CTI 2572-A

ETHERNET TCP/IP MODULE

INSTALLATION AND OPERATION GUIDE

Version 1.9

CTI Part # 062-00356

DOCUMENT DISCLAIMER STATEMENT

Every effort has been made to ensure the accuracy of this document; however, errors do occasionally occur. CTI provides this document on an "as is" basis and assumes no responsibility for direct or consequential damages resulting from the use of this document. This document is provided without express or implied warranty of any kind, including but not limited to the warranties of merchantability or fitness for a particular purpose. This document and the products it references are subject to change without notice. If you have a comment or discover an error, please call us toll-free at 1-800-537-8398 or email us at *sales@controltechnology.com.*

REVISION HISTORY		
V1.0	12/10/02	Original Issue
V1.1	01/10/03	Corrected minor typos and added missing error codes
V1.2	09/22/03	Corrected typo in part number Corrected error in Command Error Timing diagram Enhanced the Updating Firmware chapter Added description for the compatibility mode switch Updated configuration screen shot Added chapter for Modbus TCP server
V1.3	05/05/04	Added chapter for Ethernet/IP Server Added information on CAMP Multicast Corrected minor typos and formatting errors
V1.4	9/10/08	Corrected typos
V1.5	10/1/08	Added port number for Modbus slave Added comments concerning firewalls and TFTP server
V1.6	01/19/09	Corrected text describing the use of SW11 (PLC Interface Mode) to note that compatibility mode is equivalent to the 2572 interface. Also noted that the user should consider compatibility mode if the module is installed in a remote base and minimizing scan time is an issue.
V1.7	11/30/09	Revised text for the CAMP Unacknowledged Write command production timer: • Corrected specification for default timer value • Added note to avoid setting the timer value smaller than necessary • Explained how uncoupled mode should be used with the timer. • Revised example for multicast to illustrate use of timer Revised text in Appendix C regarding the operation of Uncoupled Mode. Revised copyright date of manual.

REVISION HISTORY		
V1.8	12/15/09	Corrected Command Code for CAMP Unacknowledged Write
V1.9	7/9/15	Added information regarding the CTI default shipping IP parameters

PREFACE

This ***Installation and Operation Guide*** provides reference information for the CTI 2572-A Ethernet TCP/IP Module. The information in this manual is directed to individuals who will be installing the module and those that will be developing PLC logic to control module functions.

We assume you are familiar with the installation and operation of:

1)   CTI 2500 Series and/or Siemens SIMATIC® 505 programmable controllers,

2)   Ethernet local area networks,

3)   Transmission Control Protocol/Internet Protocol.

Please refer to the appropriate user documentation for specific information on programmable controllers and I/O modules.

If you plan on developing on writing computer applications that access the module, you should also obtain the *CTI 2572 Programming Reference Manual (*CTI Part # 62-166), which provides detailed information on the module command message interface.

USAGE CONVENTIONS

NOTE:
Notes alert the user to special features or procedures.

CAUTION:
Cautions alert the user to procedures that could damage equipment.

WARNING:
Warnings alert the user to procedures that could damage equipment and endanger the user.

TABLE OF CONTENTS

TABLE OF FIGURES

CHAPTER 1. DESCRIPTION

1.1. Introduction

The 2572-A Ethernet TCP/IP Module is a high performance version of the CTI 2572 Ethernet module. Because it supports the same PLC logic commands and network protocols, it can be used as a direct replacement for the CTI 2572 modules in most applications. In addition, it provides several new features including:

- Fast Ethernet (100Mb) Operation
- Web Server Interface
- DHCP Startup Option
- Enhanced Diagnostic Facilities

The CTI 2572-A Ethernet TCP/IP Module is a communications co-processor that provides network services to CTI 2500 Series® and SIMATIC® 505 PLCs. Using the TCP/IP protocol, suitably programmed network stations can acquire data from the PLC, send data and programs to the PLC, and exercise supervisory control over the PLC operation. In addition, the PLC can use the facilities of the CTI 2572-A to access data in other PLC systems equipped with a CTI 2572 or CTI 2572-A module.

The CTI 2572-A module directly attaches to Ethernet twisted pair cabling via the Ethernet CAT5e connector (RJ-45) and can be used with either 10MB or 100Mb data links (half or full duplex operation). The firmware includes a full function TCP/IP stack that supports both TCP and UDP protocols.

The module provides extensive diagnostic facilities, accessible via a standard web browser to aid in the detection and correction of network problems. In addition, the module operating parameters may be configured via the web browser.

Despite the substantial processing power incorporated into the module, the highly integrated chip technology uses less power than the 2572 module and still fits in a single rack space.
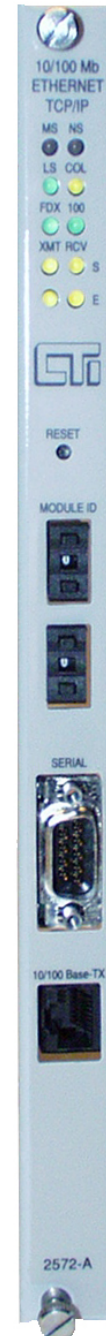
Figure 1. 2572-A Front Panel

1.2. Module Highlights

2572 Compatibility

The module supports the same CAMP message interface as the 2572. Thus, existing HMI drivers can be used with the 2572-A. In fact, CTI 2572 and 2572-A modules may be intermixed in the same application. In addition, since the 2572 command interface is fully supported, existing CTI 2572 logic will work with the 2572-A. CTI 2572-A modules can be used as direct replacements for CTI 2572 modules in these applications.

The 2572-A does not include an Ethernet AUI port, since it is not included in the 802.3 standard for 100Mb operation. However, you can connect to other media types, such as fiber optics, by using a media adapter or an Ethernet switch. The Module Status Word (WX1) has been changed slightly. See *Module Status Word* on page 92.

The 2572-A module does not support the Send-Receive or DataShare protocols. However, Multicast transmission is available as a substitute.

Enhanced Performance

Using a powerful RISC processor and embedded Ethernet controller, the 2572-A module provides significant performance improvements while maintaining a low backplane power requirement and a small single-wide form factor. Coupled with a large RAM capacity, this vastly increases the number of concurrent protocols and TCP/IP connections that can be supported.

100Mb Ethernet Port

The 2572-A provides a Category 5e RJ-45 connector which attaches directly to Unshielded Twisted Pair (UTP) or Shielded Twisted Pair (STP) Ethernet cabling. The port complies with the IEEE 802.3 specifications for 10BaseT and 100Base TX and will operate in either half of full duplex mode. The speed and mode are automatically negotiated by the module in accordance with IEEE 802.3u specifications. When attaching to a hub or switch that does not support auto-negotiation, the port will default to 10Mb half-duplex.

TCP/IP Capabilities

The 2572-A TCP/IP software meets all common industrial requirements including:
- Support for IP, ICMP, and ARP Internet Layer Protocols;
- Support for TCP, UDP, and IGMP (IP Multicast) Transport Layer protocols, including a configurable socket KeepAlive interval;
- Support for TCP and UPD Echo servers for installation testing;
- Support for SYSLOG Client to enable remote data logging;
- Support for Dynamic Host Configuration Program (DHCP) protocol to automate module startup;
- Support for HTTP server to provide access via a Web Browser. This support includes access security facilities to prevent unauthorized access.

Enhanced Startup Options

The 2572-A provides three startup options to meet almost any customer requirement. See CHAPTER 2. INSTALLATION , for a discussion of the advantages and disadvantages of each approach.

- *AutoStart from EEPROM* – The module automatically starts up using configuration parameters stored in EEPROM.

- *PLC Start* – PLC logic is used to set the network parameters and start the module.

- *DHCP (Dynamic Host Configuration Protocol) Start* -This is a new method provided by this module. The module obtains its network parameters from a network DHCP server during startup. Once configured, the DHCP server automatically assigns IP parameters to the module based on the position of the 2572-A Module ID switches.

Enhanced Diagnostics

The 2572-A provides a complete set of diagnostic data that can be accessed via a standard web browser. Diagnostic objects are provided for the module hardware, Ethernet interface, PLC Interface, TCP/IP stack, and all protocol managers. In addition, the module maintains an internal log of significant events. The log entries are maintained in non-volatile RAM, allowing the log to survive re-cycling of power. If desired, the log entries may also be logged to disk by using a PC running SYSLOG server software.

Enhanced Security

The 2572-A module adds password protection to certain module functions. If a valid password is not entered, the module will prohibit the user from changing the configuration or downloading new firmware to the module via the network. In addition, Configuration Lock and Download Lock switches can be set to prohibit anyone from changing the module configuration changes or downloading firmware via the network.

1.3. Functional Overview

The 2572-A can operate as both a *server* and a *client.* As a server, the module *responds* to messages sent by a network client, such as a PC running HMI software. As a client, the module *initiates* messages on command from the PLC to a server, such as another 2572-A module.

Server Function
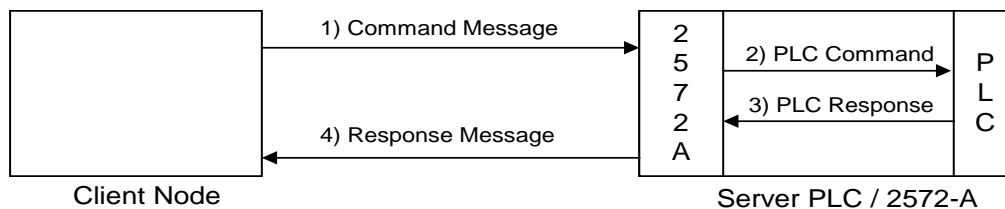
Figure 2. PLC Server Function

The 2572-A can function as a server to clients who wish to access the PLC. Figure 2. PLC Server Function illustrates the typical message dialog between the client, the 2572-A, and the PLC.

1) The client node sends a command message to the 2572-A via TCP/IP. For example, the client may request that the 2572-A read and return 100 words of V memory.

2) Based on the contents of a command message, the 2572-A sends commands and data to the PLC processor via the backplane. For example, the 2572-A would issue the applicable command to the PLC to retrieve 100 words of V memory.

3) The PLC processor responds to the command via the backplane. In the example, the PLC would return 100 V memory words.

4) After the PLC responds, the 2572-A builds the appropriate message and returns it to the client node. In this example, the 2572-A would build a network message containing the 100 words of data and send it to the client that requested it.

PLC Client Function

The 2572-A can also function as a *PLC Client.* As a PLC Client, the 2572-A acts as an agent for the PLC, sending messages to other nodes and processing the responses under control of the PLC logic.
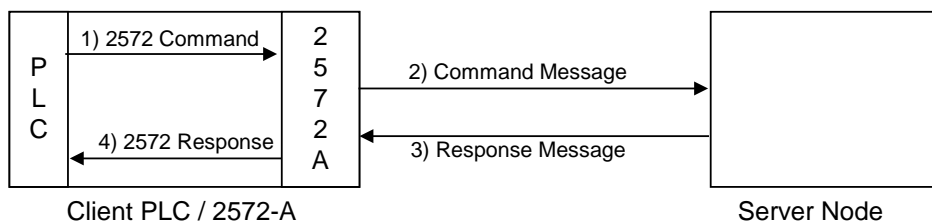
Figure 3. PLC Client Function

Data in the PLC program specifies the recipient and data contents of the message. PLC logic sets a "trigger" bit to cause the 2572-A to send the message.

