum	Poll
Synchronizing Distance (Root Distance) (32 bits)				
Synchronizing Dispersion (Root Dispersion) (32 bits)				
Reference Identifier (32 bits)				
Reference Time Stamp (64 bits)				
Originate Time Stamp (64 bits)				
Receive Time Stamp (64 bits)				
Transmit Time Stamp (64 bits)				
Authenticator (Optional) (96 bits)				

Leap Indicator (LI)

This is a two-bit code warning of an impending leap second that will be inserted or deleted in the last minute of the current day, with bit 0 and bit 1, respectively, coded as follows:

- 00: No warning
- 01: Last minute has 61 seconds
- 10: Last minute has 59 seconds
- 11: Alarm condition (clock not synchronized)

You are alerted to an alarm condition when the TymServe is first powered on—in other words, before time is initially acquired from the timing signal. An alarm condition will also signal when the timing parameters are changed. This alarm condition will persist until the TymServe acquires time. It should not signal again until the unit is powered off and on.

Version Number (VN)

This is a three-bit integer indicating the NTP version number. The TymServe will return the version number from the incoming NTP message.

Mode

This is a three-bit integer indicating the mode. For the TymServe this field is set to four indicating the server mode. The TymServe always operate in server mode, which means that it will synchronize clients but will never be synchronized by clients.

Stratum

This is an eight-bit integer indicating the stratum level of the local clock. For the TymServe this field is set to one indicating a primary reference.

Poll Interval

This is an eight-bit signed integer indicating the maximum interval between successive messages, in seconds to the nearest power of two. The TymServe will return the poll interval from the incoming NTP message.

Precision

This is an eight-bit signed integer indicating the precision of the local clock, in seconds to the nearest power of two. For the TymServe this field is set to -19 (minus nineteen) which is the value closest to the 1/2 sec precision of the TymServe.

Synchronizing Distance (Root Distance Version 3)

This is a 32-bit fixed-point number indicating the estimated round-trip delay to the primary synchronizing source, in seconds with fraction point between bits 15 and 16. Set to zero in the TymServe.

Synchronizing Dispersion (Root Dispersion Version 3)

Synchronizing Dispersion is a 32 bit fixed-point number indicating the estimated dispersion to the primary synchronizing source, in seconds. Root Dispersion indicates the maximum error relative to the primary reference source.

Reference Clock Identifier

This is a 32-bit code identifying the particular reference clock. In the case of Stratum 1 (primary reference), this is a four-octet, left justified, zero-padded ASCII string. For the TymServe the four-octet string is dependent on the time source selected, 'GPS' for GPS and 'FREE' for Free Running Clock.

Reference Time-stamp

This is the local time at which the local clock was last set or corrected, in 64-bit time-stamp format. With the TymServe, the Reference Time-stamp is the last time that a valid timing signal was detected. Therefore, the Reference Time-stamp will indicate the time at which the timing signal was lost. When the timing signal returns, the Reference Time-stamp will be updated.

Originate Time-stamp

This is the local time at which the request departed the client host for the service host, in 64-bit time-stamp format.

Receive Time-stamp

This is the local time at which the request arrived at the service host, in 64-bit time-stamp format.

Transmit Time-stamp

This is the local time at which the reply departed the service host for the client host, in 64-bit time-stamp format.

Authenticator

This field is used to hold a checksum if authentication has been enabled. Refer to the next section for more information about this mechanism.

NTP Authentication

NTP enables an NTP client to ensure two things: that the time stamp received has come from a trusted source, and that it has not been modified in transit. Because Datum has extended the authentication method, you can use it to deny service to unauthorized clients who submit NTP time stamp requests.

The NTP protocol includes space for two variables related to authentication: an authentication key identifier field and a checksum field.

Authentication Mechanism

The mechanism used to generate the authentication data must be shared by the client and the server. The popular public domain implementation of NTP, known as xNTP, allows for the use of either Digital Encryption Standard (DES) or Message Digest version 5 (MD5). Export restrictions on certain cryptographic techniques means the TymServe supports only the MD5 encryption algorithm. MD5 provides an adequate level of security for NTP transmissions.

MD5 is a one-way hash function that processes the input data and produces 128 bits (16 bytes) of hash value. This checksum is then placed in the packet. Since the data itself is not encrypted, anyone could theoretically capture the packet, modify the data, and put a new checksum into the packet. However, Datum has made the checksum secure by loading a secret key into the MD5 algorithm before the NTP data is loaded. The result: a checksum that cannot be reproduced without the knowledge of the secret key.

Programming and Storage of the Key Identifier/Key Pair

The TymServe allows for the programming and storage of four key identifier/key pairs. Although it is possible to have over four billion keys, four are sufficient for TymServe because it has only one level of access—requesting time stamps.

While there are only four key identifier/key pairs, the key identifiers themselves can have any value between 1 and 4,294,967,296. The format of the MD5 secret key is based on the approach taken by the public domain xNTP package. The key is an eight-character alphanumeric string. This key identifier/key pair is stored in a flash EPROM and need only be programmed once.

Public Domain xNTP Package

For clients not using the public domain xNTP package, the NTP packet is enlarged by 8 bytes to handle the entire checksum, which is 16 bytes (128 bits) in size as generated by the MD5. Since this field is the last in the packet, it should not present any difficulty.

NTP Authentication-Only

The NTP authentication-only mechanism is an added feature in the TymServe and not part of the NTP specification as detailed in RFC 1305. It prevents unauthorized access to the TymServe, making it unnecessary for you to adapt the authentication mechanism yourself for security or administration purposes.

How NTP Defines the Authentication Process

If authentication is enabled, and a valid authentication key identifier and checksum is received, then the NTP packet is filled in and a new checksum is computed and added to the packet. The packet is then sent back to the client.

How TymServe Uses NTP Authentication Only

However, if authentication is enabled and an authentication failure occurs, then the NTP packet is still returned but will contain no authentication data. The reasons this failure occurs is usually because the key identifier is 0—which is defined as no encryption—or because the checksum is invalid.

If NTP authentication has been enabled, and you enable the NTP Authentication Only mode, the TymServe will discard any incoming NTP packet which does not contain both a valid key identifier not equal to 0 and a valid checksum. In this way, you can limit access to the TymServe to only those clients who have been given the key identifier/secret MD5 key pair.

Sysplex Timer

“Sysplex” means SYStem comPLEX, a term often used to describe continuous computing on clusters of computers. The Sysplex Timer is sometimes called an External Time Reference (ETR). The Sysplex Timer provides a synchronized Time-of-Day (TOD) clock for multiple attached computers. A Sysplex is needed when two or more systems are configured in a Sysplex. One Sysplex Timer can do the job, but it’s a good idea for you to have a second duplex timer on the cluster as a backup in case the primary timer fails.

How TymServe Uses the Sysplex Timer

TymServe receives the signal from the GPS antenna, then provides Sysplex Timer output through its Serial Port A. The Serial Port A supplies an ASCII broadcast of UTC time that is often used by computers that cannot or do not use NTP.

Be sure your computer is set up with the correct Serial Port parameters—the correct baud rate, data bits, stop bits, and parity. The Serial Port will start broadcasting the time only after it receives a **c** or **C** character. It will stop broadcast when it receives an **r** or **R** character.

NOTE: If you set the Sysplex Timer to **Auto on** the Sysplex Timer starts automatically on power up.

The following time information string is transmitted once per second, when started with the **c** or **C** character. The **DDD** field represents three ASCII digits of days (001–366). The **Quality Indicator** indicates the validity of the time. The **Carriage Return** character is

transmitted on-time. The first rising edge of the Carriage Return character occurs within 200 nanoseconds after the TymServe 1PPS signal transitions from low to high.

(SOH)DDD:HH:MM:SSQ(CR)(LF)	
Field	Description
(SOH) (0x01)	ASCII Start of Header
DDD	Day of year
HH	Hours (24-hour clock)
MM	Minutes
SS	Seconds
Q	Quality Indicator (space = normal operation)
(CR) (0x0D)	ASCII Carriage Return (transmitted on-time)
(LF) (0x0A)	ASCII Line Feed
Quality Char	Description
space	Normal operation, time set and not flywheeling
X	Time not set yet
F	Time was set, but currently flywheeling

Chapter 4: Command Shell and Command Descriptions

In This Chapter

This chapter reviews the command shell and defines commands.

Shell Overview

Command Shell is a command line interface accessible through Serial Port B or Telnet. It is a multiple level tree where the input is entered as a command in the form of ASCII strings typed at the command prompt. The ready state of the command shell is an ASCII ? (question mark) prompt. The specific commands available at a particular tree level can be displayed by entering a <? **Enter**> at the ? prompt. A complete command shell tree is in Figure 4-1.

A CR-LF, CR, or LF sequence terminates all entered ASCII commands, depending on the translation setting in the serial configuration subdirectory. The command interface interprets the input on a character-by-character basis. As a result, only enough characters to uniquely identify the command need to be entered for the command interface to recognize which action you want performed. The command interface also accepts multiple commands on a single line when they are separated by spaces, so you don't have to press **Enter** after each command.

Maximum buffer size is 128 bytes.

The commands are categorized into three types:

- **Level command** Available at the root level and have a forward slash (/) following the command string
- **Action command** Show the current setting or set new parameters when executed with the corresponding parameter
- **Intrinsic command** Available at any level of the system

Command Description

The command shell is case sensitive so commands should be entered as they are described here.

The commands are divided into the following categories:

- Network
- Timing
- Serial
- Utility
- Intrinsic help

There may be multiple entries of the input parameters for each command. Each entry corresponds to one of the allowable input parameters. If multiple parts are shown in the command menu, then type the first part of each command. Otherwise the following parts will be treated as input parameters, which may cause some confusion. For example, if you enter file name `ts211d.hex` instead of file `ts211d.hex` the TymServe will set the file name to be **name** and `ts211d.hex` will be ignored, and incorrect configuration could result.

The commands can be accessed by RS-232 (Command Shell), Telnet (Command Shell), or SNMP (SNMP Management Software Interface). The command tree follows.

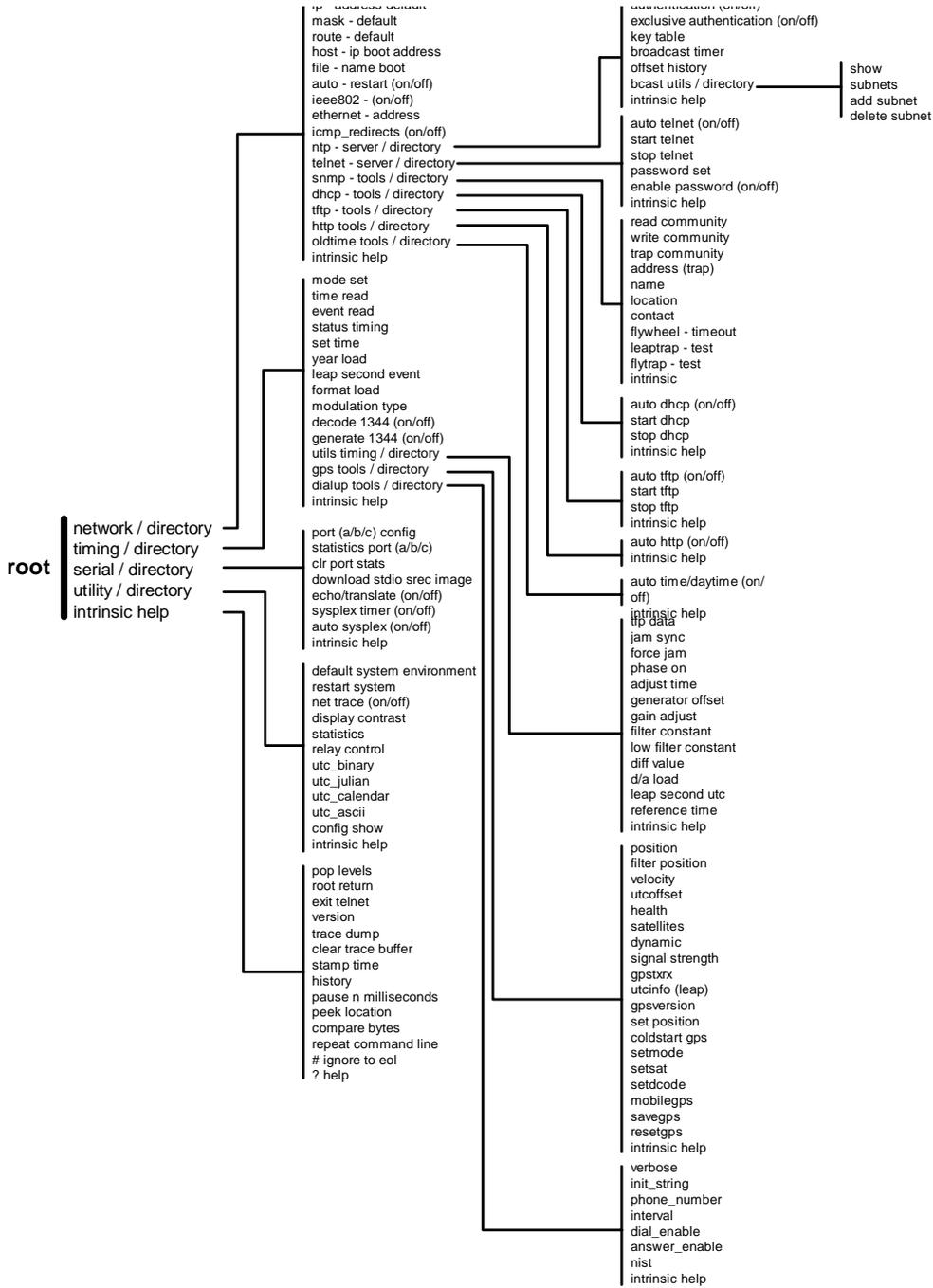


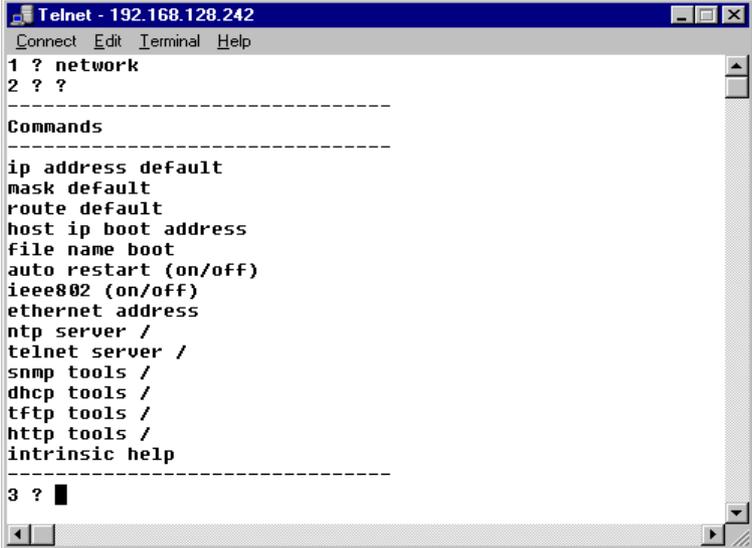
Figure 4-1 Serial/Telnet Command Tree



Network Directory

Typing `network` and pressing **Enter** under the root directory gets you into the network directory.