In the example above:

1) When the PLC detects a specified event, it sends a command to the local 2572-A module. For example, the command could be to read 5 words from another node on the network.

2) Based on the command, the 2572-A then sends the applicable command via TCP/IP to the specified network (server) node.

3) The server node processes the command and returns a response via TCP/IP. In the example, the server node would return a message containing the specified words.

4) The 2572-A processes the network message, and notifies the PLC that the operation is complete. In the example, the 2572-A would write the words to the specified PLC memory location and signal completion of the task.

The 2572-A can support multiple concurrent client sessions. The server node shown in the illustration could be another 2572-A module, a CTI 2572 module, a Siemens® 505-CP2572 module,

or a computer programmed to process the commands and send the appropriate responses. Information describing the PLC logic required for client operation can be found in CHAPTER 5. CAMP CLIENT COMMANDS.

The 2572-A can support multiple server sessions and multiple client sessions concurrently. Therefore, networked PLCs can use the facilities of the 2572-A to participate in multi-session peer-to-peer communications.

1.4. TCP/IP Overview

The CTI 2572-A module uses TCP/IP (Transmission Control Protocol/Internet Protocol) to transport messages between the module and other nodes on the network. TCP/IP is a suite of protocols that provide routing and delivery services for messages between application programs running on different processors (called hosts in TCP/IP terminology). TCP/IP may be used on your local Ethernet network, where it can co-exist with other protocols. In addition, it can be used on a Wide Area Network (WAN), including the Internet.

Although TCP/IP provides network delivery services based on a global standard, using TCP/IP does not guarantee that two workstations can effectively transfer data. To accomplish this, the nodes must be using a common application protocol, such as CAMP. Most commonly used HMI applications have driver software that supports the CTI 2572 CAMP message interface. In addition, OPC servers are available from several sources, including CTI. For additional information about TCP/IP see APPENDIX D. IP ADDRESS INFORMATION.

1.5. PLC Command Interface

Some 2572-A functions require that you use PLC logic to control the operation of the module. The 2572-A module provides a PLC logic interface for sending messages and processing responses that is identical to the CTI 2572 module. The interface consists of two parts:

- *Command Blocks -* Command Blocks are blocks of contiguous V memory words used to store module commands and associated parameters. The exact content of the Command Block will vary with the command being issued.
- *Module WX/WY Words -* The 2572-A module logs in as a Special Function module and is assigned two WX words and six WY words. PLC logic uses the WY words to select the Command Block and to trigger the command execution. The status of the module and of command execution can be monitored via the WX words.

Figure 7 illustrates how the module WX/WY words and the command blocks are used together. The 2572-A writes values in the WX words, the PLC writes values in the WY words. WX1 and WY3 contains bits allow the PLC to monitor and control module global status. WY4 and WX2 contain bits that allow the PLC to trigger commands and monitor command status. The Command Slots (WY5-8) are used to point to the starting V Memory addresses of the Command Blocks.

To use the module command interface, your PLC logic typically loads a Command Slot with the address of the desired command block. It then sets a corresponding trigger bit in WY4 to cause the 2572-A to execute the command. Your logic then monitors the condition of the command status bits in WX2 to determine whether the command completed successfully. Please refer to APPENDIX C. PLC COMMAND INTERFACE for a complete description.

MODULE WX/ WY   **COMMAND BLOCKS**

WX1	MODULE STATUS WORD
WX2	COMMAND STATUS WORD
WY3	MODULE CONTROL WORD
WY4	COMMAND CONTROL WORD
WY5	COMMAND SLOT 1
WY6	COMMAND SLOT 2
WY7	COMMAND SLOT 3
WY8	COMMAND SLOT 4
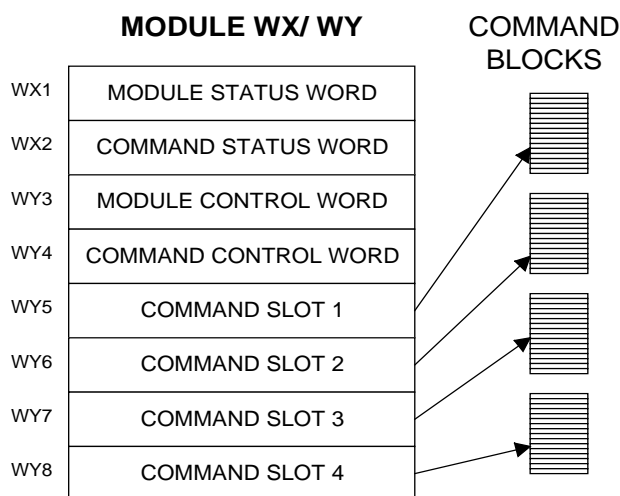
Figure 4. 2572-A PLC Interface

1.6. Getting Started

Before using the 2572-A module, you will need to perform the following steps. These steps are described in more detail in CHAPTER 2. INSTALLATION .

Set the Module Switches

Module switches are used to select the startup options and security options.

Install the Module in the PLC I/O Base

The 2572-A is a single wide module that installs in a standard SIMATIC® 505 PLC rack. For best performance you should install the 2572-A in the first I/O slot of the local base.

Enter the Module in the PLC I/O Configuration

This procedure is accomplished using your PLC programming software. The 2572-A module must be entered into the I/O configuration before operations requiring PLC logic will work.

Connect the Module to the Network

Connect an Ethernet cable between the module and an Ethernet hub or switch.

Start the Module

There are several methods available for starting the module and setting the module network parameters. These include using EEPROM stored data, using PLC logic, or using a network DHCP server.

Checking out the Module

You can use both the module indicators and CTI diagnostic software to ensure the module is operating properly.

Using the Module

Assuming you have completed the above steps successfully, the 2572-A module is ready for use as a PLC Server. If you wish to implement PLC Client functions, please refer to CHAPTER 5. CAMP CLIENT COMMANDS.

CHAPTER 2. INSTALLATION

The installation of the Model 2572-A Ethernet TCP/IP Adapter Module consists of the following steps:

1)   Planning the installation,
2)   Unpacking and configuring the module,
3)   Physical installation,
4)   Setting IP information,
5)   Connecting cables,
6)   Checking the module operation.

2.1. Installation Planning

Choosing Ethernet Media

The 2572-A module attaches directly to 10BaseT or 100Base TX media (Shielded or Unshielded Twisted Pair) via the RJ-45 connector. Ensure that the cables you use for Ethernet communications meet the appropriate IEEE 802.3 specifications and are appropriate for the environment in which you are operating. CTI recommends you use cables rated Category 5e or better.

The module can also participate in networks that use fiber optic cable. The most common use of fiber optic cable is to connect to an Ethernet hub or switch which is installed in the local work area. Copper cable (Unshielded Twisted Pair or Shielded Twisted Pair) is then run from the local hub or switch to the module. Alternately, you can procure a fiber optic to twisted pair converter.

Selecting an IP Address and Other Network Parameters

Before proceeding, you must determine what IP address you will assign to the module, the subnet mask to use, and the IP address of the default router. If you are connecting to an existing network or to the Internet, your network administrator should provide this information. If you are installing a stand-alone network, you should choose from within the set of "private" IP addresses specified in RFC 1597 and set the subnet mask accordingly. See APPENDIX D. IP ADDRESS INFORMATION for a description of the IP Address numbering conventions.

Choosing a Module Startup Method

Before the 2572-A will communicate using TCP/IP, the TCP/IP parameters must be set and the module network server must be started. The 2572-A provides several alternative methods to accomplish this task. The startup method is selected via the Option Switches and the Module ID switches.   See Section 2.4 for more information.

AutoStart using EEPROM Data

If you choose this method, the module will start up using network parameters previously written to EEPROM. The primary advantage of this approach is that it eliminates the need for additional PLC logic to initiate startup. See Section 2.10. Storing Network Parameters in EEPROM.

The downside of this method is that, when installing or replacing modules, you must manually configure them. In addition, if you arbitrarily swap 2572-A modules between PLCs, the IP address will move with the module. The effect of inadvertently swapping IP addresses can cause major problems, since communications directed at one PLC would actually be going to another PLC.

PLC Start

Using this method, PLC logic is used to start the module. A special *Start Network Server* command, triggered by PLC logic, transfers the network data stored in V memory to the module. An important advantage to this method is that it eliminates the need to manually configure the module during the initial installation or during a replacement operation. In addition, since the network parameters are stored in PLC memory, the module IP address remains associated with the PLC even when modules are swapped. The primary disadvantage is that it requires a small amount of additional ladder logic. In addition, if the PLC is not in run mode (not executing logic) the module will not start up. The PLC logic to perform this function is described in CHAPTER 4. CAMP SERVER COMMANDS.

AutoStart Using DHCP

Using this method, the module obtains its IP address and other network parameters from a Dynamic Host Configuration Protocol (DHCP). Using a patent pending method, the DHCP server provides network parameters and other startup information based on the setting of the Module ID switches.

This approach is similar to the technique used by other industrial networks and offers the advantages of both of the previous methods. No manual configuration is required and no PLC logic is required. The primary disadvantage is the need to provide and configure a DHCP server. See APPENDIX E. USING DHCP.

Choosing between TCP and UDP Protocols

Many HMI drivers and OPC servers will allow you to select either TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) for delivering messages. In addition, some of the 2572-A client functions allow you to choose between the two. The following information should help you determine which is right for your situation.

UDP Protocol

The UDP protocol allows you to send a message to another node without previously establishing a logical connection to the other node. This method, called ***connectionless delivery***, uses smaller network bandwidth, consumes less module resources, and usually results in faster response times. Although the delivery of UDP messages is not acknowledged by TCP/IP, higher level protocols, such as CAMP, confirm that the message was received and that the requested service performed.

NOTE:
In most installations, UDP is the preferred protocol for HMI applications that continuously read data from the PLC.

TCP Protocol

The TCP protocol requires that a logical connection be established between two points before messages can be sent. This method, called *connection-oriented services*, provides delivery acknowledgement and message flow control within the TCP/IP protocol. If a message is not delivered correctly, the TCP protocol will cause the message to be re-transmitted.

TCP is generally slower than UDP because additional acknowledgement messages must be transmitted and evaluated. However, there are several instances in which it should be used:
1. If you have a network whose quality requires a significant amount of message re-transmission, TCP can provide better overall performance because the TCP is quicker at delivery acknowledgement and retry than the application level, which typically relies on a message timeout measured in seconds.
2. If you are using the Internet to access the module, you may want to consider TCP. When traversing the Internet, some gateways may break a packet up into smaller chunks, a process called fragmentation. The smaller packets may be sent via different paths and could arrive out of order. TCP will ensure that the fragmented packets will be re-assembled in the correct order, while UDP will not.

Maximizing Performance

For best performance, you should place the module in a local rack (the one containing the PLC). Using a Special Function module such as the 2572-A in a Remote I/O rack imposes significant additional communications overhead and noticeably increases the scan time of the PLC. This effect is especially noticeable when transferring large amounts of data.

> *NOTE:*
> *The 2572-A will not work in a remote rack using the Profibus Remote Base Controller (RBC). Profibus does not support Special Function modules.*

The module is allowed to access to the PLC only once during a scan. Ensure that the task codes per scan setting of the PLC is set to eight (8). This allows the maximum number of PLC access requests to be processed in a single scan. Set the PLC to the shortest acceptable scan time or use the variable scan time setting.

Heavily congested networks can degrade module performance. When the network traffic is heavy, the use of an Ethernet switch can reduce loading on an individual segment. If broadcast traffic is excessive, you will have to use a router or a layer 3 switch to block broadcasts.

Security Considerations

Since the 2572-A module communicates on a TCP/IP network, you should take precautions to prevent someone from inadvertently or maliciously interrupting the operation of the module. Some actions you can take include:

Use a dedicated network that does not connect to other networks. By eliminating external physical connections, you limit access to only those on the network segment.

Use a router with firewall capability to connect to other networks. If isolating the network from other networks is not practical, you can use "firewall" techniques to limit access from the outside.

Disable routing for the 2572-A modules. If you want to prevent access to the 2572-A modules from replying to requests outside the local network segment but you want to allow your PC workstations to access the corporate network, disable routing on the 2572-A module. You accomplish this by setting the Default Router IP address to 0.0.0.0.

Use password protection to limit access to module functions that could interrupt service. Password protection is available for the Module Configuration and Firmware Download functions.

Use hardware lockout protection to prevent configuration changes or firmware download. Switches on the board can be used to disable these functions.

2.2. Power Requirements

The CTI 2572-A module consumes 2.5 watts of +5 VDC power from the backplane.

2.3. Unpacking the Module

Open the shipping carton and remove the special anti-static bag that contains the module. After discharging any static build-up, remove the module from the static bag. Do not discard the static bag. Always use this bag for protection against static damage when the module is not inserted into the I/O base.

CAUTION:
The components on the 2572-A module printed circuit card can be damaged by static electricity discharge. To prevent this damage, the module is shipped in a special anti-static bag. Static control precautions should be followed when removing the module from the bag and when handling the printed circuit card during configuration.

2.4. Setting the 2572-A Option Switches

Switches on the 2572-A are used to select the following

- Serial Port Baud Rate
- Startup Option
- Security Features
- Diagnostic Startup Option

Figure 5 indicates the location of the switchblock.

The remainder of this section describes the function of the individual switches.
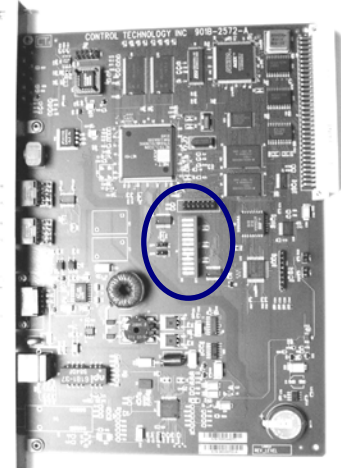
Figure 5. Switchblock Location
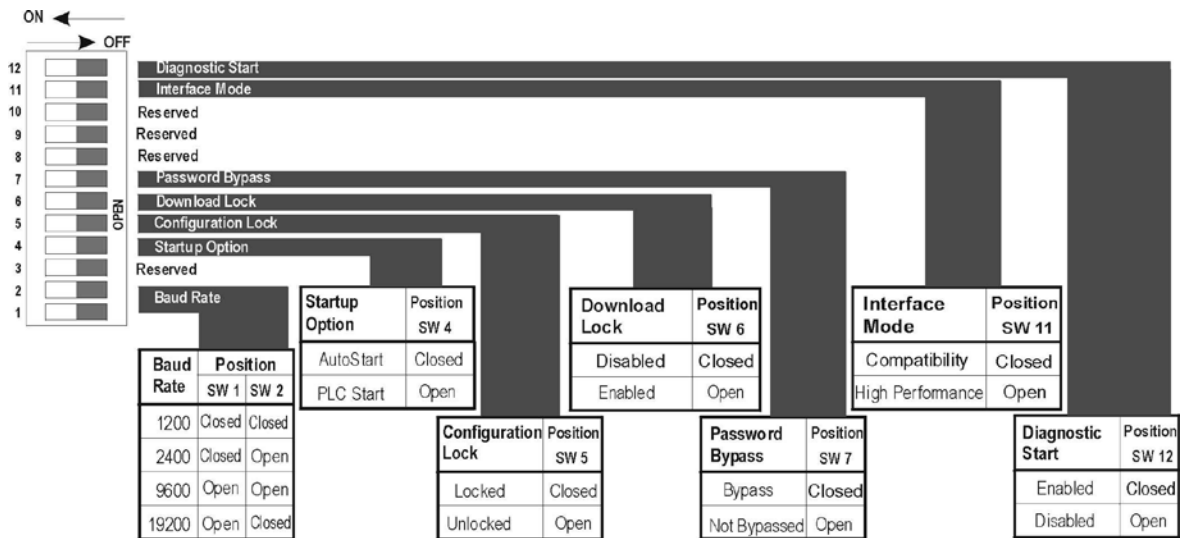
Figure 6. Option Switches

SW1, SW2 – Serial Port Baud Rate. For most applications as setting of 9600 baud provides a good balance between speed and reliability.

Baud	Position	
Rate	SW1	SW2
1200	Closed	Closed
2400	Closed	Open
9600	Open	Open
19200	Open	Closed

SW3 – Reserved. This switch position is reserved for future use.

SW4 – Module Startup Option. In the PLC START position, the module will wait for the PLC START Network Server command starting the network services. CHAPTER 4. CAMP SERVER COMMANDS describes the PLC logic required. In the AUTOSTART position, the module will automatically start up using parameters stored in the module EEPROM or obtained from a DHCP server.

Network Startup	Position SW4
AutoStart	Closed
PLC Start	Open

NOTE:
When using the PLC Start Option, the PLC must be in run mode before the module will start.

SW5 - Configuration Lock. When set to the LOCKED position, this switch prevents the user from changing the module configuration via the web server, even if a valid password is entered.

Note:
The Configuration Lock is designed to prevent changes to the module configuration via the web server interface. This does not prevent EEPROM from being automatically updated when using DHCP or PLC start options

Configuration Lock	Position SW5
Locked	Closed
Unlocked	Open

SW6 - Download Lock. When set to the LOCKED position, this switch prevents the user from the initiating a firmware download via the web server, even if a valid password is entered.

Download Lock	Position SW6
Disabled	Closed
Enabled	Open

Note:
The bootloader will still attempt to download a new application program from a TFTP server if the application program is corrupted.

SW7 - Password Bypass. When set to the CLOSED position, this switch bypasses all password checks in the web server. This is typically used to allow the user to change passwords when the current password has been forgotten or when password protection is not required.

Password Bypass	Position SW7
Bypass	Closed
Not Bypassed	Open

SW8 – 10 are reserved for future use.

SW11- PLC Interface Mode. When this switch is set to the CLOSED position, the module will use the same PLC interface as the CTI 2572. When the switch set to the OPEN position, the module will use a high performance interface that increases the amount of data per scan that can be transferred to and from the PLC and sets the task codes per scan to 8. In most applications you will want to use the high performance mode. However, for installations where minimizing scan time is an issue, you should consider using compatibility mode, especially when the module is installed in a remote base.

Interface Mode	Position SW11
Compatibility	Closed
High Performance	Open

SW12 – Diagnostic Start. When this switch is closed, the module will conduct extensive diagnostic tests during startup. Because, the tests increase them amount of time to start the module, you will usually disable the tests unless you are troubleshooting a problem. The results of the test may be viewed via the web server interface.

Diagnostic Start	Position SW12
Enabled	Closed
Disabled	Open

The module will be shipped with all dipswitches in the Open position. This corresponds to:

Baud Rate 9600
Startup Option............ PLC Start
Configuration Lock .... Unlocked
Firmware Lock .... Unlocked
Password .... Not Bypassed
PLC Interface Mode .. High Performance
Diagnostic Start .... Disabled

> *NOTE:*
> *The Option switches are read only at module startup. If you change the switch position after startup, you must reset the module before the setting will take effect.*

2.5. Setting the Module ID Switches

When the Startup Option is set to AUTOSTART, the Module ID switches are used to determine the module IP address. The switches are ignored when the Startup Option is PLC START.

When the Module ID switches are set to a value of 00, the module will use the network parameters stored in EEPROM. When they are set to a value of 01 through FE, the module will attempt to obtain the Network parameters from a DHCP server, using the Module ID as a key. See APPENDIX E.

USING DHCP for instructions. Setting the Module ID switches to a value of FF places the 2572-A in a special configuration mode. A switch value may be changed by depressing the increment/decrement button with a small object, such as the tip of a ballpoint pen.

> *NOTE:*
> *The Module ID switches are read at module startup. If you change the switch position after startup, you must reset the module before the setting will take effect.*

2.6. Physical Installation

To insert the module into the I/O base, hold the top and bottom of the bezel and slide the module carefully into the slot, pushing it all the way into the base. If you have inserted the module correctly, you will feel a slight increase in resistance as the module mates with the base backplane connector. Once the module is fully seated in the slot, tighten the captive screws at the top and bottom to hold the module in place. To remove the module from the I/O base, loosen the captive screws, then move the module. Take care not to damage the connector at the back of the module when inserting or removing the module.

2.7. Connecting the Ethernet Cable

Insert the 8 pin (RJ-45) plug on your unshielded twisted pair cable into the RJ-45 jack on the 2572. Push the plug into the jack until the plug clicks into place. Attach the other end of the cable to an Ethernet hub or switch hub.
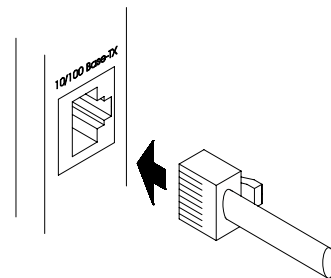
Figure 7. Ethernet Connection

2.8. Initial Power On

Turn on the base power supply. The module should perform a startup sequence, during which the LEDs will change states as described in CHAPTER 3. MODULE OPERATION.

After the module completes startup, observe the state of the Module Status (MS) and Network Status (NS) LEDs and compare to the table below.