NOTE: The format of the commands below is: **prompt** <command> (environment able to use command).



```

Telnet - 192.168.128.242
Connect Edit Terminal Help
1 ? network
2 ? ?
-----
Commands
-----
ip address default
mask default
route default
host ip boot address
file name boot
auto restart (on/off)
ieee802 (on/off)
ethernet address
ntp server /
telnet server /
snmp tools /
dhcp tools /
tftp tools /
http tools /
intrinsic help
-----
3 ? █

```

Figure 4-2 Network Commands

Network Commands

The commands in this directory provide network configuration options, and some network server daemons and tools are available in the directory.

ip <xxx.xxx.xxx.xxx> (RS-232, Telnet)

Queries or sets the network IP address of the TymServe in dotted quad notation. This variable can also be set automatically using the automatic DHCP function. If this value is changed using a Telnet session, the connection will be lost and a new connection will need to be started using the new address. The network interface will be restarted after successful storage of the new parameter in nonvolatile memory.

mask <xxx.xxx.xxx.xxx> (RS-232, Telnet)

Queries or sets the network IP mask address of the TymServe in dotted quad notation. This variable can also be set automatically using the automatic DHCP function. If this value is changed using a Telnet session, the connection will be lost and a new connection

will need to be started. The network interface will be restarted after successful storage of the new parameter in nonvolatile memory.

route <xxx.xxx.xxx.xxx> **(RS-232, Telnet)**

Queries or sets the network IP default route address of the TymServe in dotted quad notation. This variable can also be set automatically using the automatic DHCP function. If this value is changed using a Telnet session, the connection will be lost and a new connection will need to be started. The network interface will be restarted after successful storage of the new parameter in nonvolatile memory.

host <xxx.xxx.xxx.xxx> **(RS-232, Telnet, SNMP)**

Queries or sets the network TFTP server address for the TymServe in dotted quad notation to be used for downloading the new firmware. This variable can also be set automatically using the automatic DHCP function.

file <file name> **(RS-232, Telnet, SNMP)**

Queries or sets the filename of the firmware image which will be requested during a TFTP session to download new firmware. This filename can also be set automatically using the automatic DHCP function. This is used for upgrading the FLASH EPROM, which contains the TymServe operating code. This function is not necessary for normal operation of the unit. By default the file name is set to 'ts21ld.hex'.

auto <'on' or 'off'> **(RS-232, Telnet, SNMP)**

Queries or sets the auto restart mode. This function is used to control the operation of the TymServe after new firmware downloads. If this mode is enabled, the TymServe will reboot after a successful download and storage of a new version of operating firmware. This will allow the TymServe to begin using the new firmware immediately. If this mode is disabled, the TymServe must be rebooted or power cycled to load the new firmware into RAM.

Auto restart mode:

On = restart after successful firmware updates

Off = do not restart after successful firmware updates

ieee802 <'on' or 'off'> **(RS-232, Telnet)**

Queries or sets the network frame header type. The default type is off which means that DIX packet headers are used. 99% of TCP/IP based networks use DIX packet headers. Do not change this parameter unless you are certain that the packet format should be changed. If this parameter is changed improperly, the RS-232 access method will have to be used to reset this value.

Frame type parameters used by the network interface:

Off = use Ethernet DIX packet headers.

On = use IEEE 802.2 packet headers.

ethernet (RS-232, Telnet, SNMP)

Queries the hardware Ethernet address. This value is used for definitions of the TymServe recorded in BOOTP or DHCP servers. This value is a unique identifier that is programmed at the factory.

icmp_redirects <'on' or 'off'> (RS-232, Telnet, SNMP)

This command allows the user to disable the processing of icmp redirects. This feature is provided for security purposes.

NTP Server Directory

Typing `ntp` and pressing **Enter** under **network directory** gets you into the NTP directory, which carries these NTP configuration commands.

authentication <'on' or 'off'> (RS-232, Telnet, SNMP)

Sets the NTP daemon up to use the standard NTP authentication mechanism defined in RFC 1305, which provides a way to restrict access to TymServe.

NTP authentication mode:

Off = disabled

On = enabled

exclusive <'on' or 'off'> (RS-232, Telnet, SNMP)

Sets the NTP daemon up to use the standard NTP 'exclusive' authentication mode, which provides a way to further restrict access to TymServe in addition to authentication defined in RFC1305. See the NTP Authentication appendix for a complete description of this mode.

NTP 'exclusive' authentication mode:

Off = disabled.

On = enabled

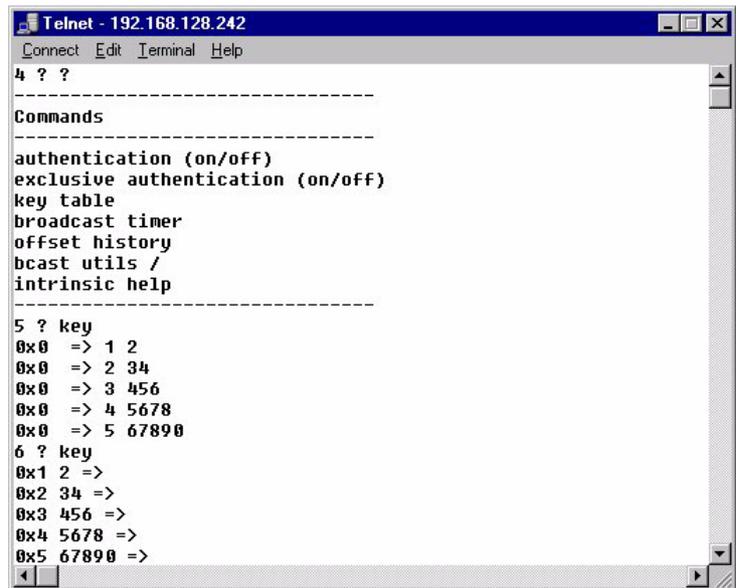
key (RS-232, Telnet, SNMP)

This function is used to query or set the NTP authentication key pairs. Refer to the NTP Authentication appendix or RFC 1305 for complete details of the use of these keys. Due to export restrictions, only MD5 authentication is supported. Also, to maintain compatibility with the public domain xNTP implementation of the NTP protocol, only ASCII character sequences can be used as authentication keys.

The <enter> at the key entry prompt => will display the 1-5 keys entries in the form => keynbr key

Where: keynbr is the NTP authentication key id
key is the 1-8 character MD5 key (ASCII only).

The fields will be blank if no key is stored. New keys can be entered using the same format as shown in Figure 4-3. Entering a blank line will terminate the key entry prompt session.



```

Telnet - 192.168.128.242
Connect Edit Terminal Help
4 ? ?
-----
Commands
-----
authentication (on/off)
exclusive authentication (on/off)
key table
broadcast timer
offset history
bcast utils /
intrinsic help
-----
5 ? key
0x0 => 1 2
0x0 => 2 34
0x0 => 3 456
0x0 => 4 5678
0x0 => 5 67890
6 ? key
0x1 2 =>
0x2 34 =>
0x3 456 =>
0x4 5678 =>
0x5 67890 =>

```

Figure 4-3 Key Commands

broadcast (RS-232, Telnet)

Selects or queries the state of the NTP broadcast mode (NTP mode 5). If this mode is enabled, the TymServe will broadcast a NTP broadcast packet to the local subnet every specified number of seconds. This mode of operation has no impact on the standard NTP client/server mode. Regardless of the state of the NTP broadcast mode, the TymServe will respond to client request packets with server packets.

NTP broadcast mode (NTP mode 5):

0 = disable broadcast

Any Positive Integer 'x' = enable broadcast every 'x' seconds of time interval

The actual time interval used by NTP broadcast is the value that is calculated by rounding down or equal to the value of 'x' to the closest value of power of 2. For example input of

10 sets time to 8 which is 2 to the power 3. Therefore, the actual time interval settings are 1, 2, 4, 8, 16, 64, and so on.

offset (RS-232, Telnet)

Queries an offset record of a NTP client. The TymServe creates a hash table at startup and continually adds and updates entries regarding NTP clients who submit NTP client mode packets. This function is useful for debugging purposes but is not required for normal operation. The values are based on data in the client request and do not include network latencies.

Statistic information of NTP clients includes:

- Packet count
- Maximum offset
- Last offset
- 10-sample rolling average

NTP Broadcast Directory

Typing `bcast` then pressing **Enter** under `ntp directory` gets you into the NTP broadcast directory. This directory contains commands that allow up to 32 broadcast addresses (subnets) to receive ntp broadcasts from the TymServe. If the broadcast command in the ntp subdirectory has been set to a non-zero value, ntp broadcast messages will be sent to the broadcast addresses entered here.

NOTE: All new commands operate on broadcast addresses, not subnet addresses. This is required because different broadcast address schema exist and the programmed broadcast address must agree with the broadcast address for the particular subnet programmed into the gateway or router which will deliver the packets.

show

Displays the currently programmed subnet broadcast addresses.

add <xxx . xxx . xxx . xxx>

Adds a ntp broadcast subnet to non-volatile storage.

NOTE: To configure ntp broadcasts to be sent on the local subnet, the value 255.255.255.255 must be used. This corresponds to the local broadcast address in the internal routing tables of the TymServe.

delete <xxx . xxx . xxx . xxx>

Deletes a broadcast subnet from non-volatile storage.

Telnet Server Directory

Typing `Telnet` and pressing **Enter** under **network directory** gets you into the Telnet directory. This directory provides Telnet configuration commands.

auto <'on' or 'off'> (RS-232, Telnet)

Select or query the state of the automatic Telnet server mode. If this mode is enabled, the TymServe will be ready to accept Telnet client after power up. Otherwise, no Telnet connection will be allowed. Note that only one Telnet session is allowed at a time.

start/stop (RS-232, Telnet)

The `start` command is used to manually start a currently disabled Telnet server. The `stop` command is used to disconnect a currently running Telnet session gracefully or disable Telnet server for the security reasons. Telnet session automatically terminates after an hour of idle time when there is no activity. The length of time for automatic termination is not configurable. The intrinsic command `trace` can be used to view the status of a Telnet session.

password <*user selected password*> (RS-232, Telnet)

This command is used to restrict Telnet access to the TymServe. The use of a password for Telnet access can be enabled or disabled from the same subdirectory. Telnet password is transmitted in an un-encrypted format, therefore, the security provided by this feature is just to discourage the casual users. If a password set previously is forgot, this command can be used to retrieve the password in the shell through a serial connection.

enable <'on' or 'off'> (RS-232, Telnet)

This command allows the user to restrict Telnet access to the TymServe to those users who know the password. Setting of the password can be accomplished using the `password` command available in the same sub-directory. Parameters: `on` or `off` enables or disables the Telnet password.

SNMP Tools Directory

Typing `snmp` and pressing **Enter** under **network directory** enters the SNMP directory. It carries SNMP configuration commands.

read <*read community name*> (RS-232, Telnet)

Queries or sets the SNMPv1 'read community name'. The default value for this variable is the ASCII string 'public'. The input could be any ASCII string with 1-40 characters. This is an industry standard community name and represents a possible security risk, therefore, this variable should be changed.

write <write community name> (RS-232, Telnet)

Queries or sets the SNMPv1 write community name. The default value for this variable is the ASCII string `private`. The input could be any ASCII string with 1-40 characters. This is an industry standard community name and represents a security risk. Query displays the current community name or blank line if it is not configured.

trap <trap community name> (RS-232, Telnet)

Queries or sets the SNMPv1 trap community name. The default value for this variable is the ASCII string 'Datum.' The input could be any ASCII string with 1-40 characters. Query displays current community name or blank line if it is not configured.

address <xxx.xxx.xxx.xxx> (RS-232, Telnet)

Queries or sets the ip address of the SNMPv1 management console in dotted quad format that should receive any trap messages generated by the TymServe. The default value is 0.0.0.0, which the TymServe will interpret to mean that trap messages should not be transmitted.

name <sysName> (RS-232, Telnet, SNMP)

Queries or sets the MIB-II variable sysName value as a ASCII string. This string is stored in nonvolatile memory and is most often used to provide a unique identifier to SNMPv1 management consoles. The input could be any ASCII string with 1-40 characters. The default value for this variable is a null string (blank).

location <sysLocation> (RS-232, Telnet, SNMP)

Queries or sets the MIB-II variable sysLocation value. The input could be any ASCII string with 1-40 characters. This string is stored in nonvolatile memory and is most often used to identify the location installation of a network device to SNMPv1 management consoles. The default value for this variable is a null string (blank).

contact <sysContact> (RS-232, Telnet, SNMP)

Queries or sets the MIB-II variable sysContact value. The input could be any ASCII string with 1-40 characters. This string is stored in nonvolatile memory and is most often used to identify the technical or administrative contact for a particular network device to SNMPv1 management consoles. The default value for this variable is a null string (blank).

flywheel SNMPv1 <flywheeling trap> (RS-232, Telnet, SNMP)

Queries or controls the generation of the SNMPv1 flywheeling trap. The new value is between 0-86400, where 0 indicates that a trap should not be sent and any other allowed

value indicates the alarm value. The decimal number indicating the number of seconds after the reference timing signal is lost before a SNMPv1 trap message will be sent.

DHCP Tools Directory

Typing `dhcp` and pressing **Enter** displays the DHCP directory as shown in Figure 4-4, which carries commands to start or stop DHCP manually and command to enable or disable automatic DHCP when system powers up.

auto <'on' or 'off'>
(RS-232, Telnet, SNMP)

Select or query the state of the automatic DHCP mode. If this mode is enabled, the TymServe will attempt to download new network parameters from a DHCP server after every reboot.

```

Telnet - 192.168.128.242
Connect Edit Terminal Help
file name boot
auto restart (on/off)
ieee802 (on/off)
ethernet address
ntp server /
telnet server /
snmp tools /
dhcp tools /
tftp tools /
http tools /
intrinsic help
-----
12 ? dhcp
13 ? ?
-----
Commands
-----
auto dhcp (on/off)
start dhcp
stop dhcp
intrinsic help
-----
14 ? █

```

Figure 4-4 DHCP Commands

For DHCP sessions, the DHCP server must be programmed with the Ethernet address of the TymServe which can be obtained using the 'ethernet' command in the network sub-directory.

start/stop (RS-232, Telnet, SNMP)

Starts or stops a DHCP session to obtain network parameters from a DHCP or BOOTP server. A DHCP session will set the IP address, network mask, and route variables. In addition, if configured on the DHCP or BOOTP server, the host and TFTP boot file name can be obtained and configured by TymServe. The network interface will be restarted after a successful DHCP session to start using the new variables. The intrinsic command `trace` can be used to view the status and values relayed during a DHCP session.

TFTP Tools Directory

Typing `tftp` then **Enter** in the **network directory** gets you into the TFTP directory as shown in Figure 4-5.

auto <'on' or 'off'> (RS-232, Telnet, SNMP)

Selects or queries the state of the automatic TFTP mode. If this mode is enabled, the TymServe will attempt to download new operating firmware from a TFTP server after every reboot.

```

Telnet - 192.168.128.242
Connect Edit Terminal Help
file name boot
auto restart (on/off)
ieee802 (on/off)
ethernet address
ntp server /
telnet server /
snmp tools /
dhcp tools /
tftp tools /
http tools /
intrinsic help
-----
3 ? tftp
4 ? ?
-----
Commands
-----
auto tftp (on/off)
start tftp
stop tftp
intrinsic help
-----
5 ?

```

Figure 4-5 TFTP Commands

For TFTP transfers, the ip address, net mask, route, host, and file variables must be configured. This mode of operation is NOT recommended.

start/stop (RS-232, Telnet, SNMP)

Starts or stops a TFTP session to download new operating firmware from a TFTP server. For TFTP transfers, the ip address, net mask, route, host, and file variables must be configured. When a TFTP session is started, a rolling indicator will be displayed in Telnet or RS-232 sessions to indicate that a transfer is taking place. If the indicator stops moving, the intrinsic command `trace` can be used to display the terminal status of the TFTP session. For more information about upgrading the firmware, see [“Appendix C: Firmware Upgrade”](#) on page 83.