Startup Option	LED States	Condition / Action
All Methods	MS – Steady Green NS – Steady Green	IP Parameters set and Network Server Started. Proceed with module check out procedure.
	MS – Steady Green NS – Solid Red	Another device on the network is using this IP address. Although the module will function, you must resolve the conflict to avoid unpredictable results.
PLC Start	MS – Steady Green NS – Off	Network Server not Started- Waiting on PLC Ensure that the PLC is in Run Mode, the module is configured in the I/O base, and that the correct PLC program is loaded. The program must contain a Start Network Server Command Block as associated logic.
	Other States	See APPENDIX A. 2572-A LED INDICATORS
AutoStart from EEPROM	MS – Flashing Red NS – Flashing Red	Invalid or Missing IP address in EEPROM This may occur the first time you use the module because nothing has been written to EEPROM. See the next section

Startup Option	LED States	Condition / Action
	Other States	See APPENDIX A. 2572-A LED INDICATORS
AutoStart using DHCP	MS – Solid Green NS – Alternating Red/Green	Unable to contact a DHCP server. Using backup IP parameters stored in EEPROM. *NOTE: This will be displayed at startup for about 10 seconds to provide a user alert.*
	MS – Flashing Red NS –Flashing Red	Unable to contact a DHCP server and unable to obtain a backup IP address from EEPROM.
	Other States	See APPENDIX A. 2572-A LED INDICATORS

> *NOTE:*
> *If you are using the PLC Start Option, you must log the module into the I/O configuration before PLC logic can be used to start the module network server.*

2.9. Entering the Module into the PLC I/O Configuration

To enter the module into the PLC I/O configuration, you will need to use your PLC programming application. The 2572-A is configured as a Special Function module with 2 WX and 6 WY words. In the example below, the 2572-A module is installed into slot 1 on I/O base 0 and will be logged in starting at address 1. Your configuration may differ.

```
I/O MODULE DEFINITION FOR CHANNEL  .  .  .  1   BASE .  .  .  .  .  .  00

I/O                      NUMBER OF BIT AND WORD I/O              SPECIAL
SLOT  ADDRESS    X           Y         WX         WY            FUNCTION
01    00001      00          00        02         06            YES
02    00000      00          00        00         00            NO
..    ......     ..          ..        ..         ..            ...
15    00000      00          00        00         00            NO
16    00000      00          00        00         00            NO
```

Figure 8. Sample I/O Configuration

After you read the I/O base, if the number of WX and WY words are the same as those shown in the example above and Special function = YES, then the PLC can recognize the module. Change the address as required by your application and save the result. If the line is blank or erroneous, re-check the module to ensure that it is firmly seated in the I/O base slot. Generate the PLC I/O configuration chart again by reading the I/O base. If the problem persists, contact your distributor or contact CTI.

> *NOTE:*
> *The module must be configured in the I/O table before you can use PLC logic to start the module or control the module operation from the PLC.*

2.10. Storing Network Parameters in EEPROM

Before you can automatically start the Network Server from EEPROM, you must enter the Module IP address and other network parameters. The following sections describe the available options.

Entering the Network Parameters via the module Serial Port

You can enter the network parameters using a serially attached PC and a configuration program from CTI. The CTIDIAG program used with the 2572 module will work in this application. It may be downloaded from the CTI web site.

- Install CTIDIAG on your computer.
- Connect the computer to the module serial port using a serial cable wired for RS-232. The serial cable that you use with your PLC programming software should work properly.
- Select the COM port and set the baud rate to correspond to the module selection (see Section 2.4. Setting the 2572-A Option Switches). Set the remaining port parameters as follows: Parity = Odd, Data Bits = 7, and Stop Bits = 1.
- Under the Commands menu item select SET NETWORK PARAMETERS.
- Follow the instructions on the screen for setting the network parameters.

Once you have completed this action, you must reset the module for the changes to take effect. The module will re-start using the parameters you just entered.

Changing Network Parameters using a Web Browser

Point your browser to the main 2572_A Menu page by entering the IP address in the browser URL field. For example, 192.168.177.55 would point to the web page of the 2572A module with IP address 192.168.177.55. From the main page, select MODULE CONFIGURATION. Unless you have bypassed password protection, you will be asked for a User ID and Password. *The default User ID and default Password are both CONFIG.* When the configuration page is displayed, enter the new IP address information in the appropriate fields and press the Update Module button.

The 2572-A is shipped from CTI with the IP address set to 169.254.1.1 and the subnet mask set to 255.255.0.0. To connect to the module, you must ensure that your PC has a compatible IP address. The PC subnet mask must be set to 255.255.0.0. The first two octets of the IP address must be 169.254 and the last two octets must not be 1.1. For example, an IP address of 169.254.1.2 will work.

You can set a static address in Windows using Control Panel. Instead of manually setting a static address, you can cause your PC to generate a compatible address, if DHCP (Dynamic Host Configuration Protocol is being used to obtain an IP address.

169.254.1.1 is a link local IP address. When a Windows PC is unable to obtain an IP address from DHCP, it automatically generates a link local address using a feature called Automatic Private IP Addressing. To cause the PC to generate a compatible address, do the following:
- Connect an Ethernet cable directly between your PC and the 2572-A module,
- Reboot the PC.

NOTE: It may take several minutes before the PC will stop trying to contact a DHCP server and generate the Link Local address. You can display the IP parameters being used by the PC by opening the Command Prompt window and entering IPCONFIG at the prompt. Once the link local IP address is generated, you can connect by typing http://169.254.1.1 in your browser's URL box.

Other EEPROM Update Methods

In addition to the manual methods of updating EEPROM, it is automatically updated when one of the following occurs:
- New parameters are obtained from the PLC using the PLC Start option,
- New parameters are obtained from a DHCP server using DHCP startup option.

2.11. Module Checkout

If functioning properly, the 2572-A will respond to an ICMP Echo Request message known as a *ping*. Using a PC on the local network, open the Command Prompt window and type:
PING *IPaddress* where *IPaddress* is the IP address of the module in dotted decimal format. For example, PING 192.168.177.55 would be used to ping a module with the IP address shown above. If the module does not reply, refer to CHAPTER 8. TROUBLESHOOTING.

CHAPTER 3. MODULE OPERATION

3.1. Front Panel Features

LED Indicators

The 2572-A provides an array of LEDs that inform the user of the module status and communications activity. The functions of the LEDs are described below. See APPENDIX A. 2572-A LED INDICATORS for more information.

MS   *Module Status*. Indicates the status of the module hardware and firmware. Steady Green indicates that the module hardware and software is operational. Flashing green indicates that the module is starting up. Steady red or flashing red indicates error conditions.

NS   *Network Status*. Indicates the status of the network interface. Steady Green indicates that the network server is operational (IP address has been set). Steady red or flashing red indicates error conditions. Off indicates that the network server has not been started.

LS   *Link Status*. Indicates the status of the Ethernet data link. Steady Green indicates that a link has been established between the module and the Ethernet hub or switch.

COL   *Collision*. Lights when a collision is detected. Some collisions are normal when sharing an Ethernet segment with other stations. Excessive collision activity typically indicates an overloaded network or faulty cabling.

FDX   *Full-Duplex*. Indicates the duplex mode in effect. When full duplex mode is used the LED is Steady Green. Both the module and the switch can transmit concurrently. There are no collisions in full duplex mode; both nodes have a separate transmission path. The mode is automatically negotiated between the module and the attached Ethernet switch. Full duplex can be used only with Ethernet switch configurations that have one station per segment.

100   *100 Mb*. Indicates the speed at which the network interface is operating. When the LED is Steady Green the interface is operating at 100Mb. Otherwise the Ethernet speed is 10Mb. The speed is automatically negotiated between the module and attached Ethernet hub or switch.

XMT   *Transmit*. There is one LED each for the serial port and the Ethernet port, which illuminates when data is transmitted.

RCV   *Receive*. There is one LED each for the serial port and the Ethernet port, which illuminates when a signal is received. The Ethernet LED will flash when any network traffic is detected, not just packets addressed to the module.

Reset Button

Some module functions, such as reading module switch settings, are performed only at startup. The Reset Button is a momentary contact switch that allows you to restart the module without having to cycle power to the base. It is recessed to prevent inadvertent use. To reset the module, use a small object such as the tip of a ball point pen to depress and hold the switch for approximately one second. When the switch is released, the module will begin the startup sequence (see Section 3.2).

Module ID Switches

The Module ID switches are used to identify the module to a DHCP server. See APPENDIX E. USING DHCP. When the switches are set to a value of 00, the module will obtain IP parameters from EEPROM. A value of FF selects a special configuration mode. By depressing the actuator at the top or bottom of the switch, you can decrement or increment the switch value. The top switch is the most significant digit in the Module ID.

> *NOTE:*
> *The value of the Module ID switches are read only at module startup. They are ignored if you are using the PLC start option.*

Serial Port

The Serial port can be used to set network parameters such as the IP address when no other method is acceptable. It provides a subset of the RS-232 interface that should work with most PLC programming cables.

Ethernet Port

The Ethernet Port accepts standard 10BaseT or 100BaseTX cables (shielded or unshielded twisted pair). To connect the cable, align the connector tabs and insert the cable until the restraining lock snaps in place. To remove, press the cable release and remove the cable.

3.2. Module Startup

When power is applied to the module or the module is reset, the module will perform a lamp test which will flash all the software-controlled LEDs in sequence.

Once the test has been successfully completed, the module will read the network parameters and start the application firmware. The exact sequence depends on the startup method you have selected. See **Choosing a Module Startup Method** on page 9. During the startup process, the Module Status indicator will blink green. Once the application firmware has successfully started, the Module Status indicator will be steady green. When the network server has successfully started the Network Status LED will be steady green.

3.3. Normal Operation

Status LEDs

Indicator	Normal State
Module Status (MS)	Steady Green - Operational
Network Status (NS)	Steady Green – Operational
Link Status (LS)	Steady Green – Physical Link Established

Other LEDs

The state of the other LEDs may vary depending on the method of operation.

Indicator	Normal State
Collision (COL)	May flash occasionally in normal operation. Heavy activity indicates a network problem (excessive traffic or faulty cabling).
Full Duplex (FDX)	Steady Green – Full duplex, Off – Half Duplex
100 Mb (100 Mb)	Steady Green – 100Mb, Off – 10Mb
Serial XMT	Will illuminate/flash if the serial port is transmitting data
Serial RCV	Will illuminate/flash if the serial port is receiving data
Ethernet XMT	Will illuminate/flash if the Ethernet port is transmitting data (see note
Ethernet RCV	Will illuminate/flash if the Ethernet port detects a packet being received. (see note below)

Server Operation

To use the module as a server, no special PLC logic or configuration is required. You simply provide a client application that communicates with the module. For example, your HMI application, using a 2572 driver or OPC server, can be used to read and write PLC data. Also, programming software, such as Workshop by FasTrak Softworks can be used to program the module via the network.

Client Operation

To use the module to perform client operations, you must include PLC logic that triggers the module operation. See CHAPTER 5. CAMP CLIENT COMMANDS.

CHAPTER 4. CAMP SERVER COMMANDS

4.1. Overview

This chapter explains how to use PLC logic to start the 2572-A CAMP network server. If you are starting the module using one of the AutoStart options, you can skip the remainder of this chapter.

The *Start Network Server* command is used when you want to establish the network parameters using PLC logic. When you use PLC logic to set the network parameters, you can ensure that the IP address is directly associated with the PLC and not the module.

> **NOTE:**
> *Before you can use PLC logic to start up the PLC network server function, the Network Startup Option switch must be set to PLC Start (See Section 2.4).*

The 2572-A uses the PLC V memory to store command information and the module WX/WY words to control execution of the commands. If you are not familiar with this interface, please refer to APPENDIX C. PLC COMMAND INTERFACE .

The network parameters are set by the PLC when the *Start Network Server* command block is executed. This block is shown on the following page. In the illustration, a **bold** entry is a required value. A non-bold entry is a *recommended* value that you should use unless you have reason to do otherwise. Values for the command block entries are shown in both hexadecimal and decimal (integer) format. Using your PLC programming software, you can configure a chart to display the values either way.

This command should be executed only when the *Network Configuration Required* bit (NET CFG) is set. The NET CFG bit is set shortly after power is first applied to the module or after the module is reset for any reason. It remains on until the network parameters have been set. If you have chosen the *PLC Start* option for network startup, you must successfully complete this command before the 2572-A will respond to any other network commands. See the ladder example on page 29.

> **NOTE:**
> *When you trigger the Start Network Server command while the command block contains invalid data, the 2572-A will return an error code and then halt. To recover, you must correct the command block entry and reset the module.*

4.2. Start Network Server Command Block

Offset	Description	Hex Value	Decimal Value
0	Command Error Word	**0000**	**0**
1	Command (Start Network Server)	**0004**	**4**
2	Connection Number (19291 - 19299)	4B62	19298
3	Protocol Manager Number	**0023**	**35**
4	Startup Option Bits (see description below)	0000	0
5	TCP Keep Alive Interval in Seconds (0=default = 60) (Set to 65000 or greater to disable Keep Alive)	0000	0
6	IP Address of this Module (High 16 bits)		
7	IP Address of this Module (Low 16 bits)		
8	TCP / UDP Port Number	05E1	1505
9	IP Address of Default Router (High 16 bits)		
10	IP Address of Default Router (Low 16 bits)		
11	Max Number of TCP Connections (0=default)	0000	0
12	Subnet Mask (High 16 bits)		
13	Subnet Mask (Low 16 bits)		
14	IP Multicast Receive Address (High 16 bits). If you do not want to receive multicast, set this value to 0.	0000	0
15	IP Multicast Receive Address (Low 16 bits). If you do not want to receive multicast, set this value to 0.	0000	0

Offset 0   *Error Word* - Set to 0 so that any previous error code is cleared.

Offset 1   *Command Code* - The Command for Start Network Server is 4.

Offset 2   *Connection Number* - You should set this to number in the range of 19291 to 19299 to prevent inadvertent conflict with any client connections you may create. The value of 19298 is used in CTI examples.

Offset 3   *Protocol Manager Number* - Protocol Managers control the operation of the serial and network ports. Protocol Manager 35 (23 hex) selects the PLC Network Server.

Offset 4   *Startup Option Bits* - These bits allow you to configure certain options for the PLC server. The bits are used as follows:

Bit 1	Bit 2	Bit 3	Bits 4-16
Used by CTI 2572 module, ignored by 2572-A.	Used by CTI 2572 module, ignored by 2572-A.	Used by CTI 2572 module, Ignored by 2572-A.	Reserved (set to 0)

Offset 5   *TCP Keep Alive Interval* - This value specifies the amount of elapsed time (in seconds) without any messages from the client application before the 2572-A will automatically close a server TCP socket. If the value is set to 0, then the 2572-A will use the default value of 60 seconds. To disable Keep Alive, set the value to 65,000 or greater.

Offset 6-7   *IP Address* Offset 6 should contain the high 16 bits of the module IP address. Offset 7 should contain the low 16 bits of the IP address. An IP address of 0.0.0.0 (0000 0000 hex) or greater than 223.255.255.255 (DFFF FFFF hex) is will return an error.

Offset 8   *TCP/UDP Port* - This will be the port number used to connect to the 2572-A PLC Server application. The examples in this manual assume that this will be set to 1505 decimal. You should use this value unless you have a reason to do otherwise. A port number of 0 is invalid.

Offset 9-10   *IP Address of Default Router* - This identifies the address of the router to which unknown IP addresses will be directed. Offset 8 contains the high 16 bits of the address and Offset 9 contains the low 16 bits. An address greater than 223.255.255.255 (DFFF FFFF hex) will return an error. If you do not have a router on your network, set this to 0.0.0.0 (0000 0000 hex).

Offset 11   *Maximum Number of TCP Connections*- This specifies the maximum number of concurrent TCP connections to the PLC server that will be allowed. Once the maximum number has been attained, the 2572-A will reject further attempts to connect until a connection is relinquished. Once a connection is properly closed, the slot is available for another connection. If you set the value in this word to 0, then the 2572-A will use the default module value of 16. You may set this to a number less than 16 to limit access or increase the number up to 24 to allow more connections.

Offset 12-13 *Subnet Mask* - Specifies the subnet mask assigned to this network. Offset 12 contains the high 16 bits of the mask and Offset 13 contains the low 16 bits. If offset 12 and 13 contain a value of 0, then the subnet mask will default to the standard for the IP address class. A subnet mask must contain all 1's in the network portion of the IP address and must allow at least 2 bits of host address. In addition, the subnet mask cannot be set so that the derived host address is 0 or a broadcast address (all bits set to 1). See APPENDIX D. IP ADDRESS INFORMATION.

NOTE:
All computers on a physical network must use the same Subnet mask and
Network ID; otherwise, addressing and routing problems can occur. Host ID's on the same network
must be unique.

Offset 14-14 *IP Multicast Receive Address* – If you want the module to receive multicast data, enter the multicast address that you want the module to listen to. The valid range of multicast addresses is 224.0.0.34 through 239.255.255.255. If you do not want to listen to a multicast address, set these words to a value of 0.

When you are setting up the various IP addresses and subnet mask, you should set up your PLC programming software to display the words in hexadecimal. Then you can enter each byte of the dotted notation individually. For example, if the IP address were 198.35.34.10, you could enter the first word as hex C623 where the high byte (C6) is the hex equivalent of decimal 198 and the low byte (23) is the hex equivalent of decimal 35. Similarly, you would enter the second word as hex 220A. See the following illustration.

Hex Value	**C6 23** ⟶	**C623**	Offset 6
Dotted Decimal	**198. 35.34.10**		
Hex Value	**22 0A** ⟶	**220A**	Offset 7
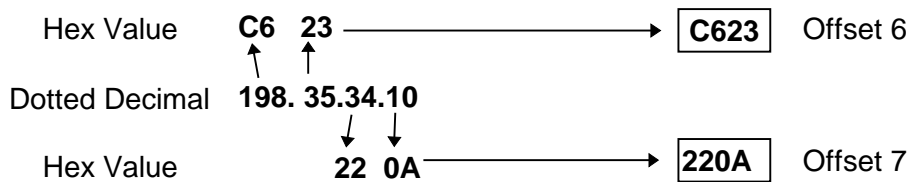
Figure 9. Representing IP Address in Hexadecimal Format

Command Block Example

The following command block can be used to start up the 2572-A network server at IP address 192.168.177.08 (in hex notation this is C0.A8.B1.08). The server is set up to listen on TCP/UDP port number 1505. The IP address of the default router is 192.168.177.241 (hex equivalent C0.A8.B1.F1).

To enter the IP addresses, you will find it much easier to enter the values in hexadecimal format. When the V memory display is set to hex, you enter the hex equivalent of the first number in the high byte of offset 6 and the hex equivalent of the second number in the low byte of offset 6. Similarly, the third and fourth numbers in the address are entered in the high and low byte of offset 7.

Offset	Description	Hex	Decimal
0	Error Word	0000	0
1	Command (Start Network Server)	0004	4
2	Connection Number (19291 -- 19298)	4B62	19298
3	Protocol Manager Number	0023	0035
4	Startup Option Bits	0000	0
5	TCP Stale Socket Timeout in seconds (0=none))	0000	0
6	IP Address of this Module (High 16 bits)	C0A8	49320
7	IP Address of this Module (Low 16 bits)	B108	45320
8	TCP / UDP Port Number	05E1	1505
9	IP Address of Default Router (High 16 bits)	C0A8	49320
10	IP Address of Default Router (Low 16 bits)	B1F1	45553
11	Max Number of TCP Connections (0=default)	0000	0
12	Subnet Mask (High 16 bits)	0000	0
13	Subnet Mask (Low 16 bits)	0000	0
14	IP Multicast Address (High 16 bits)	0000	0
15	IP Multicast Address (Low 16 bits)	0000	0

NOTE:
This command block should be executed only at module startup time. The 2572-A will set the Network Configuration Required bit (WX1.3) to indicate that this is necessary.

Ladder Logic Example

The following diagram illustrates the ladder logic that executes the Start Network Server command block. This example assumes that the command block is located in V memory starting at V500 and that command slot 1 is used for the command.
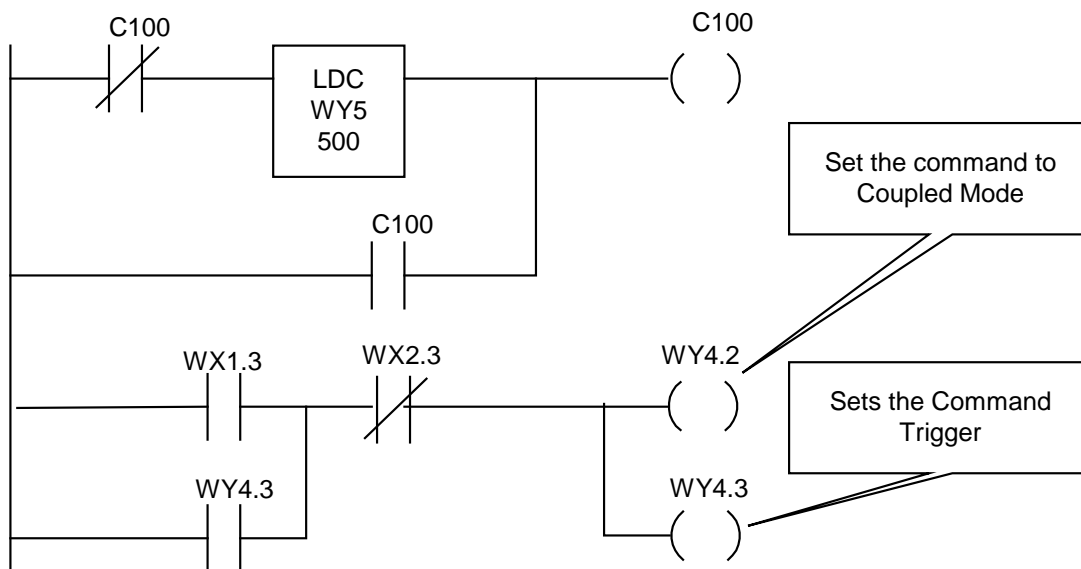
Rung 1 loads the location of the Command Block (V500) into Command Slot 1 (WY5). Once the control relay is on, it seals off the command. The load command will be bypassed on subsequent scans.