HTTP Tools Directory

Typing `http` and pressing **Enter** in the **network directory** accesses the HTTP directory.

auto <'on' or 'off'>
(RS-232, Telnet, SNMP)

Selects or queries the state of the automatic HTTP mode.

```

Telnet - 192.168.128.242
Connect Edit Terminal Help
route default
host ip boot address
file name boot
auto restart (on/off)
ieee802 (on/off)
ethernet address
ntp server /
telnet server /
snmp tools /
dhcp tools /
tftp tools /
http tools /
intrinsic help

-----
3 ? http
4 ? ?

-----
Commands
-----
auto http (on/off)
intrinsic help

-----
5 ? █

```

Figure 4-6 HTTP Commands

Oldtime Tools Directory

Typing `<oldtime>` then **Enter** in the **network directory** accesses the OLDTIME directory.

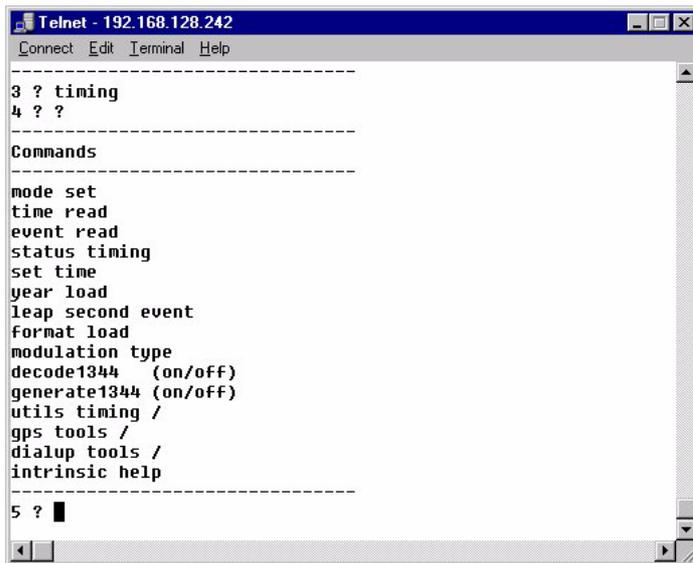
auto <'on' or 'off'> (RS-232, Telnet, SNMP)

This command allows the user to disable both the time (RFC868) and daytime (RFC867) protocol daemons. This feature is provided for access control purposes.

NOTE: This command has no impact on the standard NTP (RFC1305) daemon.

Timing Directory

Typing `timing` then pressing **Enter** under **root directory** enters the timing directory as shown in Figure 4-7. Its commands configure the time engine. Some timing-related utility tools are available in the directory.



```

Telnet - 192.168.128.242
-----
3 ? timing
4 ? ?
-----
Commands
-----
mode set
time read
event read
status timing
set time
year load
leap second event
format load
modulation type
decode1344 (on/off)
generate1344 (on/off)
utils timing /
gps tools /
dialup tools /
intrinsic help
-----
5 ? █

```

Figure 4-7 Timing Commands

Timing Commands

mode <mode-value> (RS-232, Telnet, SNMP)

Selects the reference time source that will be used by the TymServe to synchronize its internal clock, where mode-value is one of the following

- 0 = Time code
- 1 = Freerun
- 6 = GPS

time (RS-232, Telnet, SNMP)

Queries the current date and time.

event (RS-232, Telnet, SNMP)

Queries the captured event every 100ms. Enter `Control-C` to stop it. Captured event about every 100 ms.

status (RS-232, Telnet, SNMP)

Queries the current timing status of the TymServe and this bitmask relays information shows the internal PLL disciplining to the selected timing reference source:

‘Status: 0x0v’

where ‘v’ has value 0 – 7, and can be represented by <Bit 2> <Bit 1> <Bit 0>

Bit 0 = 0 if receiving reference signal (Tracking)

= 1 if NOT receiving reference signal (Flywheeling)

Bit 1 = 0 if Bit 0 = 0 AND if phase difference < 2 usec in mode 6 or 5 usec in mode 0

= 1 otherwise

Bit 2 = 0 if Bit 0 = 0 AND if frequency difference < 5E8 per second (Locked)

= 1 otherwise

where phase difference is between internal oscillator and reference signal

and frequency difference is between internal oscillator and reference signal

Thus

0 = 000 – Locked, where Tracking and Locked light are on (stabilized)

1 = 001 – not defined

2 = 010 – Tracking, where Tracking light is on and Locked light off (stabilizing)

3 = 011 – not defined

4 = 100 – Tracking, where Tracking light is on and Locked light off (stabilizing)

5 = 101 – not defined

6 = 110 – Tracking, where Tracking light is on and Locked light off (stabilizing)

7 = 111 – Flywheeling, where Tracking and Locked light are off (cold starting)

set <time> (RS-232, Telnet, SNMP)

Sets the current time. While this command can be used in any mode, it is useful only for the special Freerun mode. The input is in one of the following format:

x.y

mm / dd / yyyy hh : mm : ss.x

yyyy ddd hh : mm : ss.x

MON dd yyyy hh : mm : ss.x

hh : mm : ss.x

where *x.y*

mm / dd / yyyy = month / day / year.

yyyy ddd = year number-of-day-in-the-year.

MON dd yyyy = 3-up-case-letter-month date year.

hh : mm : ss.x = hour : minute : second . second-fraction

UTC time in the format of *second . second-fraction* since 0:00AM on January 1, 1970, where the trailing .0 is required.

year <xxxxx> (RS-232, Telnet, SNMP)

Sets the year used by the TymServe between 1970–2050. While this command can be used in any of the modes, it is not useful for GPS where the year is automatically set from the GPS signal.

leap <type> <Time> (RS-232, Telnet)

Queries and sets leap second event information. The command without parameter returns current setting of leap second event information. If the UTC second count of leap second event time is the past, the leap event type should be 0 (zero). If the UTC second count of leap second time is in the future, the leap event type should be either 1 or -1

where **type** is the leap second event type:

0 = no action or cleared

1 = insertion.

-1 = deletion.

and **Time** is UTC time when the leap event will occur in one of the following formats:

x.y

mm / dd / yyyy hh : mm : ss.x

yyyy ddd hh : mm : ss.x

MON dd yyyy hh : mm : ss.x

hh : mm : ss.x

where *x.y* = *second . second-fraction*.

mm / dd / yyyy = month / day / year.

yyyy ddd = year number-of-day-in-the-year.

MON dd yyyy = 3-up-case-letter-month date year.

hh : mm : ss.x = hour : minute : second . second-fraction

UTC time is in the format second . second-fraction since 0:00AM on January 1, 1970.

The second-fraction part for a leap second event should be always 0.



WARNING: This command is critical to a TymServe that is running in Freerun mode because the time reference does not provide leap second information. It is user's responsibility to set the leap second event so that TymServe can operate correctly in the event of a leap second insertion or deletion.

For a TymServe that is running in GPS mode, the leap second event does not need to be set by this command because it is done automatically. However, this command can be used to query or verify a leap second event.

tfp (RS-232, Telnet)

Queries various information from the timing co-processor on the TymServe as shown in the table that follows.

Table 4-1: TFP Queries

Input Parameter	Returns
0 (tfp d/a)	0xXXXX (PLL oscillator disciplining voltage in hex)
1 (tfp leap second count)	xx (current leap second count for GPS mode)
2 (firmware version of timing coprocessor)	TS21 V.vvv MM/DD/YYYY HH:MM:SS where V.vvv = major version . minor version MM/DD/YYYY = month/day/year HH:MM:SS = hour:minute:second
3 (current timing coprocessor selected timing mode)	Mode (this should match the value returned by the mode command)
4 (timecode mode)	Mode (this should match the value returned by the format command)
5 (gain for 10 MHz phase lock loop)	Value of gain
6 (filter gain KM)	Value of KM
7 (filter gain KO)	Value of KO

jam <'1' enable or '0' disable> (RS-232, Telnet)

Enables or disables automatic jam-synch.

force (RS-232, Telnet)

Forces a jam-synch on next reference pps with GPS.

phase <'0' or positive disturbance-100ns step size> (RS-232, Telnet)

Reads and displays phase values for ten seconds then forces a phase step of user specified magnitude such as 10, 100, or 1000. Then continues to read and display phase until a key is pressed. It reads and displays current undisturbed phase if 0 is entered. Any value as magnitude of phase disturbance (0 as no disturbance).

adjust <value at step size - 100ns> (RS-232, Telnet)

Adjusts the timing engine time so that it speeds up with a positive value and slows down with a negative value in step size 100ns. Do not change this parameter unless you are absolutely certain that it is necessary to do so. Adjust at a step size of 100ns.

gain <Gain value> (RS-232, Telnet)

Sets discipline filter gain value for time reference signal. Do not change this parameter unless you are absolutely certain that it is necessary to do so.

The gain value range is -32767 to +32768.

filter <value> (RS-232, Telnet)

Sets filter constant. Do not change this parameter unless you are absolutely certain that it is necessary to do so. The floating point value range is 0.0 – 1.0

Low (RS-232, Telnet)

Current low pass filter constant. Not applicable to TymServe currently.

diff <x> (RS-232, Telnet)

Sets diff value to adjust the period of the HC11 generated 1PPS. A value of 0 resets the diff to 33920 which causes the pps to be 0x2E6 clock cycles. Positive values lengthen the diff while negative values shorten the diff. The effect on diff is cumulative, except for value 0. Do not change this parameter unless you are absolutely certain that it is necessary to do so.

d/a <DAC control value between 0x0000 - 0xFFFF> (RS-232, Telnet, SNMP)

Queries or sets the d/a control steering voltage that controls the TymServe oscillator value. This setting, in conjunction with the gain and constant, is used to control the frequency of the on-board oscillator. The setting of this value is recommended only for advanced users who wish to control the frequency of the oscillator in the special freerunning mode.

leap second utc (RS-232, Telnet)

This command allows the user to query the current leap second information in the TymServe. The first value returned is the leap action which can be:

- 0 = no action
- 1 = leap second insertion scheduled
- 1 = leap second deletion scheduled

The second value returned is the UTC binary second time at which this event will take place. Note that the time can be in the past, which is typical for GPS. If the time is in the past, no action will be taken regardless of the state of the leap action variable.

reference (RS-232, Telnet)

Query latest reference time. The reference time reflects whether the reference source is available currently or not. This command can be used to check when TymServe loses its reference source if the reference time returned is not current.

Serial Directory

Typing `serial` and pressing **Enter** under the **root directory** displays the serial directory. The serial commands are used for status or configuration of TymServe through the Serial Port B.

port <port> <baud> <data-bit> <stop-bit> <parity> **(RS-232, Telnet)**

Queries or sets serial configuration for port A, B, and C. If a port is currently in use and its parameters are changed, the connection will be lost and a new connection with proper parameters will need to be started.

where <port> = A, B, or C

<baud>= baud rate between 50 and 115200.

<data-bit>= data length between 5 and 8 bits.

<stop-bit>= stop bit length either 1 or 2.

<parity>= one of parity choices: none, odd, low, even and high.

statistics (RS-232, Telnet)

Queries statistics information including number of transmitting and receiving counts, number of receiving breaks and drops, and so forth. It also gives statistics information for a selected port. Port name: A, B, or C.

clr <port 'A', 'B' or 'C'> **(RS-232, Telnet)**

Clears port statistics selected by user.

downloads (RS-232, Telnet)

This function tells the TymServe to start looking for a new version of firmware to be downloaded via the rear panel RS-232 port Serial B. After issuing this command, the user should select `text file download` from his ASCII terminal and stream the file containing the new firmware to the TymServe. Once the command is issued, a rolling indicator will be displayed to confirm that the TymServe is waiting for a firmware download. Once the file begins streaming, the rolling indicator should continue. If, instead, a string of errors is reported, check that the record terminators (that is to say, `cr`, `cr-lf`, and so on) are properly matched with the settings in the serial menu. This is used for upgrading the FLASH EPROM which contains the TymServe operating code. This function is not necessary for normal operation of the unit. The file format is Motorola S-records.

echo <port> <echo-state> <translate-state> **(RS-232, Telnet)**

Queries or sets the state of echo and translate for port A, B, C, and Telnet port. If echo is ON, a character entered will be echoed on screen, otherwise it will not. But if translate is on, the carriage-return entered will be translated to new-line-feed. The translation should be coordinated with the setting of the serial for hyper-terminal, tip or whatever term emulator.

where <port> = A, B, or C
 = telnd (for Telnet port).
 <echo-state> = on (echo enabled).
 = off (echo disabled).
 <translate-state>= on (translate enabled).
 = off (translate disabled).

sysplex <'on'> or <'off'> **(RS-232, Telnet)**

Transmits UTC time through the rear panel Serial Port when sysplex is set to 'on.' Once `sysplex` is on, system starts to poll the Serial Port A. It starts the time transmission after it receives 'c' or 'C' character via the Serial Port. It stops when it receives an `r` or **RS-232** character. It transmits UTC time in ASCII format once every second at the time when carriage-return is transmitted (the carriage-return is transmitted on time each second).

auto sysplex <'on' enable> or <'off' disable> **(RS-232/Telnet)**

Queries and sets if the TymServe should automatically start the sysplex timer output without waiting for an input 'c' or 'C' character. This command is only useful if sysplex has been turned on. If auto is set on, the TymServe will ignore any input characters and continuously generate serial time output.

Utility Directory

Typing `utility`, then pressing **Enter** under **root directory** gets the utility directory. These commands provide a set of utility commands for TymServe.

default **(RS-232, Telnet)**

Sets all TymServe system parameters to default values that are hard-coded in the firmware. These parameters include (1) system state; (2) network related parameters such as IP address, net mask, default route, boot host and boot file name; (3) serial related parameters such baud rate, stop bit, parity for all ports, and so on. If this command is executed while DHCP is running, network related parameters such as IP address, net mask, and so forth, will be restored after they are set to default values at the time when ip address lease needs to be renewed.

restart (RS-232, Telnet)

Restarts the system.

net <'on'> or <'off'> (RS-232, Telnet)

Queries or sets the state of the network trace facility. The network trace uses promiscuous mode to dump network data to the trace buffers. This function is provided for debugging purposes and is not necessary for normal operation of the TymServe.

display (RS-232, Telnet)

Displays and sets front panel display contrast value. Bigger positive value makes contrast bigger. Negative value sets zero-contrast. A good value should be around 5000-10000.

statistics (RS-232, Telnet)

Queries system statistics including number of ethernet transmitting, receiving and dropping, timer usage by system, DHCP binding number, and TFTP, Telnet server and NTP Server session numbers. Statistical information about network activities and system timer usage.

relay <new relay1-state><new relay2-state> (RS-232, Telnet)

Queries and sets relay 1 and relay 2 state: quiet or alarm. The allowed relay states are

0 = QUIET

1 = ALARM

2 = NO CHANGE

Command without parameter returns current relay-state associated with time stamp. Relay 1 is designated for monitoring power. A loss of power turns relay 1 alarm on, where continuity would be detected between the C (Common) and the NC (Normally Closed) contacts. Relay 2 is designated for monitoring the flywheeling state of TymServe. After a certain number of seconds after the reference timing signal is lost, relay 2 alarm is turned on and continuity would be detected between the C (Common) and the NC (Normally Closed) contacts. The number of seconds can be set through the `flywheel` command in `snmp` directory. Note that a default number (600 seconds) will be used if the number set by the `flywheel` command is 0. See the `flywheel` command for more details. Note that this command is useful only when the system is equipped with relays.

utc_binary (RS-232, Telnet)

Converts input time to UTC second counts since 0:00AM on January 1, 1970. If only hh:MM.:ss.x is used as input, it assumes the date is January 1, 1970.

One of following formats:

mm / dd / yyyy hh : mm : ss.x

yyyy ddd hh : mm : ss.x

MON dd yyyy hh : mm : ss.x

hh : mm : ss.x

where

mm / dd / yyyy = month / day / year.

yyyy ddd = year number-of-day-in-the-year.