Rung 2 sets the COMMAND TRIGGER (WY4.3) and COMMAND MODE (WY4.2) when the NET CFG bit (WX1.3) is on and the COMMAND BUSY bit (WX2.3) is off. When the logic sees the 2572-A raise COMMAND BUSY (WX2.3), it lowers the COMMAND MODE (WY4.2) and COMMAND TRIGGER (WY4.3), completing the coupled mode cycle.

The NET CFG bit will be raised by the 2572-A at any time the network configuration parameters are not set. Therefore this logic will re-execute the Start Network Server command, if the 2572-A is reset for any reason.

> *NOTE:*
> *Do not use retentive relays in this logic. Proper operation of this logic depends on the control relay transitioning from off to on when power is cycled.*

CHAPTER 5. CAMP CLIENT COMMANDS

5.1. Overview

The CAMP client commands are used when you wish to use PLC logic to initiate communications. This function may be used for peer to peer communications among PLCs or to send unsolicited data to your HMI application. For example, you might use this function to report alarms to a supervisory PC, avoiding the requirement to continuously poll for alarm data.

> *NOTE:*
> *If you are using the 2572-A in Server mode only, you can skip the this chapter*

5.2. CAMP Multicast Operation

Firmware versions 2.00 and above provide support for IP Multicast. Using multicast, you can write data to multiple modules using one command. This reduces network loading and simplifies the client logic.

The TCP/IP protocol reserves a block of IP addresses (224.0.0.0 through 239.255.255.255) for multicast use. 2572-A modules can be configured to accept packets with one of these addresses. When a packet with the specified address is received, the message is passed to the CAMP server, which processes the command. Unlike the typical unicast address, multiple modules can have the same multicast address; thus, a single packet can be used to update multiple modules. Modules that are not configured with a multicast address or that use a different multicast address do not process the message. This allows you to create a group of modules that will participate in a specific multicast session.

You can configure a 2572-A to receive on a multicast address using the same methods used to establish the other TCP/IP network parameters.
1. If you are using the PLC Start method, the multicast address can be specified in the Start Network server command block. See *Section 4.2. Start Network Server Command Block.*
2. If you are starting the module using IP parameters stored in EEPROM, you can use the Web Server interface to enter the multicast address.
3. If you are using DHCP, you can add the multicast address to the parameters that are provided by the DHCP server.

> *Caution:*
> *To prevent inadvertent overwriting of V memory data in other PLCs, ensure that only the modules that you want to participate in the multicast session are configured with the multicast address.*

To send a multicast message, you need to do the following:
1. Execute the CREATE SOCKET command using a multicast address. This command is explained in the following section.
2. Use the UNACKNOWLEDGED WRITE command to send a multicast message containing the data you wish to write. See page 40 for a description of this command.

5.3. Create Socket Command

The CREATE SOCKET command provides a means for your PLC logic to refer to another network node when sending messages. You must complete the CREATE SOCKET command before you can send messages to another node on the network.

The CREATE SOCKET command creates a local TCP/IP socket and associates it with the remote socket specified by the values for IP address and port in the command block. If TCP is specified, an actual logical connection to the remote node is attempted. If the connection cannot be established, the 2572-A will return an error code to the PLC. If UDP is specified, the 2572-A module saves the address and port number as the default remote socket, but no connection attempt is made. Once the CREATE SOCKET command completes successfully, your logic can use the Connection Number to refer to the remote socket. You can establish up to eight concurrent connections.

Create Socket Command Block

Offset	Description	Hex	Decimal
0	Error Word	**0000**	**0**
1	Command Code (Create Socket)	**0003**	**03**
2	Connection Number (19221 - 19228)		
3	Protocol Manager Number	**0024**	**36**
4	Startup Option Bits (see description below)	*0000*	*0*
5	Type of Service (1 = TCP, 2 = UDP/Multicast)		
6	IP Address of Remote Device or Multicast Address (High 16 bits)		
7	IP Address of Remote Device or Multicast Address- (Low 16 bits)		
8	Unused (Set to 0)	**0000**	**0**
9	Remote Device - TCP/UDP Port Number		
10-15	Unused (Set to 0)	**0000**	**0**

Offset 0   *Error Word* - Set to 0 so that any previous error codes are cleared.

Offset 1   *Command Code* - The Command Code of the CREATE SOCKET command is 03.

Offset 2   *Connection Number* - Network Client connection numbers may range from 19221
                  through 19228. Any connection number within the valid range can be assigned, as
                  long as the number is unique. Connections can be closed and re-used, if desired. To
                  help keep track of the connection numbers, you may wish to assign connection
                  numbers sequentially.

Offset 3   *Protocol Manager Number* - Protocol Managers control the operation of the serial
                  and network ports. The Protocol Manager Number for the CAMP Client protocol
                  manager is decimal 36 (hex 24).

Offset 4   *Startup Option Bits* -

Bits 1 - 14	Bit 15 - IP Address Location	Bit 16
Reserved	0 = Use IP Address in CREATE SOCKET Command Block. 1 = Use IP Address in MEMORY TRANSFER Command Block (UDP Only)	Not Used in 2572-A

When bit 15 is set to 1 (Offset 4 = 0x0002) and the UDP protocol is selected (in
Offset 5), the Command Blocks used for Memory Transfer (READ REMOTE, WRITE
REMOTE, and MEMORY EXCHANGE) will specify the IP Address and Port Number for
the remote device.

This feature allows you to use a single socket to communicate with different remote
devices. When bit 15 is set to 0, the IP address and port number entered in this
CREATE SOCKET command block will be used. The TCP protocol, since it is
connection-oriented, will always use the IP address and port number in this CREATE
SOCKET command block. If you select TCP and set bit 15 to 1, the 2572-A will
return an error.

> *NOTE:*
> *Even if you set bit 15 to 1, you still must provide a valid IP address and Port number in the Command Block of the CREATE SOCKET command. If you don't do this, a Command Error will be generated when you execute the CREATE SOCKET command.*

Offset 5   *Type of Service* - Selects TCP or UDP/Multicast service. Using TCP, a connection is
                  established with the other node. If the TCP connection cannot be established, the
                  2572-A will indicate an error. Using UDP/Multicast, the local socket is created but
                  no connection is established with the target node.

> *NOTE:*
> *If TCP is selected and the connection with the target node (remote host) is lost, the 2572-A will report a socket connection error code (such as 240A - Socket not Connected) the next time you attempt to read/write data. After the error is acknowledged, the 2572-A will complete error recovery by **automatically closing the socket**. A subsequent attempt to read/write data will result in a 00A6 (connection not active) error. See Appendix B for error code listings. Your logic should re-execute the Create Socket command if the connection is not active.*

Offset 6-7 *IP Address* - If the IP ADDRESS SELECTION option bit in Offset 4 is set to 0, these words specify the IP address of the destination node. Since the IP address consists of 32 bits, the address is contained in two 16 bit words. An IP address of 0.0.0.0 will return an error. If you are using TCP, the largest valid IP address is 223.255.255.255. If you are using UDP/Multicast, you can also enter multicast addresses ranging from 224.0.0.2 through 239.255.255.255.

Offset 8 *Unused* - This word is not used when creating a TCP/IP socket. It should be set to 0.

Offset 9 *TCP/UDP port number* - If the IP ADDRESS SELECTION option bit in Offset 4 is set to 0, this word specifies the TCP/UDP port number of the remote node. If you are accessing another 2572, you will typically set this value to 1505 (the recommended value for the 2572-A PLC server). If you are using UDP and bit 15 of offset 4 is set to 1, then this address becomes the default port number.

Offset 10-15 *Unused* - These words are unused and should be set to 0.

5.4. Close Socket Command

The following command block will close a connection to a TCP/IP socket. Once the connection has been successfully closed, you can re-use the connection number in a subsequent CREATE SOCKET command block.

Offset	Description	Hex Value	Decimal Value
0	Error Word	0000	0
1	Command Code (Close Connection)	0002	02
2	Connection Number (19221 - 19228)		
3- 15	Unused (Set to 0)	0000	0

Offset 0 *Error Word* - Set to 0 so that any previous error codes are cleared.

Offset 1 *Command Code* - The Command Code of the Close Connection command is 02.

Offset 2 *Connection Number* - You can specify any connection number that has been previously established in a Create Socket command block.

Offset 3-15 *Unused* - These words are unused by this command and should be set to 0.

> *NOTE:*
> *This command can be used only for client connections. You cannot use the command to close the connection to the PLC Network Server.*

5.5. Memory Transfer Commands

Memory Transfer commands are designed to provide a device independent method of transferring data words. For SIMATIC® 505 PLCs, the memory transfer commands provide a simple way to transfer V memory between the local PLC and another PLC (or suitably programmed computer) on the network. These commands access only the first 64K bytes of V memory. Before using the Memory Transfer commands you must have successfully completed a CREATE SOCKET command.

Word Transfer - Write

This function reads the contents of a designated area of V memory in the local PLC and writes the values in a specified area of memory in another PLC. You can specify the starting memory addresses on both the local and remote PLCs and the number of words to be transferred (up to 256 words). When the command is triggered, the 2572-A reads the local V memory and sends a request message to the remote PLC. When the response is returned from the remote PLC, the 2572-A verifies that the message was properly processed. If not, the 2572-A places the error code in the command block and raises the applicable error bit. The following command block is used for the WRITE command.

Offset	Description	Hex	Decimal
0	Error Word	0000	0
1	Command Code (Write)	0201	513
2	Connection Number (19221 - 19228)		
3	Source: Starting V Memory Address in the Local PLC		
4	Number of Words to Transfer (1-256)		
5	Destination: Starting V Memory Address in Remote PLC		
6	Command Timeout in seconds (0 = Use Default)	0000	0
7 - 9	Unused (Set to 0)	0000	0
10	IP Address of Remote Device - High 16 bits (UDP Only: IP Address Location bit in the Create Socket command must be set to 1)		
11	IP Address of Remote Device - Low 16 bits (UDP Only: IP Address Location bit in the Create Socket command must be set to 1)		
12	UDP Port Number of Remote Device (UDP Only: IP Address Location bit must be set to 1)		
13 - 15	Unused (Set to 0)	0000	0

Offset 0   *Error Word* - Set to 0 so that any previous error codes are cleared.

Offset 1   *Command Code* - The Command Code is 513 decimal (or 0201 hexadecimal).

Offset 2   *Connection Number* - You can specify any connection number that has been previously established in a CREATE SOCKET command block.

Offset 3   *Source* - The starting address of V memory which contains the values you want to transfer. The address is 1 relative.