MON dd yyyy = 3-up-case-letter-month date year.

hh : mm : ss.x = hour : minute : second . second-fraction

UTC time in the format of second . second-fraction since 0:00AM on January 1, 1970.

utc_julian (RS-232, Telnet)

Converts input time to Julian time. If only hh : mm : ss.x is used as input, it assumes the date is January 1, 1970.

One of following formats:

x.y

mm / dd / yyyy hh : mm : ss.x

MON dd yyyy hh : mm : ss.x

hh : mm : ss.x

where

x.y = second . second-fraction.

mm / dd / yyyy = month / day / year.

MON dd yyyy = 3-up-case-letter-month date year.

hh : mm : ss.x = hour : minute : second . second-fraction

Julian time in the format of yyyy ddd hh : mm : ss.x, where

yyyy ddd = year number-of-day-in-the-year.

utc_calendar (RS-232, Telnet)

Converts input time to Calendar time. If only hh : mm : ss.x is used as input, it assumes the date is January 1, 1970.

One of following formats:

x.y

yyyy ddd hh : mm : ss.x

MON dd yyyy hh : mm : ss.x

hh : mm : ss.x

where

x.y = second . second-fraction.

yyyy ddd = year number-of-day-in-the-year.

MON dd yyyy = 3-up-case-letter-month date year.

hh : mm : ss.x = hour : minute : second . second-fraction

Calendar time in the format of mm / dd / yyyy hh : mm : ss.x, where

mm / dd / yyyy = month / day / year

utc_ascii (RS-232, Telnet)

Converts input time to ASCII time. If only hh : mm : ss.x is used as input, it assumes the date is January 1, 1970.

One of following formats:

x.y

mm / dd / yyyy hh : mm : ss.x

yyyy ddd hh : mm : ss.x

hh : mm : ss.x

where

x.y = second . second-fraction.

mm / dd / yyyy = month / day / year.

yyyy ddd = year number-of-day-in-the-year.

hh : mm : ss.x = hour : minute : second . second-fraction

ASCII time in the format of MON dd yyyy hh : mm : ss.x, where

MON dd yyyy = 3-up-case-letter-month date year.

config show (RS-232, Telnet)

This is a configuration dump utility, which provides a single interface to retrieving current configuration settings. Entering the command without any parameter will display the format. System, network, or ALL settings maybe be retrieved. This command is not required for typical operation but allows the administrator to make a record of the current settings for use if replacement is ever required.

Intrinsic Help

Intrinsic help commands are commands that can be used in any directory as a basic shell command tool. To get a list of intrinsic commands, enter `intrinsic`.

pop (RS-232, Telnet)

Moves the command shell to the previous level. The command `root pop <Enter>` disconnects the Telnet session.

root (RS-232, Telnet)

Moves the command shell to point to the main shell directory. While this function is not necessary for operation, it can be useful for navigating the command shell.

exit (RS-232, Telnet)

This command exits the Telnet client session while it is active. This command has no effect if it is executed in the serial session. To terminate the existing Telnet session from a serial session use `stop` command as explained in the Telnet directory.

version (RS-232, Telnet)

Displays the current firmware version and build date of the TymServe

Rev V.VVV MM/DD/YYYY HH:MM:SS.

Filename: ts21ld.hex

Where V.VVV = major.minor version.

MM / DD / YYYY = month / day / year, HH : MM : SS = hour : minute :
second

Filename: Name of Firmware Image file

trace (RS-232, Telnet)

Displays current contents of the trace buffers. These buffers contain information reported by various subsystems of the TymServe. After a restart, the buffers will contain status reports from each major initialization steps. If an error occurs, a message is written to the

trace buffers whenever possible. The trace buffers are implemented in a circular buffer where newer entries will overwrite older information when the buffers are full. The clear command can be used to flush the trace buffers. If you suspect an error has occurred, use this command to query the system.

clear (RS-232, Telnet)

Clears the trace buffers. While this function is not necessary for operation, it can be useful for debugging purposes.

stamp (RS-232, Telnet)

Queries the time stamp of internal operating system clock which is set to zero when TymServe is powered on. The time stamp of the internal operating system clock is in milliseconds.

history (RS-232, Telnet)

Displays the last fifteen commands that have been executed.

pause (RS-232, Telnet)

Waits for user specified number of milliseconds and then executes next command if it is provided in the same command line following the number. For example, the `pauses 5000 history` command waits for five seconds and then executes the `history` command. Input any integer number as the number of milliseconds to pause.

Peek <address> <count> (RS-232, Telnet)

Displays memory contents in number of bytes specified by count at location specified by address. The address and count can be hex numbers but should begin with '0x.'

where <address> = starting address of memory to be displayed.

<count> = number of bytes of memory to be displayed.

Memory contents in hex at memory location specified by input parameters.

compare <src address> <des address> <count> (RS-232, Telnet)

Compares memory contents of source and destination specified by addresses. If they are the same, nothing is returned. Otherwise only the contents that are different are displayed.

where <src address> =starting address of source.

<des address> =starting address of destination.

<count> = number of bytes to be compared.

repeat (RS-232, Telnet)

Repeats number of times specified by user to execute command prior to repeat commands in the same command line. Use any integer number for `repeat` in executing commands.

(RS-232, Telnet)

Provides shell command parsing a mark that indicates the end of command line.

? (RS-232, Telnet)

Displays various commands available in current directory for use on the TymServe.

Chapter 5: *SNMP Configuration and Control*

In This Chapter

This chapter reviews SNMP (Simple Network Management Protocol) configuration, including variables and security.

SNMP Configuration Overview

To use SNMPv1 set and request packets, the network parameters must be configured using either RS-232 or Telnet access methods.

Once the network parameters have been set, you can send SNMPv1 packets to configure the operating mode. Then, compile the ASN.1 datumMIB definition file provided on the SNMPv1 management platform. Select the variable `tsTengMode` to set the operating mode. The initial read community name is `public` and the initial read/write community name is `private`.

Datum has designed and implemented a custom MIB extension to complement our support of the MIB-II variable set. The datumMIB provides access to data and controls specific to the TymServe and NTP service. The datumMIB extension also provides SNMPv1 traps, which are generated by the TymServe in the event of NTP leap indicator changes or extended reference time source signal losses. An ASN.1 definition of the datumMIB extension is provided on an MS-DOS formatted diskette. This file is suitable

for compilation on any SNMP management platform which supports RFC 1155 (SMI), RFC 1213 (TRAPS), and RFC 1215 (OBJECT MACRO DisplayString).

Whatever your plans for SNMPv1 access, these community names should be changed for security reasons.

The following section covers the Datum MIB Extension, MIB compilation, and security aspects of the SNMP.

Datum MIB II Extension

The data available from the TymServe through SNMP is based on the MIB-II variable set which has been enhanced with a custom MIB extension to provide data unique to NTP and the TymServe. Manufacturer-specific or enterprise MIB extensions are given a unique identifier, or enterprise number, which defines where the extension is located in the MIB tree. Datum has been assigned an enterprise number of 601. Details about the MIB extension are in [“Appendix D: Datum MIB Extension” on page 87](#) of this User Guide.

Additional Stored MIB Variables

The first 39 characters of the sysName, sysContact, and sysLocation will be stored in flash EPROM and loaded during any subsequent initialization or powerup. You can set these variables through either the command interface or SNMP set requests.

MIB Compilation

Most SNMP management platforms are capable of reading MIB-II data. The Datum-specific MIB extension needs to be added to the manager. Typically, these MIB extensions are defined using a syntax known as ASN.1. The Datum MIB extension is provided on an MS-DOS format floppy disk and is defined using ASN.1, and includes imports from RFC 1155-SMI, RFC 1212, RFC 1213-MIB, and RFC 1215. Consult your SNMP manager documentation to determine how to compile the Datum MIB extension into your SNMP software package.

Security

Once the SNMP management software has been configured to recognize data from the TymServe, the security parameters on the manager need to be defined to match those set on the TymServe.

SNMPv1

The security parameters for SNMPv1 are based on a community name, which is a string of ASCII characters (“public”), and an IP address. The TymServe defines the IP address such that SNMPv1 packets will be accepted from any IP address which has a valid

community name. The community name in SNMPv1 dictates the level of access. The TymServe allows for the definition of two community names: one read-only, and one read-write. Consult your SNMP manager documentation to determine how to create an object and set the community names. Typically, the information required will be the IP address of the TymServe and the community names which were set through the command interface of the TymServe.

MIB-II Extension File

Datum MIB-II extension defined in the next section is available to users in the Utility Diskette shipped with the TymServe. The MIB file name is **TS2100.mib**. This file is also available through Datum's FTP site at **ftp.datum.com**, then click on **pub/NetProducts/TymServe2100**.

For Datum MIB Extension code and commands, see "Appendix D: Datum MIB Extension" on page 87.

Chapter 6: FAQ and Troubleshooting

In This Chapter

This chapter provides answers to frequently-asked questions, and solutions to problems that might arise while installing and operating the TymServe 2100LD.

Frequently Asked Questions

How can we obtain NTP client software to use with TymServe?

NTP client software information and configuration details are available from:

- <http://www.eecis.udel.edu/~ntp/>
- <http://www.microsoft.com/NTServer/nts/exec/vendors/freeshare/IClient.asp>
- <http://cs3.ecok.edu:457/NetAdminG/netadminN.about.html>

Client software and configuration information for Unix, Windows, and Novell platforms can be downloaded from these sites.

SNTP client software (DatumTime) is included with the TymServe hardware.

What are the main differences between SNTP and NTP clients?

SNTP is a Simple Network Time Protocol. It is based on RFC 1361/2030: it gets its time from the specified time servers of the machine on which it is installed. This protocol

cannot be configured to obtain time from an alternate time server if the primary server is down. This could be called as a short version of NTP client software.

NTP, Network Time Protocol, is based on RFCs 1305 and 1119 which can be configured to obtain and distribute the time on the network. It has a built-in algorithm that calculates the time accurately up to 1-10 milliseconds. The algorithm can be configured to obtain time from an alternate source in case the original time server fails or gets out of synchronization.

How does the TymServe 2100LD interface with SNMP?

The TS2100 is designed for a computer network. Computer networks typically use SNMP to monitor the devices on the network. The TS2100 reports alarms/traps if you have implemented SNMP.

Datum has written a .mib that can be compiled with SNMP management software. MIBs contain information specific to that device. Once compiled, the MIB can help the SNMP management software understand the status of the TS2100.

Is there a way to get GPS time instead of UTC time from the TymServe?

The TymServe normally provides UTC time. However, it can be configured to output GPS time—currently UTC + 13 seconds—by making several hardware changes to the unit.

What outputs are available on the TymServe 2100LD?

These are:

- Ethernet 10BaseT (RJ 45)
- RS-232 Serial Port (DTE, Sysplex Timer)
- RS-232 Serial Port (DCE) for Configuration/Status (Telnet)

How does the TymServe handle Leap Second?

Today's clocks keep pace with one another to within two or three millionths of a second over a year's time. However, the earth on its rotation might randomly accumulate almost a full second in a year. This time is deleted (or added, if needed) as a *leap second* from (or to) the UTC time on the last day of June or December in the affected year. This way, the clocks stay in step with the earth's rotation.

The GPS satellites send notice of an upcoming leap second about two months in advance. The TymServe receives this notice and, following NTP specifications, starts advising clients 24 hours in advance. At the leap second event, the TymServe will add or delete the leap second from the transmitted time.

NOTE: In the event of a leap second, if the time source is Freerun, you must pre-program the leap second event with the command **leap** so that TymServe can be notified and maintain time correctly.

What signal strengths are required by the TymServe receiver to start tracking?

TymServe requires four satellite signals with strengths greater than 6 dB to turn the tracking LED on. After the tracking LED is on, TymServe requires only one satellite signal to maintain its time. If it loses the fourth signal, the TymServe will automatically transfer to Freerun mode and will keep on providing time.

What does *doing position fixes error code: 1* mean?

This means that the TymServe does not have DC backup power supply. Ignore this message because the current design does not have DC backup power supply.

How do I check versions of the firmware in TymServe?

To check for the version of TymServe firmware:

1. Enter **version** in the serial or Telnet connection.
2. The version of firmware for the TymServe is displayed.

To check for the version of GPS receiver:

1. Enter **gpsversion** in the timing command line.
2. Enter the **gps directory** through the serial or Telnet connection.
3. The version of firmware for the GPS is displayed.

What is the maximum number of computers that can be networked to the TymServe?

TymServe acts as a standalone time server. Average time to process the NTP request is approximately four milliseconds. Therefore, TymServe can handle approximately 250 requests per second. However, clients running as Stratum 2 computers access TymServe in an interval of 64 to 65,536 seconds as the time progresses. Some clients request time only once an hour or once a day. The optimum number of computers that the TymServe can handle is based on the client NTP software/configuration, on the capability of the network, and on the acceptable level of load on the network.

What is the maximum antenna cable length for use with TymServe?

A maximum length of 300 feet can be used with the standard (Bullet II) antenna. From 300–500 feet, the High Gain Antenna option is required. If you need longer lengths, please contact Datum Technical Support.

What are the available antenna cable lengths and antenna requirements?

These are:

Cable length/cable type	Antenna
50'–100' Belden RG58:	Standard bullet-type
100'–300' Belden 9913:	Standard bullet-type
300'–500' Belden 9913:	High Gain
Over 500':	Contact Datum

What are some guidelines for correctly cutting the cable, using splitters, and using cable connectors?

Some critical “do’s and don’ts” are:

- *Do* use pre-made kits from Datum.
- *Do* install the antenna where there are no obstructions—either on the roof, or with a horizontal view of the horizon that is at least 30 degrees.
- *Do not* split the antenna cable signal to try to use the signal to drive other GPS devices.
- *Do not* cut the cable to a shorter length. Instead, bundle any excess cable. Correct antenna cable length—even if you do not “use it all”—is critical to proper TymServe operation, which should have a gain within the range of 15dB–25dB.

How do I set up a TymServe for operation once the antenna is installed?

Here are the steps:

1. Place the unit in the mounting rack.
2. Attach the antenna cable, power input, and network connection to the RJ 45 jack.
3. Switch on the power.
4. Enter the IP information by using the console connection.
5. Confirm the unit is in GPS mode by typing: `root tym mode 6 <return>`.
6. Wait for the Tracking and Locked lights to come on, about 15-30 minutes.

For more details about antenna installation, see [“Antenna Installation: GPS” on page 22](#).

How do I verify TymServe performance?

One way to do this is to establish a Telnet session with the TymServe, then:

1. Enter the command `root tym gps sat<return>`. This will show you the satellites currently viewed by the GPS module.
2. Enter `root tym gps sig <return>`. This will show you the signal strength of the satellites currently in view.
3. Enter `root tym gps health <return>`. This will show you the current system health status. Status Code 1 is good; other responses could indicate a problem.

How many satellites are necessary for me to operate TymServe?

Four. The unit will usually track six to eight satellites.

How do I know if the signal strength is good?

Any signal over 6 is good and usable by TymServe. The unit will continue to track a satellite down to 3 once it has acquired it at a level 6 or over.

How do I use the TymServe's HTML access page?

To do this:

1. Open your browser. (Netscape usually performs better than IE.)
2. On the address line, enter the IP address for your TymServe, in the standard quad notation (xxx . xxx . xxx . xxx), then <return>.
3. The page will open, and you will see the satellites currently being tracked by your TymServe.

How do I perform a firmware upgrade on the TymServe?

See [“Appendix C: Firmware Upgrade”](#) on page 83 for instruction on this.

Troubleshooting

The front panel LCD is unreadable

Wait until the unit is locked and tracking before attempting to adjust the front panel LCD. The LCD is made darker via Telnet. Go to the `root util` menu, and select `display contrast`. Enter 40000, a good baseline contrast level, and adjust up or down from there.

Tracking LED does not light up

During the initial warm-up cycle it may take 15-60 minutes to track the satellites' signals and turn the Tracking LED on. An unlit Tracking LED on the front panel means the timing source is either not available or not usable.

Make sure the correct timing source mode is selected in the Timing directory (for details on this, Chapter 4).

If the timing source mode is correct, check the antenna location and the cable connections. Be sure the type and length of the cable is correct (see Figure 2-1).

Locked LED does not light up

Once the four satellite signals reach sufficient strength to be received by the TymServe, its Tracking light comes on. Then the internal clock stabilizes, and the Locked LED light comes on. The Locked LED may take up to an hour to light.

If the Tracking LED light is on but the Locked light does not come on, then the TymServe's internal crystal may not be stable. In this case, please call Datum TymServe technical support.

TymServe does not respond to ping command

Establish a serial or Telnet connection and verify that the IP, subnet mask, and default gateway addresses are entered correctly in the **Network** directory of the TymServe.

Also check the Ethernet 10baseT cable connections between the RJ45 connector and the hub or network. If TymServe is directly connected to the computer, verify that the 10baseT cable is connected through the crossed-over connector or through the hub.

TymServe does not respond to NTP queries

Verify that the TymServe can be pinged (see above). If TymServe can be pinged, but it doesn't respond to NTP queries, then verify that the NTP software on your computers is set up properly, and also verify that the client has the correct IP address of the TymServe.

Cannot make Telnet connection

Only one Telnet connection is allowed at a time. Make sure that the TymServe can be pinged and then try again.

If you still are unable to make a Telnet connection, it is possible that the previous Telnet session is not disconnected yet. To disconnect the previous Telnet session, access TymServe through the serial B port and issue the `stop` command through the **network->Telnet** directory, or wait until the session is timed out after an hour. The other alternative is to power cycle the unit.

Cannot establish serial connection with the TymServe

Make sure that the connection is made with straight-through serial cable to Serial Port B, *not* Serial Port A.

Also check that the configuration settings are set to a VT100 ASCII terminal using 9600, 8, N, 1. For more details, see [“Chapter 3: TymServe 2100LD Operation and Time-Related Protocols”](#) on page 27.

My TymServe won't track satellites

Check the following:

Possible cause of tracking problems:	How to fix:
Antenna not positioned correctly	Be sure antenna is on the roof or location with a view of at least 30° of the horizon, and at least two meters from other active receiving antennas and shielded from transmitting antennas
Cable is cut to the wrong length, causing dB gain problems	Replace with cable of correct length
Incorrect connector(s) at the end(s) of the cable(s) or along the cable run, causing dB gain problems	Replace with correct connector
Incorrect use of splitters, including signal splitting to another GPS device or cable cut to wrong length	Replace with splitter that does not “share” signal, on a cable of correct length

During firmware upgrade the TFTP session fails

Sometimes it takes three to four attempts to complete the Firmware upgrade process. When there is a failure in the TFTP downloading portion of the upgrade, it could be due to one of the following reasons:

Alert	Cause	Fix
The download-process spinning bar stops after only a few rotations	The TymServe cannot receive data from the TFTP server because the TFTP server configuration is not correct	Make sure the firmware file name and host IP address are entered correctly in the TymServe. Make sure the firmware file is placed in the correct directory in the TFTP server.
The download-process spinning bar spins for a long time, then stops before finishing the download	The traffic on the network is interfering with the downloading process	Excessive traffic can cause packet collision, hindering the download process. To fix this, have the TymServe and host machine connected to the same network hub ; this reduces the chances of traffic collision

TFTP is a UDP-based, connectionless protocol.

Modified files are being “lost” by the file server in a distributed computing environment

File servers will typically compare a submitted file time stamp to that of the same named file resident on the server. Only if the submitted file is dated later will it be accepted. In poorly synchronized networks it is possible for a user to modify a file, such as in a software build, then submit it to the file server, and have it rejected without the user’s knowledge—all because the user’s workstation has a clock with the incorrect time which results in an incorrect file time stamp.

The solution is to set up the network with a hierarchical time distribution system based on NTP. TymServe receives time from the Global positioning System and distributes time to workstations further down the hierarchy by using the Network Time Protocol (NTP). This is a public domain protocol that can be installed on user workstations, then synchronized to the Stratum 1 TymServe to within 1–10 milliseconds. Thus files would be accurately time stamped and users could be sure that modified files will be correctly accepted and installed on the server.

Some users are denied access to the network by network security algorithms.

One common threat to network security is the so-called “man in the middle” attack: a packet or series of packets are intercepted, modified, and then replayed by the attacker to simulate a “good guy”.

A simple protection to this attack is to provide packet-filtering algorithms whereby a packet is accepted only if it has a current secret time stamp. An example is a filter that screens out packets older than one second. If a user’s workstation clock is off by more than the filter’s time window.

The solution is the same as to the previous question: set up the network with a hierarchical time distribution system based on NTP. The accurate time stamps provided by such a time distribution system would make it impossible to alter packets without detection.

Our local Stratum 2 time server, a salvaged workstation running in the computer vault, “hung” but we didn’t know it until we got denial of service complaints from users.

Synchronizing to remote time servers is possible, but more users now say this results in a *decrease* in control. Public domain servers are fine for redundant backup, but for mission-critical LANs the primary source of time should be a dedicated time server such as TymServe. Many processes are dependent on accurate workstation-to-workstation and workstation-to-server synchronization. One “hung” event is usually enough to convince an IT manager to install a dedicated, standalone TymServe in the computer vault as a dependable solution.

Appendix A: Data Sheet Specifications

Table A-1: Data Sheet Specifications: TymServe 2100LD

Component	Specifics	Description
Network Interface	Ethernet over 10BaseT	IEEE 802.3 specifications
	Connection	10BaseT, Twisted Pair RJ45
	Time Protocols	NTP Version 2 (RFC 1119) NTP Version 3 (RFC 1305) SNTP (RFC 1361) Time Protocol (RFC 868) Daytime Protocol (RFC 867)
	Supported Protocols	DHCP, BOOTP, and TFTP MD5 Authentication (NTP) Telnet HTTP/HTML Status Page SNMP v1 with custom MIB II Extension
Serial Connection	Port A	DTE-style RS-232 port with DB9 (male) connector for Sysplex timer. Default 9600 baud, 8 data bits, 1 start/stop bit, no parity
	Port B	DCE-style RS-232 port with DB9 (female) connector for status and configuration. Default 9600 baud, 8 data bits, 1 start/stop bit, no parity
Timing Accuracy	Network	1–10 milliseconds, typical
	Internal Clock	<10 microseconds, relative to UTC, GPS tracking
GPS Receiver	Channels	Six
	Frequency	1.575 GHz, C/A Code
	GPS	<2 microseconds, relative to UTC
Chassis	A/C Power In	100–130V A/C / 220–240V A/C, 48–440Hz, 20W
	Size and Weight	1.75”h x 17.0”w x 9.5”d 1U Height Rack Mount, <10 lbs. (4.5Kg) 19” width with Rack Mount ears
Operating and Storage Environments	Temperature	0° C to 50° C Operating -20° C to 70°C Non-operating
	Relative Humidity	10%–80% Operating (non-condensing) 5%–95% Non-operating (non-condensing)
Mean Time Between Failures (MTBF)	Average Time	56,000 hours

Appendix B: Input/Output Connectors

Overview

The TymServe 2100LD input/output connectors located on the rear panel of the unit are shown in Figure B-1 below. These connectors provide inputs for timing sources, general purpose timing outputs, the GPS connector, two RS-232 Serial Ports, and the A/C power entry.

TymServe 2100LD: Front and Rear Panels

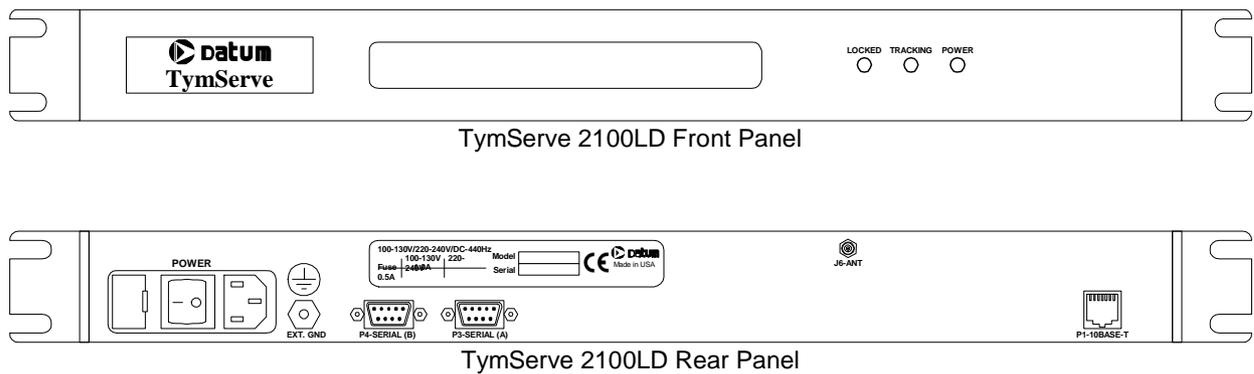


Figure B-1 Front and Rear Views of the TymServe 2100LD

Pin Descriptions

P1: Ethernet RJ45	
<i>Description: 8-pin Phone Jack, Mfr: AMP, Part # 555153-1</i>	
Pin Number	Description
1	TX (+)
2	TX (-)
3	RX (+)
4	N/C
5	N/C
6	RX (-)
7	N/C
8	N/C

P2: DCLS I/O	
<i>Description: 9-pin "D" Socket, Mfr: AMP, Part # 869520-2</i>	
Pin Number	Description
1	External Oscillator Control Voltage
2	Ground
3	Ground
4	DCLS IN (+ or single-ended)
5	DCLS IN (-)
6	DCLS OUT (+)
7	DCLS OUT (-)
8	Reserved (+)
9	Reserved (-)

P3: Serial A (Data Terminal Port/DTE)	
<i>Description: 9-pin “D” Plug, Mfr: AMP, Part # 869436</i>	
Pin Number	Description
1	RS-232 Data Carrier Detect (in)
2	RS-232 Receive Data (in)
3	RS-232 Transmit Data (out)
4	RS-232 Data Terminal Ready (out)
5	Ground
6	RS-232 Data Set Ready (in)
7	RS-232 Request to Send (out)
8	RS-232 Clear to Send (in)
9	RS-232 Ring Indicator (in)

P4: Serial Port B (Setup Port: DCE)	
<i>Description: 9-pin “D” Plug, Mfr: AMP, Part #869436-1</i>	
Pin Number	Description
1	N/C
2	RS-232 Transmit Data (out)
3	RS-232 Receive Data (in)
4	N/C
5	Ground
6	N/C
7	RS-232 Clear to Send (in)
8	RS-232 Request to Send (out)
9	N/C

Appendix D: Datum MIB Extension

Overview

The following is code and commands for the use of Datum MIB Extension. Please also refer to Chapter 5 for more information about Datum MIB.

```
DATUM DEFINITIONS ::= BEGIN

IMPORTS
OBJECT-TYPE
FROM RFC-1212
DisplayString
FROM RFC1213-MIB
TRAP-TYPE
FROM RFC-1215
enterprises
FROM RFC1155-SMI;

datumMIB  OBJECT IDENTIFIER ::= {enterprises 601}

bancomm  OBJECT IDENTIFIER ::= {datumMIB 1}
timing    OBJECT IDENTIFIER ::= {datumMIB 2}
austron  OBJECT IDENTIFIER ::= {datumMIB 3}
fts      OBJECT IDENTIFIER ::= {datumMIB 4}
efratom  OBJECT IDENTIFIER ::= {datumMIB 5}
experiment OBJECT IDENTIFIER ::= {datumMIB 99}

productsOBJECT IDENTIFIER ::= {bancomm 1}

ts2000    OBJECT IDENTIFIER ::= {products 1}
ts2100    OBJECT IDENTIFIER ::= {products 2}
```

```

version      OBJECT IDENTIFIER ::= {ts2100 1}

ntp          OBJECT IDENTIFIER ::= {version 1}
tyming      OBJECT IDENTIFIER ::= {version 2}
gps         OBJECT IDENTIFIER ::= {version 3}
dialup      OBJECT IDENTIFIER ::= {version 4}
net         OBJECT IDENTIFIER ::= {version 5}
etc         OBJECT IDENTIFIER ::= {version 6}

```

```

ntpLeapIndicator OBJECT-TYPE
    SYNTAX INTEGER {
        nowarning(1),
        leapinsertion(2),
        leapdeletion(3),
        unsynchronized(4)}
    ACCESS read-write
    STATUS mandatory

```

DESCRIPTION

"NTP Leap Indicator. This is a two-bit code warning of an impending leap second to be inserted into the NTP timescale. The bits are set before 23:59 on the day of insertion and reset after 00:00 on the following day. This causes the number of seconds (rollover interval) in the day of insertion to be increased or decreased by one. In the case of primary servers the bits are set by operator intervention, while in the case of secondary servers the bits are set by the protocol. The two bits, bit 0 and bit 1, respectively, are coded as follows:

```

=====
00    no warning
01    last minute has 61 seconds
10    last minute has 59 seconds
11    alarm condition(clock not synchronized)
=====

```

In all except the alarm condition(11), NTP itself does nothing with these bits, except pass them on to the time-conversion routines that are not part of NTP. The alarm condition occurs when, for whatever reason, the local clock is not synchronized, such as when first coming up or after an extended period when no primary reference source is available."

```

::= {ntp 1}

ntpMode OBJECT-TYPE

```

```

SYNTAX INTEGER {
    unspecified (1),
    symactive (2),
    sympassive (3),
    client (4),
    server (5),
    broadcast (6),
    reservedctl (7),
    reservedpriv (8)}

```

ACCESS read-only

STATUS mandatory

DESCRIPTION

"NTP association mode. This is an integer indicating the association mode, with values coded as follows:

```

=====
0    unspecified
1    symmetric active
2    symmetric passive
3    client
4    server
5    broadcast
6    reserved for NTP control messages
7    reserved for private use
=====

```

Note: In the Datum 2100 series, this value is currently ALWAYS set to 4 (server only)."

::= {ntp 2}

ntpStratum OBJECT-TYPE

```

SYNTAX INTEGER (0..255)

```

ACCESS read-only

STATUS mandatory

DESCRIPTION

"Current NTP stratum level. This is an integer indicating the stratum of the local clock with values defined as follows:

```
=====
0    unspecified
1    primary reference (e.g., calibrated atomic clock, radio clock)
2-255 secondary reference (via NTP)
=====
```

Note: In the Datum 2100 series, this value is currently ALWAYS 1 (primary reference).
 ::= {ntp 3}

ntpPrecision OBJECT-TYPE

```
SYNTAX INTEGER (-127..127)
ACCESS read-only
STATUS mandatory
DESCRIPTION
```

"Current NTP precision value. This is a signed integer indicating the precision of the various clocks, in seconds to the nearest power of two. The value must be rounded to the next larger power of two; for instance, a 50-Hz (20ms) or 60-Hz (16.17ms) power-frequency clock would be assigned the value -5 (31.25ms), while a 1000-Hz (1ms) crystal-controlled clock would be assigned the value -9 (1.95ms)."