Offset 4   *Number of Words* - This indicates the number of words you want to transfer.

Offset 5   *Destination* - The starting address of V memory in the remote PLC that you want to
                update. This address is 1 relative.

Offset 6   *Command Timeout in seconds* - When set to 0, the default value of approximately 9
                seconds is selected. A value of 999 specifies an infinite timeout.

Offset 7-9   *Unused* - Set to 0.

Offset 10-11   *IP Address* – **UDP Only**. If you set the IP Address Location bit to 1 (see offset 4 of
                the CREATE SOCKET command block), you must specify the IP address of the remote
                device or a multicast address in these words. If the IP Address Location bit is set to
                0, these words are ignored and the IP address contained in the CREATE SOCKET
                command block is used. An IP address of 0.0.0.0 (0000 0000 hex) or greater than
                223255.255.255 (DFFF FFFF hex) will return an error.

Offset 12   *UDP port number* – **UDP Only**. If you set the IP Address Location bit to 1 (see
                offset 4 of the CREATE SOCKET command block), you must specify the UDP port
                number of the remote device. If you are accessing another 2572, you will typically
                set this value to 1505 (the recommended value for the 2572-A PLC server). If the IP
                Address Location bit is set to 0, this word is ignored and the port number contained
                in the CREATE SOCKET command block is used.

Offset 13-15   *Unused* - Set to 0.

Word Transfer - Read

This function reads the contents of a designated area of V memory in the remote PLC and writes the
values in a specified area of V memory in the local PLC. You can specify the starting V memory
addresses on both the local and remote PLCs and the number of words to be transferred (up to 256
words). When the command is triggered, the 2572-A sends a request message to the remote PLC.
When the response is returned, the 2572-A verifies the response. If there is no error, the 2572-A
writes the data in local V memory. If an error is encountered, the 2572-A will post an error which
may be processed by PLC logic.

The following command block will cause the 2572-A to read the designated V memory in the remote
PLC and store the result in local V memory.

Offset	Description	Hex	Decimal
0	Error Word	**0000**	**0**
1	Command Code (Read)	**0202**	**514**
2	Connection Number (19221-19228)		
3	Source: Starting V Memory Address in Remote PLC		
4	Number of Words to Transfer (1-256)		
5	Destination: Starting V Memory Address in this PLC		
6	Command Timeout in seconds (0 = Use Default)	0000	0
7-9	Unused (Set to 0)	**0000**	**0**

Offset	Description	Hex	Decimal
10	IP Address of Remote Device - High 16 bits		
	(UDP Only: IP Address Location bit in the Create Socket command must be set to 1)		
11	IP Address of Remote Device - Low 16 bits		
	(UDP Only: IP Address Location bit in the Create Socket command must be set to 1)		
12	UDP Port Number of Remote Device		
	(UDP Only: IP Address Location bit in the Create Socket command must be set to 1)		
13 - 15	Unused (Set to 0)	**0000**	**0**

Offset 0   *Error Word* - Set to 0 so that any previous error codes are cleared

Offset 1   *Command Code* - The Command Code is 514 decimal (or 0202 hexadecimal).

Offset 2   *Connection Number* - You can specify any connection number that has been previously established in a CREATE SOCKET command block.

Offset 3   *Source* - The starting address of V memory in the remote PLC which contains the values you want to transfer. This address is 1 relative.

Offset 4   *Number of Words* - This indicates the number of words you want to transfer.

Offset 5   *Destination* - The starting address of V memory in the local PLC that you want to update. This address is 1 relative.

Offset 6   *Command Timeout in seconds* - When set to 0, the default value of approximately 9 seconds is selected. A value of 999 specifies an infinite timeout.

Offset 7-9   *Unused* - Set to 0.

Offset 10-11   *IP Address* - **UDP Only.** If you set the IP Address Location bit to 1 (see offset 4 of the CREATE SOCKET command block), you must specify the IP address of the remote device. Since the IP address consists of 32 bits, the address is contained in two 16 bit words. An IP Address of 0.0.0.0 (0000 0000 hex) or greater than 223.255.255.255 (DFFF FFFF hex) will return an error. If the IP Address Location bit is set to 0, these words are ignored and the IP address contained in the CREATE SOCKET command block is used.

Offset 12   *UDP port number* - **UDP Only.** If you set the IP Address Location bit to 1 (see offset 4 of the CREATE SOCKET command block), you must specify the UDP port number of the remote device. If you are accessing another 2572, you will typically set this value to 1505 (the recommended value for the 2572-A PLC server). If the IP Address Location bit is set to 0, these words are ignored and the port number contained in the CREATE SOCKET command block is used.

Offset 13-15   *Unused* - Set to 0.

Word Transfer - Exchange

This function is a combination of the WRITE and READ commands. As the name implies, it is intended to be used in applications that exchange values between two PLCs or a PLC and a PC. The command writes the contents of a block of local PLC V memory to a block of memory in the remote PLC, then reads a block of V memory in the remote PLC and writes the values to a block of V memory in the local PLC. Since this is accomplished in one transaction, it is much faster than executing separate read and write commands.

You can specify the locations of the V memory blocks in the local and the remote PLC, the number of words to be written to the remote PLC, and the number of words to be read from the remote PLC. When the command is triggered, the module in the local PLC retrieves the data from the specified memory and sends a message containing the data to be written to the module in the remote PLC. If the write was successful, the module in the remote PLC will read the specified V memory and build a reply message containing the data. When the response message is returned, the local module will write the data to the local PLC V memory.

If an error is encountered writing the data to the remote PLC, no data will be read from the remote PLC; an error message indicating the write failed will be returned. If an error is encountered reading data, an error message indicating the read failed will be returned. In either case, the module will set the applicable error bit and write the error code into the Command Error Word.

The following command block is used for the Exchange command.

Offset	Description	Hex	Decimal
0	Command Error Word	**0000**	**0**
1	Command Code (Exchange)	**0203**	**515**
2	Connection Number (19221 - 19228)		
3	Write Source: Starting V Memory Address in Local PLC		
4	Number of Words to Write (1-254)		
5	Write Destination: Starting V Memory Address in Remote PLC		
6	Command Timeout in seconds (0=Use Default)	0000	0
7	Read Source: Starting V Memory Address in Remote PLC		
8	Number of Words to Read (1-256)		
9	Read Destination: Starting V Memory Address in Local PLC.		
10	IP Address of Remote Device - High 16 bits (UDP Only: IP Address Location bit in the Create Socket command must be set to 1)		
11	IP Address of Remote Device - Low 16 bits (UDP Only: IP Address Location bit in the Create Socket command must be set to 1)		

12	UDP Port Number of Remote Device (UDP Only: IP Address Location bit in the Create Socket command must be set to 1)		
13 - 15	Unused (Set to 0)	**0000**	**0**

Offset 0   *Command Error Word* - Your PLC logic should set this to 0 so that any previous error code is cleared. If a processing error is encountered, the module will write an error code into this word.

Offset 1   *Command Code* - The Command Code for EXCHANGE is 515 (hex 0202).

Offset 2   *Connection Number* - Use the connection number that was established in the CREATE SOCKET command block.

Offset 3   *Write Source: Starting V Memory* - Enter the first V memory location in the *local* PLC which contains the values which you wish to write to the remote PLC.

Offset 4   *Number of Words to Write* - Enter the number of words you want to write.

Offset 5   *Write Destination: Starting V Memory* - Enter the beginning address of the V memory block in the *remote* PLC to which you want to write this data.

Offset 6   *Command Timeout in seconds* - When set to 0, the default value of approximately 9 seconds is selected. A value of 999 specifies an infinite timeout.

Offset 7   *Source: Starting V Memory* - Enter the first V memory location in the *remote* PLC from which you wish to read data.

Offset 8   *Number of Words to Read* - Enter the number of words you want to read.

Offset 9   *Destination: Starting V Memory* - Enter the beginning address of the V memory block in the *local* PLC to which you want to write this data.

NOTE:
The memory exchange command must contain at least one word to write or an error will be returned. The maximum number of words which can be written with a single command is 254. The maximum number of words that can be read is 256.

Offset 10-11   *IP Address* - **UDP Only.** If you set the IP Address Location bit to 1 (see offset 4 of the CREATE SOCKET command block), you must specify the IP address of the remote device. Since the IP address consists of 32 bits, the address is contained in two 16 bit words. An IP Address of 0.0.0.0 (0000 0000 hex) or greater than 223.255.255.255 (DFFF FFFF hex) will return an error. If the IP Address Location bit is set to 0, these words are ignored and the IP address contained in the CREATE SOCKET command block is used.

Offset 12   *UDP port number* - **UDP Only**. If you set the IP Address Location bit to 1 (see offset 4 of the CREATE SOCKET command block), you must specify the UDP port number of the remote device. If you are accessing another 2572, you will typically set this value to 1505 (the recommended value for the 2572-A PLC server). If the IP Address Location bit is set to 0, these words are ignored and the port number contained in the CREATE SOCKET command block is used.

Offset 13-15   *Unused* - Set to 0.

Word Transfer – Unacknowledged Write

This command is designed to be used with multicast addresses, where one message can be used to update multiple modules. Like the standard write command, this command reads the contents of a designated area of V memory in the local PLC and writes the values in a specified area of memory in another PLC. However, because multiple modules could receive this message, CAMP servers that receive this command do not reply and the client does not verify that the message was received by any server.

The following command block is used for the UNACKNOWLEDGED WRITE command.

Offset	Description	Hex	Decimal
0	Error Word	**0000**	**0**
1	Command Code (Unacknowledged Write)	**0204**	**516**
2	Connection Number (19221 - 19228)		
3	Source: Starting V Memory Address in the Local PLC		
4	Number of Words to Transfer (1-256)		
5	Destination: Starting V Memory Address in Remote PLC		
6 - 9	Unused (Set to 0)	**0000**	**0**
10	IP Address of Remote Device - High 16 bits (UDP/Multicast Only: IP Address Location bit in the Create Socket command must be set to 1)		
11	IP Address of Remote Device - Low 16 bits (UDP Only/Multicast: IP Address Location bit in the Create Socket command must be set to 1)		
12	UDP Port Number of Remote Device (UDP/Multicast Only: IP Address Location bit must be set to 1)		
13	Minimum Production Interval in milliseconds. (0= Default Value = 1000ms)	0000	0
14- 15	Unused (Set to 0)	**0000**	**0**

Offset 0   *Error Word* - Set to 0 so that any previous error codes are cleared.

Offset 1   *Command Code* - The Command Code is 516 decimal (or 0204 hexadecimal).

Offset 2   *Connection Number* - You can specify any connection number that has been previously established in a CREATE SOCKET command block.

Offset 3   *Source* - The starting address of V memory which contains the values you want to transfer. The address is 1 relative.

Offset 4   *Number of Words* - This indicates the number of words you want to transfer.

Offset 5   *Destination* - The starting address of V memory in the remote PLC that you want to update. This address is 1 relative.