::= {ntp 4}

ntpRefClkID OBJECT-TYPE

```
SYNTAX DisplayString (SIZE (1..40))
ACCESS read-only
STATUS mandatory
DESCRIPTION
```

"NTP Reference Clock Identifier. This is a 32 bit code 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 spec, the following are suggested ASCII identifiers:

```
=====
```

DCN	DCN routing protocol
NIST	NIST public modem
TSP	TSP time protocol
DTS	Digital Time Service

ATOM	Atomic clock (calibrated)
VLF	VLF radio (OMEGA,etc.)
callsign	Generic radio
LORC	LORAN-C radionavigation
GOES	GOES UHF environment satellite
GPS	GPS UHF satellite positioning

=====

The following ref ids are used by the 2100:

GPS TS2100-GPS (GPS satellite)
 FREE TS2100-ALL (INTERNAL CLOCK)"

::= {ntp 5}

ntpRefTime OBJECT-TYPE

SYNTAX DisplayString (SIZE(1..40))

ACCESS read-only

STATUS mandatory

DESCRIPTION

"NTP Reference Timestamp. This is the time, in timestamp format (converted to DisplayString), when the local clock was last updated. If the local clock has never been synchronized, the value is zero."

::= {ntp 6}

ntpVersion OBJECT-TYPE

SYNTAX INTEGER (0..127)

ACCESS read-only

STATUS mandatory

DESCRIPTION

"NTP Version. This is an integer indicating the version number of the sender. NTP messages will always be sent with the current version number NTP.VERSION and will always be accepted if the version number matches NTP.VERSION. Exceptions may be advised on a case-by-case basis at times when the version number is changed."

=====

Note: The 2100 series was implemented using NTP version 3. However, the 2100 series will accept a version of 2 or 3 and return the same version number in the packet. This behavior is subject to change."

::= {ntp 7}

ntpAuthOnOff OBJECT-TYPE

SYNTAX INTEGER (0..1)

ACCESS read-write

STATUS mandatory

DESCRIPTION

"Enable or disable MD5 Authentication Mode."

::= {ntp 8}

ntpAuthOnlyOnOff OBJECT-TYPE

SYNTAX INTEGER (0..1)

ACCESS read-write

STATUS mandatory

DESCRIPTION

"Enable or disable MD5 Authentication Only Mode."

::= {ntp 9}

ntpNumberRequests OBJECT-TYPE

SYNTAX INTEGER (0..32768)

ACCESS read-write

STATUS mandatory

DESCRIPTION "This variable is a rollover counter which reflects the number of ntp packets received by the 2100. It is valid for all versions of the 2100. The counter may be set to 0."

::= {ntp 10}

ntpLeapChange TRAP-TYPE

ENTERPRISE ntp

VARIABLES {ntpLeapIndicator}

DESCRIPTION "The trap indicates a change in state of the ntp leap indicator. It will pass the new value of the leap indicator."

::=0

tyimingTimeSrcUTCOffset OBJECT-TYPE

SYNTAX INTEGER (-11..12)

ACCESS read-write

STATUS mandatory

DESCRIPTION "This variable is valid for the 2100-IRIG or the 2100-GPS when operating in IRIG decoder mode. The variable represents the offset of the input timecode from UTC in signed hours. The allowable values for this variable are -11 through 12. If this variable is queried on the 2100-ACTS it will return 0."

::= {tyiming 1}

tyimingStatus OBJECT-TYPE

SYNTAX DisplayString (SIZE(1..40))

ACCESS read-only

STATUS mandatory

DESCRIPTION "This variable reflects the current status information on the 2100 Time and Frequency Processor. This info is only available on the GPS versions. The string will indicate either Tracking or Flywheeling. This is a direct reflection of bit 0 of the 2100 status bit 0. Bits 1 & 2 are not relevant for network users.

Status Register Definitions

=====
bit 0 1 = flywheeling(not locked)

0 = locked(to selected reference)

bit 1 1 = time offset > X microseconds

0 = time offset < X microseconds

(X = 2 for GPS)

bit 2 1 = frequency offset > 5E8

0 = frequency offset < 5E8

====="

::= {tyiming 2}

tyimingMode OBJECT-TYPE

SYNTAX INTEGER {

timecode (1),

freerun (2),

internal (3),

gps (7)}

ACCESS read-write
STATUS mandatory
DESCRIPTION "Operating mode of the timing engine."
::= {tyiming 3}

tyimingTime OBJECT-TYPE
SYNTAX DisplayString (SIZE(1..40))
ACCESS read-write
STATUS mandatory
DESCRIPTION "Time returned from the time registers."
::= {tyiming 4}

tyimingEventTime OBJECT-TYPE
SYNTAX DisplayString (SIZE(1..40))
ACCESS read-only
STATUS mandatory
DESCRIPTION "Time returned from the event registers."
::= {tyiming 5}

tyimingYear OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-write
STATUS mandatory
DESCRIPTION "Year used by timing engine."
::= {tyiming 6}

tyimingInTcFormat OBJECT-TYPE
SYNTAX INTEGER {
 tcIRIGA (65),
 tcIRIGB (66),
 tc2137 (67),
 tcNASA36 (78),
 tcXR3 (88)}
ACCESS read-write

```
STATUS mandatory
DESCRIPTION "Format of the input timecode (i.e. B,N)."
::= {tyiming 7}

tyimingInTcModulation OBJECT-TYPE
    SYNTAX INTEGER {
        dcllevel (68),
        modulated (77)}
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION "AM or DC format timecode."
::= {tyiming 8}

tyimingOutTcFormat OBJECT-TYPE
    SYNTAX INTEGER {
        tcIRIGB (66)}
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION "Timecode Generator output format."
::= {tyiming 9}

tyimingVersion OBJECT-TYPE
    SYNTAX DisplayString (SIZE(1..40))
    ACCESS read-only
    STATUS mandatory
    DESCRIPTION "String containing timing engine version and
    creation date and time."
::= {tyiming 10}

tyimingLeapSeconds OBJECT-TYPE
    SYNTAX INTEGER (0..255)
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION "Current leap second count in timing engine."
```

::= {tyiming 11}

tyimingD2a OBJECT-TYPE

SYNTAX INTEGER (0..65535)

ACCESS read-write

STATUS mandatory

DESCRIPTION "oscillator disciplining d2a value."

::= {tyiming 12}

tyimingKval OBJECT-TYPE

SYNTAX DisplayString (SIZE(1..40))

ACCESS read-write

STATUS mandatory

DESCRIPTION "Oscillator disciplining filter constant value."

::= {tyiming 13}

tyimingFlyPeriod OBJECT-TYPE

SYNTAX INTEGER

ACCESS read-write

STATUS mandatory

DESCRIPTION

"Period in seconds of allowable flywheeling before the tyimingFlywheel trap will be sent. If the value is set to 0, the trap will never be generated."

::= {tyiming 14}

tyimingFlywheel TRAP-TYPE

ENTERPRISE tyiming

VARIABLES {ntpRefTime}

DESCRIPTION

"The trap is intended to provide notification of extended flywheeling events. The user programmable value tyimingFlyPeriod is the number of seconds the 2100 may flywheeling before a trap is sent."

::=0

gpsPosition OBJECT-TYPE

SYNTAX DisplayString (SIZE(1..80))

ACCESS read-only

STATUS mandatory

DESCRIPTION

"This variable returns a position fix. It is only valid on the 2100-GPS. The returned string will contain the latitude & longitude expressed in degrees & minutes and the altitude in meters. If this variable is queried on the 2100-ACTS the returned value will be N/A."

::= { gps 1 }

gpsVelocity OBJECT-TYPE

SYNTAX DisplayString (SIZE(1..80))

ACCESS read-only

STATUS mandatory

DESCRIPTION

"This variable returns a velocity fix. It is only valid on the 2100-GPS. The returned string will contain the East-North-Up velocity expressed in meters/second. If this variable is queried on the 2100-ACTS the returned value will be N/A."

::= { gps 2 }

gpsUTCOffset OBJECT-TYPE

SYNTAX INTEGER (0..127)

ACCESS read-write

STATUS mandatory

DESCRIPTION

"This variable returns the current offset between the monotonic time maintained by the GPS satellite constellation and UTC time. This value is commonly referred to as the leap second count. It is only valid on the 2100-GPS. This value is obtained from the GPS receiver but there may be a time lag between the incidence of a leap second correction and the capture of that correction by the 2100-GPS. For this reason the user is allowed to program the leap second value which will be used until the 2100-GPS receives the leap second count from the GPS satellite constellation. If this variable is queried on the 2100-ACTS the value returned will be 0."

::= { gps 3 }

gpsHealth OBJECT-TYPE

SYNTAX DisplayString (SIZE(1..80))

ACCESS read-only

STATUS mandatory

DESCRIPTION "Health packet from GPS."
::= { gps 4 }

gpsAllInView OBJECT-TYPE
SYNTAX DisplayString (SIZE(1..80))
ACCESS read-only
STATUS mandatory
DESCRIPTION "Satellites in view packet from GPS."
::= { gps 5 }

gpsMode OBJECT-TYPE
SYNTAX INTEGER (0..20)
ACCESS read-write
STATUS mandatory
DESCRIPTION "GPS Receiver Operating Mode."
::= { gps 6 }

gpsDynamicsCode OBJECT-TYPE
SYNTAX INTEGER { land (1), sea (2), air (3), static (4) }
ACCESS read-write
STATUS mandatory
DESCRIPTION "GPS Receiver Dynamics Code."
::= { gps 7 }

dialForceCall OBJECT-TYPE
SYNTAX INTEGER (0..1)
ACCESS read-write
STATUS mandatory
DESCRIPTION "The variable is used to either initiate a call to the NIST ACTS service or abort a call that is in progress. It is only valid on the 2100-ACTS. Reading this value will return abort(0) if offline and call(1) if online. Sending a set of this value to 0 or 1 will cause the 2100-ACTS to take the appropriate action."
::= { dialup 1 }

dialCallRefTime OBJECT-TYPE
SYNTAX DisplayString (SIZE(1..40))

ACCESS read-write

STATUS mandatory

DESCRIPTION "FORMAT: MM/DD/HH. All 8 digits are required for set requests. Use \ or / as delimiters. The variable is used to read or set the call reference time. It is only valid on the 2100-ACTS. For more information on this variable, refer to the *TymServe 2100LD User Guide*. If this variable is queried on the 2100-GPS it will return N/A."

::= {dialup 2}

dialCallInterval OBJECT-TYPE

SYNTAX DisplayString (SIZE(1..40))

ACCESS read-write

STATUS mandatory

DESCRIPTION "FORMAT: MM/DD/HH. All 8 digits are required for set requests. Use \ or / as delimiters. The variable is used to read or set the call interval time. It is only valid on the 2100-ACTS. For more information on this variable, refer to the *TymServe 2100LD User Guide*. If this variable is queried on the 2100-GPS it will return N/A."

::= {dialup 3}

dialCallOnReset OBJECT-TYPE

SYNTAX INTEGER (0..1)

ACCESS read-write

STATUS mandatory

DESCRIPTION "The variable is used to read or set the 2100-ACTS Reset behavior. It is only valid on the 2100-ACTS. For more information on this variable, refer to the *TymServe 2100LD User Guide*. If this variable is queried on the 2100-GPS it will return 0."

::= {dialup 4}

dialInitString OBJECT-TYPE

SYNTAX DisplayString (SIZE(1..40))

ACCESS read-write

STATUS mandatory

DESCRIPTION "The variable is used to read or set the NIST ACTS dial prefix. It is only valid on the 2100-ACTS. For more information on this variable, refer to the *TymServe 2100LD User Guide*. If this variable is queried on the 2100-GPS it will return N/A."

::= {dialup 5}

dialPhonePrefix OBJECT-TYPE

SYNTAX DisplayString (SIZE(1..40))

ACCESS read-write

STATUS mandatory

DESCRIPTION "The variable is used to read or set the NISTACTS dial prefix. It is only valid on the 2100-ACTS. For more information on this variable, refer to the *2100LD User Guide*. If this variable is queried on the 2100-GPS it will return N/A."

::= {dialup 6}

dialPhoneNumber OBJECT-TYPE

SYNTAX DisplayString (SIZE(1..40))

ACCESS read-write

STATUS mandatory

DESCRIPTION "The variable is used to read or set the NISTACTS phone number. It is only valid on the 2100-ACTS. For more information on this variable, refer to the *2100LD User Guide*. If this variable is queried on the 2100-GPS it will return N/A."

::= {dialup 7}

dialServiceType OBJECT-TYPE

SYNTAX INTEGER (0..6)

ACCESS read-write

STATUS mandatory

DESCRIPTION "The variable is used to read or set the type of time service being accessed."

::= {dialup 8}

netTftpHost OBJECT-TYPE

SYNTAX DisplayString (SIZE(1..40))

ACCESS read-write

STATUS mandatory

DESCRIPTION "Ip address of tftp host machine."

::= {net 1}

netTftpFile OBJECT-TYPE

SYNTAX DisplayString (SIZE(1..40))

ACCESS read-write

STATUS mandatory

DESCRIPTION "File name of boot file image for tftp."
::= {net 2}

netAutoRestart OBJECT-TYPE
SYNTAX INTEGER (0..1)
ACCESS read-write
STATUS mandatory
DESCRIPTION "Enable or disable automatic restarts after downloading new firmware."
::= {net 3}

netRestart OBJECT-TYPE
SYNTAX INTEGER (0..1)
ACCESS write-only
STATUS mandatory
DESCRIPTION "Force a restart of the 2100."
::= {net 4}

netAutoTftp OBJECT-TYPE
SYNTAX INTEGER (0..1)
ACCESS read-write
STATUS mandatory
DESCRIPTION "Enable or disable automatic tftp downloads on power up."
::= {net 5}

netTftpSession OBJECT-TYPE
SYNTAX INTEGER (0..1)
ACCESS read-write
STATUS mandatory
DESCRIPTION "Start or stop a tftp session."
::= {net 6}

netAutoDhcp OBJECT-TYPE
SYNTAX INTEGER (0..1)
ACCESS read-write

STATUS mandatory
DESCRIPTION "Enable or disable automatic bootp on power up."
::= {net 7}

netDhcpSession OBJECT-TYPE
SYNTAX INTEGER (0..1)
ACCESS read-write
STATUS mandatory
DESCRIPTION "Start or stop a bootp session."
::= {net 8}

etcBootVersion OBJECT-TYPE
SYNTAX DisplayString (SIZE(1..40))
ACCESS read-only
STATUS mandatory
DESCRIPTION "Version and creation date and timestamp for the bootstrap firmware."
::= {etc 1}

etcOpVersion OBJECT-TYPE
SYNTAX DisplayString (SIZE(1..40))
ACCESS read-only
STATUS mandatory
DESCRIPTION "Version and creation date and timestamp for the runtime firmware."
::= {etc 2}

etcSerialNbr OBJECT-TYPE
SYNTAX DisplayString (SIZE(1..40))
ACCESS read-only
STATUS mandatory
DESCRIPTION "Unique serial number burned into each unit."
::= {etc 3}

etcImageLoc OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-write

```
        STATUS mandatory
        DESCRIPTION "Start location for the image download."
 ::= {etc 4}

etcInfo OBJECT-TYPE
    SYNTAX INTEGER (0..65535)
    ACCESS read-write
    STATUS mandatory
DESCRIPTION "Get or set the value of the info bit on the 2100. Not used in standard
product at this time."
 ::= {etc 5}
etcSysplexOnOff OBJECT-TYPE
    SYNTAX INTEGER (0..1)
    ACCESS read-write
    STATUS mandatory
DESCRIPTION "Enable or disable the sysplex first protocol output on the 2100 Serial
Port."
 ::= {etc 6}

END
```

Appendix C: Firmware Upgrade

Overview

This *Appendix C* supplements the release file containing the Motorola S-Record for the new firmware image.

There are two ways of loading the new firmware image onto your TymServe:

- Remote TFTP protocol loads the new image from the TFTP server through an Ethernet connection to TymServe (preferred method)
- Local RS232: Send the text file through your connection to TymServeThrough the Serial Port you connect to the TymServe command shell (slower)

Either of these methods requires that the new firmware image be downloaded to a local machine on your network.

The program code that operates TymServe is stored in the flash or non-volatile RAM. A **boot** section is stored separately from the program code to allow for recovery in the event of a catastrophic error during the download of a program update. If such an event occurs, the affected TymServe can be power cycled and will recover to a point sufficient to allow a reload of the program update.

Readability of Displays

Some units have what initially look like unreadable displays. To fix this, adjust the contrast to a readable level by using the 4 or 9 buttons to make the screen text darker or lighter.

Before You Start the Firmware Upgrade

The latest upgrades of firmware are available for download from the Datum FTP site at <ftp://ftp.datum.com/SanJose/NetProducts/TymServe2100LD/>. The latest version of firmware is always on the web site.

- TymServe 2100LD Firmware Update Instructions are found in `Upgrade.txt`
- Release notes (`Release.txt`) are also available at the FTP site; these tell you what is new and what is changed in the latest release of firmware.
- Image filename: `ts211d.hex`.

NOTE: When downloading the `ts211d.zip` file, don't unzip the file until you have it on the computer you intend to run the upgrade from. This way, either Win32 or UNIX will handle the translation when unzipping.

- Image version: the version specified in `Release.txt`

To download the `ts211d.hex` file, you may use either FTP as **anonymous** user, or a Web browser.

NOTE: Although the firmware image file has an extension hex it is *not* a binary file. It is ASCII so translation *must be enabled* when flipping the file back and forth across UNIX and DOS machines. To be safe, use the command `<type ascii>` before transferring the file to any machine by FTP. If you use a GUI FTP client, you must find and disable any auto-sensing file filter. Once you have downloaded the new firmware image, refer to the notes that follow for examples of typical installation.

TFTP Download

Overview

If you do not have a TFTP server available, some shareware TFTP server applications are available. For instance, 16 and 32 bit versions for Microsoft Windows are available from Datum's FTP site at `ftp://ftp.datum.com/SanJose/NetProducts/TymServe2100/`. Download the `3cs117.zip` file. If you have a Unix platform available, it is likely that it includes a TFTP server. Contact your network administrator for details.

TFTP Server

On the available TFTP server, install the new firmware image in a location accessible to the TFTP server daemon. This may be accomplished with TFTP upload, FTP, or even a Unix `cp` depending on your setup.

On the TymServe, use the shell to change to the net directory (root net).

Automatic Restart

If you would like the TymServe 2100LD to automatically restart after TFTP downloads, confirm that the auto mode is enabled in the 'network' submenu. (root net auto on).

Then execute following commands:

```
root net file <filename>
root net host <your TFTP server IP in dotted quad notation>
root net TFTP start
```

A spinning bar displays while the image is being downloaded.

If the indicator spins a few times and then stops, or spins for longer than 10 minutes without stopping, an error has occurred. For troubleshooting such an error, see [“Chapter 6: FAQ and Troubleshooting” on page 69](#).

Serial Download

These are the instructions for downloading a firmware upgrade to the TymServe using the RS-232 serial connection.

NOTE: If you are using another OS (such as Unix), translate the information and settings provided here into commands suitable for your system. If there is an error, it is probably because you need the proper CR-LF sequences at the end of each S-Record.

Serial Installation to Windows

To prepare for installation on Windows:

1. Install the file on your host computer.
2. Connect the host computer to the target TymServe by using a standard RS-232 cable.
3. Start Windows.

To install upgrade files for your TymServe:

1. In Windows Start Menu, choose Programs->Accessories->HyperTerminal.
2. Create new Hyperterminal connection specifying the following:
 - Direct to COMx (x = Serial Port)
 - 9600, 8, N, 1
 - XOFF/XON flow control
 - ASCII setup (do NOT append lf to outbound text)
3. In the main window, press <Enter> a few times to get a ? prompt.
4. type **root** <Enter><Enter> to reach the base of the command tree with
 - timing/
 - network/
 - serial/
 and so on
5. Type **serial** <Enter> to go to the serial directory.
6. Type ? <Enter> and look for a command called **download**. This is what you are going to use.
7. Type **download** <Enter> and you should see a spinning bar display. This means the TymServe is waiting for data.
8. Go to **Transfers**-> Send text file. Find the firmware file and start sending.

NOTE: This download could take at least 10 minutes. You should still see the spinning bar which indicates that the listen thread is either waiting or receiving data. If you see the display continuously displaying messages of `Invalid Command` then the translation mode is wrong, and you should change the translation mode.

Troubleshooting

If the download fails through either the TFTP or Serial methods, *do not reset your TymServe*. Once you have started the download process, the current image is erased in flash memory. However, a copy of the current image is loaded in RAM and running, which guarantees a normal operation unless it is restarted.

The intrinsic command `trace` may display data which will help you determine the source of the error. Once you have entered this command, do the following:

1. Stop the current transfer (`root net tftp stop`)

2. Check to see that the configuration data required for TFTP (ip, mask, route, host, file) is correct, then try the TFTP download again.
3. If this fails, try using a TFTP client to download the new firmware to a test platform (Unix or windows) to determine whether the error is on the TFTP server side or the TymServe side.
4. If you continue to experience difficulties, try using the serial download paradigm detailed earlier in this section.

NOTE: In the event that a restart is required after failure in downloading the new firmware, all is not lost. A permanent 'boot' image is programmed into the TymServe. While this version of firmware does not have all the capabilities of the standard code (no SNMP, no HTTP, and so forth), it does have all necessary components to allow you to download a new firmware.

After the Download

After the download completes, the system will reboot.

When the system comes back up, type **ver** <Enter> to display the version number and the updated version information.

Confirmation Message

After the firmware has been updated, the front of the TymServe will display ***** err *** Flash Env** in the front panel. This is normal after new firmware has been downloaded and indicates that the flash environment size has changed, and all user programmable values (IP) are reset to their default settings.

NOTE: You will have to re-enter the settings to the TymServe, such as IP, subnet, gateway, and host. Once the program update has been successfully downloaded, it will be stored in non-volatile RAM.

Next Step

Next, the TymServe can be restarted, either locally or remotely, and will start using the new program code.

Appendix E: Glossary

Time Glossary

This section defines some of the commonly-used TymServe and network time-related terms.

For additional details about time-related concepts, see the section [“Frequently Asked Questions”](#) on page 69, in Chapter 6 in this *User Guide*.

Access Control

Network managers define access control by requiring authentication of the user’s identity before permitting or limiting entry to a network or server resource/printer.

ACTS

Automated Computer Time System, a NIST service that provides announced time via telephone.

Advanced Encryption Standard (AES)

Developed by NIST and private companies, this standard is 256-bit based and is a stronger defense for sensitive material when compared to 40-bit or 128-bit.

Algorithm

Any mechanical or recursive computational procedure.

ANSI

American National Standards Institute. The agency that sets US standards in such areas as computer communications.

Antiwarrant

Attribute certificate that has the same expire date as its valid date; in other words, it was never valid. This is still sent, at times, because it contains other information that the system needs. See also *Warrant*

API

Application Program Interface. This interface allows software developers to write their software so that it can communicate with the computer's operating system or other programs.

ASCII

American Standards Code Information Interchange, a code in which each alphanumeric character is represented as a number from 0 to 127, in binary code so the computer can understand it. Its simplicity allows diverse computers to understand one another.

ATM

Asynchronous Transfer Mode, or ATM switching. This is a type of packet switching that makes it possible to transmit data at high speeds over a network. It also allows dynamic

allocation of bandwidth, meaning users get only the bandwidth they need and are charged accordingly.

Audit Trail

A series of events, usually kept in and managed by a computer-based log, that give proof of a defined activity.

Authentication

Method by which a person is verified to be who they say they are, by password or other means.

Authorization

Method by which an authenticated person is allowed certain access to the system, via password or other means.

BCD

Binary Coded Decimal. Also called packed decimal, this is the representation of a number by using 0s and 1s, or four-bit binary numbers. So the number 29 would be encoded as 0010 1001.

CA

Certificate Authority

Calibration

To fix the graduations of time measurement against the established national standard, including any periodic corrections that should be made.

CDMA

Code Division Multiple Access. A technique of multiplexing, also called spread spectrum, in which analog signals are converted into digital form for transmission.

CDSA

Common Data Security Architecture. This describes the security structure for the entire network. It is unique to each network because security is managed differently for each.

Certificate

Often called “digital certificates”, this is a credential that includes security information and keys.

Certificate Authority (CA)

Independent organization or vendor that acts as a notary, verifying the identification of involved parties, and issues certificates that contain authenticating and identifying data. The certificate also contains keys and other security information.

Certificate Extension

An extension of the X.509 standard that lets the certificate hold additional identifying information.

Certification Path

A specified sequence of issued certificates necessary for the user to get their key.

Certificate Request Message

A certificate request message is composed of the certificate request along with other identifying data.

Certification Revocation List

A CA maintains a list of certificates that have been cancelled but remain unused; revocation lists are vital when certificates have been stolen, for example.

Confidentiality

Keeping secret data from unauthorized eyes.

Coordinated Universal Time (UTC)

The international time standard is called Universal Coordinated Time or, more commonly, UTC, for “Universal Time, Coordinated”. This standard has been in effect since 1972 by worldwide representatives within the International Telecommunication Union. The UTC designation was chosen as a compromise among all the countries’ abbreviations for Universal Coordinated Time. UTC is maintained by the Bureau International de l’Heure (BIPM) which forms the basis of a coordinated dissemination of standard frequencies and time signals. The acronyms UTC and BIPM are each a compromise among all the participating nations.

Content Filtering

A filter that screens out data by checking, for example, URLs or key words.

Credential(s)

Much like a photo ID or birth certificate, electronic credentials are recognized as proof of a party's identity and security level. Examples: certificate, logon ID, secure ID, and so forth.

CRM

See *Certificate Request Message*

Cross-Certificate

Two or more CAs which issue certificates (cross-certificates) recognized in each others’ domains.

Cryptography

See *Encryption*

Data Encryption Standard (DES)

Encryption method in which both the sender and receiver of a message share a single key that decrypts the message.

Datum Secure Network Time Protocol (DS/NTP)

The protocol created by Datum, based on NTP, that includes additional security features.

DCLS

Direct Current Level Shift, or digital IRIG.

See also: *IRIG*

Decryption

The transformation of unintelligible data (“ciphertext”) into original data (“clear text”).

Denial of Service

When a network is flooded with traffic, the systems cannot respond normally, so service is curtailed or denied. This is a favorite technique of network saboteurs, along with Distributed DOS.

DES

See *Data Encryption Standard*

DHCP

Dynamic Host Configuration Protocol, or Windows server software that assigns an IP address to each node in a network.

Diffie-Hellman

A key-agreement algorithm used to create a random number that can be used as a key over an insecure channel.

Digital Certificate

Digital Certificates are issued by a Certificate Authority, which verifies the identification of the sender. The certificate is attached to an electronic message, so the recipient knows the sender is really who they claim to be.

Digital Fingerprint

Similar to digital signature, a digital fingerprint is the encryption of a message digest with a private key.

Digital Signature

Like a digital certificate, a digital signature is a data string that is verified by a Certificate Authority, and is attached to an electronic message so that it can verify that the sender is really who they claim to be. The difference between a digital certificate and a digital signature is found in how the message is encrypted and decrypted.

Digital Signature Algorithm (DSA)

The asymmetric algorithm that is at the core of the digital signature standard.

Digital Signature Standard (DSS)

A National Institute of Standards and Technology (NIST) standard for digital signatures, used to authenticate both a message and the signer. DSS has a security level comparable to RSA (Rivest-Shamir-Adleman) cryptography, having 1,024-bit keys.

Digital time-stamp

See *time-stamp*

Directory

The directory is the storage area for network security information such as keys or server names.

DSA

Digital Signature Algorithm. DSA is a public-key method based on the discrete logarithm problem.

DS/NTP

Datum Secure Network Time Protocol

DSS

See *Digital Signature Standard*

DTT

Datum Temporal Token

Element Manager (ENMTMS)

Software that manages the components of an application.

Encryption

The transformation of clear data (clear text) into unintelligible data (ciphertext). Asymmetric encryption, also known as public key encryption, allows for the trading of information without having to share the key used to encrypt the information. Information is encrypted using the recipient's public key and then the recipient decrypts the information with their private key. Symmetric encryption, also known as private key encryption, allows information to be encrypted and decrypted with the same key. Thus the key must be shared with the decrypting party--but anyone who intercepts the key can also use it.

ENMTMS

See *Element Manager*

Ephemeris Time

Time obtained from observing the motion of the moon around the earth.

FIPS

Federal Information Processing Standards. These are a set of standards for document processing and for working within documents. Some commonly-used FIPS standards are 140-1, 140-2, and 180.

Firewall

Firewalls are software and hardware systems that define access between two networks, offering protection from outside data that could be harmful, such as a virus sent via the Internet.

GMT

Greenwich Mean Time, the mean solar time of the meridian of Greenwich, England, used until 1972 as a basis for calculating standard time throughout the world.

GPS

Global Positioning System. The GPS is a constellation of 24 US Department of Defense satellites orbiting the earth twice a day.

Hack/crack

“Hackers” are unauthorized programmers who write code that enables them to break into a computer network or program. “Crackers” are unauthorized programmers whose goal it is to break into computer networks or programs protected by security software or hardware.

Hash

Also called “hash function” or hashing, used extensively in many encryption algorithms. Hashing transforms a string of characters usually into a shorter, fixed-length value or key. Information in a database is faster to search when you use a hashed key, than if you were to try to match the original data.

HTML

HyperText Markup Language, the computer language used to create pages for the World Wide Web.

HTTP

HyperText Transfer (or Transport) Protocol, the protocol most often used to transfer information from World Wide Web servers to users of the Web.

Identity Certificate

The hash creates a message digest based on the contents of the message. The message is then encrypted using the publisher's private key, then it is appended to the original message.

IEEE

Institute of Electrical and Electronic Engineers, an international organization that sets standards for electrical and computer engineering.

IETF

Internet Engineering Task Force, an international organization which sets standards for Internet protocols in their Request for Comment (RFC) papers.

These papers are numbered (RFC 1305, RFC 868, and so on) and are referred to by engineers worldwide as they work on technologies that support IETF standards.

IKE

Internet Key Exchange, a security system that uses a private key and an exchange key that encrypts private keys. Passwords are delivered via the Internet.

In-band Authentication

When you use PKI for authentication, it is called in-band authentication.

See also: *out-of-band authentication*

Integrity

Data that has retained its integrity has not been modified or tampered with.

IPSec

Internet Protocol Security describes the IETF protocols that protect the secure exchange of packets on the IP layer.

IRIG

InteRange Instrumentation Group is an analog standard for serial time formats.

Irrefutability

In the time security world, irrefutability means the source of the message cannot be disproved.

ITU

International Telecommunications Union, the international organization that sets standards for data communication.

Key

An alphanumeric string that encrypts and decrypts data.

Key Escrow

A secure storage maintained by a trusted third party, which holds keys.

Key Generation

Creation of a key.

Key Management

The process by which keys are created, authenticated, issued, distributed, stored, recovered, and revoked.

Key Pair

An integrated pair of keys, one public, one private.

Key Recovery

A method that allows messages to be decrypted even if the original key is lost.

L1 Band, L2 Band

Each Navstar GPS satellite currently transmits in two dedicated frequency bands: L1 and L2, which is centered on 1227.6 MHz. L1 carries one encrypted signal, as does L2, both being reserved for the military. L1 also carries one unencrypted signal, for civilian use.

LDAP

The Lightweight Directory Access Protocol allows access to a directory service.

Leap Second

Today's scientists and engineers have perfected clocks based on a resonance in cesium atoms to an accuracy of better than one part in 10 trillion. These clocks keep pace with each other to within one two- or three-millionth of a second over a year's time. The earth, on the other hand, might randomly accumulate nearly a full second's error during a given year. To keep coordinated with the rotation of the earth, this error is added to (or deleted from) UTC time as a leap second, on the last day of the June or December in that year.

Message Authentication Code(MAC)

A MAC is a function that takes a variable length input and a key to produce a fixed-length output.

Message Digest

The hash of a message.

See also: *Hash*

MIB

Management Information Base, a database on the network that tracks, records, and corrects performance for each device on the network.

MTBF

Mean Time Between Failure, a measure of reliability. The longer the time span between failures, the more reliable the device.

Multiplexing

Process during which two or more signals are combined into one; at the other end, signals are "unbundled" by a demultiplexer. *TDM* is Time Division Multiplexing, *FDM* is Frequency Division Multiplexing, and *CDMA* is Code Division Multiple Access.

National Measurement Institute

The national authority in each country that is recognized as the source of official time.

Network Time Management System (NTMS)

Datum's architecture for the use of its Trusted Time product.

NIST

National Institute of Standards and Technology, the National Measurement Institute in the United States. In the form of FIPS documents, NIST produces standards for security and cryptography.

NMI

National Measurement Institute(s) or National Metrology Institute(s), the national authority in each country that is usually recognized as the source of official time.

NMIServer

National Measurement Institute Server

NOC

A Network Operations Center monitors and manages networking.

Non-repudiatable

The Trusted Time time-stamp has an audit trail back to its time source, during which the sender of the transaction is authenticated. Therefore, the sender cannot deny the time of the transaction.

Notarization

Certification of the identity of the party in a transaction based on identifying credentials.

NTMS

Network Time Management System, the architecture for Datum's Trusted Time product.

NTP

Network Time Protocol is a protocol that provides a reliable way of transmitting and receiving the time over the TCP/IP networks. The NTP, defined in IETF RFC 1305, is useful for synchronizing the internal clock of the computers to a common time source.

Online validation

A way of validating a key each time before it is used to verify that it has not expired or revoked.

OCSP

Online Certificate Status Protocol, a method for validating digital certificates and signatures.

OID

Object Identifier.

OSI

Operations System Interface,

Out-of-band Authentication

When authentication is performed using relatively insecure methods, such as over the telephone, it is called out-of-band authentication. In-band authentication, which uses PKI, is preferred.

See also: *In-band Authentication*

PCI

Peripheral Component Interconnect, a local bus that supports high-speed connection with peripherals. It plugs into a PCI slot on the motherboard.

PKCS

Public Key Cryptography Standards. These standards allow compatibility among different cryptographic products.

PKI

Public Key Infrastructure. The PKI includes the Certificate Authority (CA), key directory, and management. Other components such as key recovery, and registration, may be included. The result is a form of cryptography in which each user has a public key and a private key. Messages are sent encrypted with the receiver's public key; the receiver decrypts them using the private key.

PKI Certificate

Verifies a person's identification.

PKIX

Extended Public Key Infrastructure, of PKI with additional features approved by the IETF.

PLB

Private Label Branch

Policy

A company's security policy.

PSTN

Public Switched Telephone Network, a voice and data communications service for the general public which uses switched lines.

Private Key

This is a secret key, known to only of the parties involved in a transaction.

Public Key

Messages are sent encrypted with the recipient's public key, which is known to others; the recipient decrypts them using their private key.

Public Key Certificate

Certificate in the form of data that holds a public key, authentication information, and private key information.

RA

A Registration Authority does not issue certificates, but does the required identification for certain certificate data.

Resolution

Resolution of a time code refers to the smallest increment of time, whether it is days, hours, seconds, or other.

Revocation

The withdrawing of a certificate by a Certificate Authority before its expiration date or time.

Also see *Certificate Revocation List (CRL)*

Risk Management

The tasks and plans that help avoid security risk, and if security is breached, helps minimize damage.

RSA

The RSA (Rivest-Shamir-Andleman) algorithm is used to create digital signatures.

SHA-1

Secure Hash Algorithm, which has a larger message digest, making it more secure against certain hacker attacks.

Smart card

A card the size of a credit card, which holds a microprocessor that stores information.

S/MIME

Secure Multipurpose Internet Mail Extensions. The standard for secure messaging.

SNMP

Simple Network Management Protocol is the Internet standard protocol for network management software. It monitors devices on the network, and gathers device performance data for management information (data)bases (“MIB”).

Solar Time

Time based on the revolution of the earth around the sun.

SSL

Secure Sockets Layer, a protocol that allows secure communications on the World Wide Web/Internet.

SSL Client Authentication

Part of the SSL “handshake” process, when the client responds to server requests for a key.

SSL Server Authentication

Part of the SSL “handshake” process, when the server informs the client of its certificate (and other) preferences.

SSL-LDAP

Secure Sockets Layer-Lightweight Directory Access Protocol.

Stratum Level

These are standards set by Network Time Protocol RFC 1305. The highest level are Stratum 0 devices such as GPS, which get their time from a primary time source such as a national atomic clock. Stratum 1 servers, such as TymServe, source their time from a Stratum 0 device. Stratum 2 and beyond obtain their time from Stratum 1 servers. The further away a network is from a primary source, the greater the chance of signal degradations due to variations in communications lines, and so forth.

Sysplex Timer

The Sysplex Timer provides a synchronized Time-of-Day clock for multiple attached computers.

TCCert

Time Calibration Certificate

TCP/IP

A mainstay of the Internet, the Transmission Control Protocol (TCP) provides dependable communication and multiplexing. It is connection-oriented, meaning it requires a connection be established before data transfer. It sits on top of the Internet Protocol (IP), which provides packet routing. This is connectionless, meaning each data packet has its source and destination data embedded, so it can bounce around a network and still get to its destination.

Telnet

Telnet is a terminal emulation application protocol that enables a user to log in remotely across a TCP/IP network to any host supporting this protocol. The keystrokes that the user enters at the computer or terminal are delivered to the remote machine, and the remote computer response is delivered back to the user's computer or terminal.

time-stamp

A record mathematically linking a piece of data to a time and date.

time-stamp Request

The client computer or application sends a time-stamp request to a stamp server.

time-stamp Token

The essential part of the time-stamp. It contains the time, the message digest/the message imprint (hash), and it is signed to verify the accuracy of that time. In detail, it is a signed data object where the encapsulated content is a TSTInfoObject, thus it verifies the stamp as coming from the device you submitted it to, and it is bound to the file you are working with.

time-stamping Authority

An authorized device that issues time-stamps, and its owner.

TLS

Transport Layer Security, security that protects the OSI layer that is responsible for reliable end-to-end data transfer between end systems.

Tool box

A group of software applications that have similar functions.

Token

See *time-stamp token*

TMC

See *Trusted Time Master Clock*

TPC

Third Party Certificate.

See also: *Certificate*

TPCA

Third Party Certification/Certificate Authority.

See also: *Certificate Authority*

Traceability

Traceability infers that the time standard used on the time-stamp server was set using time directly or indirectly from a National Measurement Institute.

Transaction

An activity, such as a request or an exchange.

Triple-DES

Also called Triple Data Encryption Algorithm (TDEA) Data Encryption Standard is an algorithm that encrypts blocks of data.

Trust

In the network security context, trust refers to privacy (the data is not viewable by unauthorized people), integrity (the data stays in its true form), non-repudiation (the publisher cannot say they did not send it), and authentication (the publisher--and recipient--are who they say they are).

Trusted Time

Datum's family of products that produce extremely accurate and auditable time-stamps.

Trusted Time Infrastructure

The internal architecture of Datum's Trusted Time products.

Trusted Time MasterClock (TMC)

Datum's Trusted MasterClock is a rubidium-based master clock synchronized to UTC time and certified by a National Measurement Institute.

Trusted Time NMIServer

Datum's NMI Trusted Time Server, or NMIServer, is a standalone secure server based on the Trusted MasterClock, which is dedicated to the creation of trusted UTC time at the NMI.

Trusted Time Products (TTP)

The family of Datum's Trusted Time products, including the Network Time Management System, Trusted MasterClock, Trusted time-stampServer, and Trusted Time application software.

Trusted time-stampServer (TSS)

Datum's Trusted time-stampServer (TSS) services time-stamp requests from applications, transactions, or computer logs.

TSA

See *time-stamp Authority*

TSP

time-stamp Protocol

TSR

See *time-stamp Request*

TSS

See *time-stampServer*

TT

See *Trusted Time*

TTI

See *Trusted Time Infrastructure*

TTDS

See *Trusted Time Distribution Service*

TTP

See *Trusted Time Product*

UDP/IP

User Datagram Protocol/Internet Protocol is a communications protocol that provides service when messages are exchanged between computers in a network that uses the Internet Protocol. It is an alternative to the Transmission Control Protocol.

USNO

U.S. Naval Observatory, in Washington, D.C., where the atomic clock that serves as the official source of time for the United States is maintained.

UTC

See *Coordinated Universal Time*

Vault

Secure data storage facility.

Verification

The process of making sure the identity of the parties involved in a transaction is what they claim it to be.

Virus

An unwanted program that hides “behind” legitimate code, and which is activated when the legitimate program is activated.

VPN

Virtual Private Network, a way that authorized individuals can gain secure access to an organization's intranet, usually via the Internet.

W3C

The World Wide Web Consortium, based at the Massachusetts Institute of Technology(MIT), is an international organization which creates standards for the World Wide Web.

Warrant

An attribute certificate that attests to the time of the device. It is used to adjust the clock. See also: *PKI certificate*

Wireless Application Protocol (WAP)

Wireless Application Protocol, a worldwide standard for applications used on wireless communication networks.

WPKI

Wireless Public Key Infrastructure.

WTLS

Wireless Transport Layer Security

X.509

The ITU's X.509 standard defines a standard format for digital certificates, the most-widely used PKI standard.

X.509 v3 Certificate Extension

The X.509 standard with extended features approved by the IETF.

Appendix F: Declaration of Conformity

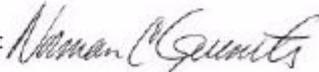
EC DECLARATION OF CONFORMITY

Application of Council Directives:	89/336/EEC, 93/68/EEC, 73/23/EEC
Manufacturer's Name:	Datum – Irvine
Manufacturer's Address:	3 Parker Avenue, Irvine, CA 92618, USA
Importer's Name:	
Importer's Address:	
Type of Equipment:	Information Technology Equipment
Equipment Class:	Commercial and Light Industry
Model:	TS2100 Network Time Server
Conforms to the following Standards:	EN55022-1 (1998), EN55024-1 (1998), EN60950
Year of Manufacture:	2001

I the undersigned, hereby declare that the equipment specified above conforms to the above directive(s) and standard(s).

Place: Datum – Irvine

Date: December 13, 2001

Signature: 

Full Name: Norman C. Guenther

Position: Vice President Quality

Index

A

About This User Guide 9
and Business 7
Antenna
 Best location 22
 Cable length 22
 Cable signal losses 23
 GPS, installation 22
 Options 14

B

Buffer size 38

C

Cable Options 14
Cable Signal Losses 23
Chassis 77
Command Description 38
Command Shell 37
Command Tree 39
Commands
 HTTP Tools Directory 49
 Key 43
 Network 38, 40
 NTP Broadcast Directory 44
 NTP Server Directory 42
 Telnet Server Directory 45
 TFTP Tools Directory 48
 Timing 50
Configuration
 Initial 16
Configuration methods 24
Configurations
 Suggested 20
Conventions Used in this Guide 9
Cryptochecksum 33

D

DatumTime™ 17
Daytime Protocol (RFC 867) 30
DHCP Tools Directory 47

E

Ethernet 17

F

Firmware Upgrade 83
Firmware Upgrade Procedure 83
Freerun mode 27
Frequently Asked Questions 69
Functionality, Testing 17

G

Global Positioning System (GPS) 7, 22
Glossary 105
GPS
 7, 22, 28
 Antenna installation 19
GPS Receiver 77

H

HTTP Tools Directory 49

I

IETF 6
Importance of 7
Input/Output Connectors 79
Internet HTTP Access 25
Intrinsic Help 38, 61

K

Key Pair 33

L

Lightning arrester 19
Locked 17, 27

M

Mean Time Between Failures (MTBF) 77
MIB 25, 65
 Additional Stored MIB Variables 66
 Compilation 66
 Datum MIB Extension 87
 Datum MIB II Extension 66
 MIB-II Extension File 67

N

Network Commands 40
Network Directory 40
Network Interface 77
Network Time Protocol (RFC 1305 and RFC 1119) 30
NTP 5, 28
 27, 28, 30
 Authentication 33
 Authentication Mechanism 33
 Authentication-Only 34
 Authenticator 33
 Broadcast Directory 44
 Client software 21
 Functionality 17
 How it defines the authentication process 34
 Leap Indicator 31
 Message Data 31
 Mode 31
 Network Time Protocol 30
 NTP Data Format 30
 Originate Timestamp 32
 Poll Interval 32
 Receive Time stamp 32

Reference Clock Identifier 32
Reference Timestamp 32
Server Directory 42
Stratum 32
Synchronizing Dispersion 32
Synchronizing Distance 32
Transmit Time stamp 32
Version Number 31

O
Operating and Storage Environments 77
Oscillator 17
Overview of TymServe 5

P
Permanent Installation 13, 19
Pin Descriptions 80
Precision 32
Programming and Storage of the Key Identifier/Key Pair 33
Public Domain xNTP Package 33

Q
Quick Initial Setup 13

R
RFC 1119 28, 30
RFC 1305 6, 30
RFC 1361 30
RFC 867 30
RFC 868 29
Root Dispersion Version 3 32
Root Distance Version 3 32
RS-232 Serial Port B 24

S
Satellite signals
 Acquiring 16
Security 66
Serial 38
Serial Connection 77
Serial connection
 Establishing 15
Serial Directory 56
Serial Download 84
Serial/Telnet Command Tree 39
Simple Network Time Protocol (RFC 1361) 30
SNMP Access 25
SNMP Configuration 65
SNMP Tools Directory 45
SNMPv1 66
SNTP 27, 30
Specifications 77
Spread-spectrum signal 22
Stratum Levels
 About 6
 and GPS 29
Sysplex Timer 27, 34

T
TCP/IP 5, 27
Technical Support 9
Telnet 37
 Access 24
 Commands 16
 Server Directory 45
Testing Functionality 17
TFP Queries 54
TFTP Download 84
TFTP Tools Directory 48
Time Distribution 27
Time Distribution Model 28
Time Protocol (RFC 868) 29
Time Protocols 29
Time Synchronization
 About 7
Timing 38
Timing Accuracy 77
Timing Commands 50
Timing Directory 50
Tracking 16, 27
Transmission Control Protocol (TCP) 29
Troubleshooting 73
TymServe
 and GPS 28
 As Stratum 1 device 6
 Client 7
 Client Software 28
 Components 6
 Configurations, suggested 20
 Front and Rear Views 15, 79
 How it uses NTP authentication-only 34
 How it uses the Sysplex timer 34
 Operation 27
 Sample uses of 8
 Server 6
 Time Distribution 27
 Unpacking 10
TymServe Distributing Time 5

U
Universal Coordinated Time 7
Unpacking Your TymServe 10
User Datagram Protocol (UDP) 30
User Guide
 Obtaining additional copies 9
UTC 7
Utility 38
Utility Directory 57



Datum - Trusted Time Division

10 Maguire Road, Suite 120

Lexington, MA 02421-3110 USA

(1)(781) 372-3600 Toll-free (U.S.): (888) 551-4022

www.datum.com e-mail: ts@datum.com

2002/02