Offset 6-9   *Unused* - Set to 0.

Offset 10-11   *IP Address* – **UDP/Multicast Only**. If you set the IP Address Location bit to 1 (see offset 4 of the CREATE SOCKET command block), you must specify the IP address of the remote device or a multicast address in these words. If the IP Address Location bit is set to 0, these words are ignored and the IP address contained in the CREATE SOCKET command block is used. An IP address of 0.0.0.0 (0000 0000 hex) or greater than 239.255.255.255 (EFFF FFFF hex) will return an error.

Offset 12   *UDP port number* – **UDP/Multicast Only**. If you set the IP Address Location bit to 1 (see offset 4 of the CREATE SOCKET command block), you must specify the UDP port number of the remote device. If you are accessing another 2572, you will typically set this value to 1505 (the recommended value for the 2572-A PLC server). If the IP Address Location bit is set to 0, this word is ignored and the port number contained in the CREATE SOCKET command block is used.

Offset 13   *Minimum Production Interval* – When uncoupled trigger mode is used, this word allows you to specify the minimum time interval (in milliseconds) between successive transmissions of the command message. A value of 0 uses the default of 1000 ms. The value may range from 50 to 10,000.

> *NOTE:*
> *If you want to use the timer to control message production, you should select uncoupled mode and leave the trigger bit set. See APPENDIX C. PLC COMMAND INTERFACE for more information*
>
> *Depending on the PLC scan time, the actual interval may be greater than the interval specified. It requires two scans to process the command. If the Minimum Production Interval value is greater than two scan times, you must add one scan time to the interval specified.*

> *NOTE:*
> *You should avoid setting the minimum production level to a value lower than you actually need. This can create additional messages that unnecessarily increase the load on the modules involved in the multicast session, resulting in reduced performance.*

Offset 14-15   *Unused* - Set to 0.

5.6. Application Examples

TCP Client Example

This example creates a TCP connection to another module and writes data from the local PLC V memory to V memory in a remote PLC.

Create Socket Command Block

This command block creates a TCP socket that is associated with another 2572-A on the network at IP address 192.168.177.01 (hex C0.A8.B1.01) and TCP port 1505. The TCP protocol is selected.

Offset	Description	Hex	Decimal
0	Error Word	0000	0
1	Command Code (Create Socket)	0003	03
2	Connection Number (19221 - 19228)	4B15	19221
3	Protocol Manager Number	0024	36
4	Startup Option Bits	0000	0
5	Type of Service (1 = TCP, 2 = UDP)	0001	1
6	Remote Device - High 16 bits of IP Address	C0A8	49320
7	Remote Device - Low 16 bits of IP Address	B101	45313
8	Unused (Set to 0)	0000	0
9	TCP/UDP Port Number	05E1	1505
10-15	Unused (Set to 0)	0000	0

Depending on your application requirements, you may wish to create the socket(s) immediately after the network server is started and leave the socket active all the time. If you do not need to free up a socket for another use, you will probably select this option. Alternately, you could create the socket, send the data, and then close the socket.

> *NOTE:*
> *You should use Coupled Mode logic since you want to execute this command only once per trigger.*
> *See Appendix D for additional information on command modes.*

Word Transfer Command Block

The following command block writes 25 words obtained from local PLC V memory starting at V100 to the a block of V memory starting at V200 in the remote PLC.

Offset	Description	Hex	Decimal
0	Error Word	0000	0
1	Command Code (Write)	0201	513
2	Connection Number (19221 - 19228)	4B15	19221
3	Source: Starting V Memory Address in this PLC	0064	100
4	Number of Words to Transfer (1-256)	0019	25
5	Destination: Starting V Memory Address in Remote PLC	00C8	200
6	Command Timeout in seconds (0 = Use Default)	0000	0
7-15	Unused (Set to 0)	0000	0

If you need to verify that the command was completed successfully, you can monitor the error status. If a problem occurs while executing the command, the 2572-A will set the CMD ERR bit and place the applicable error code in the Error Word. See *Appendix D* for additional information.

UDP Client Example

This example creates a UDP Socket with the address location bit set to allow the target IP address to be set in the Word Transfer commands. The Write command block can then be used to write to different modules.

Create Socket Command Block
This command block creates a UDP socket with a default IP address of 192.168.177.01 (hex C0.A8.B1.01) and UDP port 1505. Note that the startup option bit 15 is set (Word 4 = 0x0002).

Offset	Description	Hex	Decimal
0	Error Word	0000	0
1	Command Code (Create Socket)	0003	03
2	Connection Number (19221 - 19228)	4B15	19221
3	Protocol Manager Number	0024	36
4	Startup Option Bits	0002	2
5	Type of Service (1 = TCP, 2 = UDP)	0002	2
6	Remote Device - High 16 bits of IP Address	C0A8	49320
7	Remote Device - Low 16 bits of IP Address	B101	45313
8	Unused (Set to 0)	0000	0
9	TCP/UDP Port Number	05E1	1505
10-15	Unused (Set to 0)	0000	0

Word Transfer Command Block

The following command block writes 25 words obtained from the local PLC V memory starting at V100 to a block of V memory starting at V200 in the remote PLC. The target IP address and port is specified in the command, allowing it to be changed to point to a different PLC in subsequent execution.

Offset	Description	Hex	Decimal
0	Error Word	0000	0
1	Command Code (Write)	0201	513
2	Connection Number (19221 - 19228)	4B15	19221
3	Source: Starting V Memory Address in this PLC	0064	100
4	Number of Words to Transfer (1-256)	0019	25
5	Destination: Starting V Memory Address in Remote PLC	00C8	200
6	Command Timeout in seconds (0 = Use Default)	0000	0
7 - 9	Unused (Set to 0)	0000	0
10	IP Address of Remote Device - High 16 bits (UDP Only: IP Address Location bit in the Create Socket command must be set to 1)	C0A8	49320
11	IP Address of Remote Device - Low 16 bits (UDP Only: IP Address Location bit in the Create Socket command must be set to 1)	B103	45315
12	UDP Port Number of Remote Device (UDP Only: IP Address Location bit must be set to 1)	05E1	1505
13 - 15	Unused (Set to 0)	0000	0

If you need to verify that the command was completed successfully, you can monitor the error status. If a problem occurs while executing the command, the 2572-A will set the CMD ERR bit and place the applicable error code in the Error Word. See *Appendix D* for additional information.

Multicast Client Example

This example creates a Multicast Socket which can be used to send data to multiple PLCs concurrently. The Unacknowledged Write command block is used to send the multicast data.

> *NOTE:*
> *The 2572-A modules in the PLCs that will participate in the multicast session must be configured to receive on the same multicast address as the client using to send data.*

Create Socket Command Block

This command block creates a Multicast socket that will send to multicast address 225.1.1.1. (0xE1010101).

Offset	Description	Hex	Decimal
0	Error Word	0000	0
1	Command Code (Create Socket)	0003	03
2	Connection Number (19221 - 19228)	4B15	19221
3	Protocol Manager Number	0024	36
4	Startup Option Bits	0000	0
5	Type of Service (1 = TCP, 2 = UDP/Multicast))	0002	2
6	Remote Device or Multicast IP Address- High 16 bits	E101	57601
7	Remote Device or Multicast IP Address - Low 16 bits	0101	257
8	Unused (Set to 0)	0000	0
9	TCP/UDP Port Number	05E1	1505
10-15	Unused (Set to 0)	0000	0

Word Transfer Command Block

The following command block writes 25 words obtained from local PLC V memory starting at V100 to the a block of V memory starting at V200 in all PLCs that have a 2572-A module listening at IP multicast address 225.1.1.1. The Unacknowledged Write command is used to prevent multiple replies.

Offset	Description	Hex	Decimal
0	Error Word	0000	0
1	Command Code (Write)	0204	516
2	Connection Number (19221 - 19228)	4B15	19221
3	Source: Starting V Memory Address in this PLC	0064	100
4	Number of Words to Transfer (1-256)	0019	25
5	Destination: Starting V Memory Address in Remote PLC	00C8	200
6-9	Unused (Set to 0)	0000	0
10-12	Not used in this example	0000	0
13	Minimum Production Interval in milliseconds. (0= Default Value = 1000ms)	05DC	1500
14-15	Unused (Set to 0)	0000	0

In this example, the minimum production interval is set to 1500ms (1.5 second). To use the timer effectively, you should use uncoupled mode and leave the trigger bit set .

Since the command is not acknowledged, you cannot directly verify that the data was actually written to the remote PLCs by monitoring the error status. Since most multicast applications will send the same data periodically, lack of verification may be less important. If you wish to verify that data is

written you must use TCP or UDP unicast addresses, as illustrated in the previous examples, or you may program the remote PLCs to send verification messages.

PLC Ladder Logic Example

The following pages contain a sample of a PLC ladder logic application that implements the 2572-A Client Mode. Client Mode allows the PLC to send a message containing commands and/or data from the local PLC to another network node via TCP/IP. It is typically used to send unsolicited alarm messages or production data based on an event detected by the PLC. Potential message recipients include network computers or other PLCs using a 2572.

This sample application executes a START NETWORK SERVER command to set the module IP address and other network parameters. Once this command is completed successfully, the application establishes a socket to communicate with another network device using the CREATE SOCKET command.

The example command block is for UDP; however, it can be easily modified to create a TCP connection by changing one parameter in the command block. Once the CREATE SOCKET command has completed successfully, the logic will continuously execute a memory transfer command (read remote) as long as an event represented by C100 is present. Error recovery logic includes simple command logging and retry and TCP re-connection attempts.

Obviously, there is no single "right" way to accomplish this application. This example is not necessarily the most elegant or efficient alternative, but it is known to work. The logic includes error detection, logging, and recovery.

In this example, the module is assumed to be logged in starting at WX1. Thus, WX2 will contain the command status bits, WY4 will contain the command control bits, and WY5 - WY 8 will contain Command Slots 1 - 4. If your configuration is different, you will need to change the sample logic to match your configuration.

This example uses Command Slot 1 (WY5) for all commands. WY5 will contain the V memory address of Command Block being used. The state of the logic (e.g. which control relay is set) will determine which address is loaded into WY5.

The Command Blocks are assumed to be already stored in V memory. You may enter them in directly using PLC programming software, use PLC logic to copy them from K memory, or create them directly in ladder logic using the load constant box. The example uses the following Command Blocks:

Start Network Server .... located at V100
Create Socket .... located at V120
Memory Transfer .... located at V140.

A single rung of ladder logic is used to set the trigger for all commands for the single command slot. The trigger uses the coupled mode, which enforces "handshaking" between the 2572-A and the PLC. See APPENDIX C. PLC COMMAND INTERFACE for a detailed discussion of the command mode.

Note the function of C14 and C15. They are used to detect the fact that a 2572-A command cycle has completed. Refer to the timing diagram below. The 2572-A will raise the Command Busy it after the PLC logic sets the command trigger. If there is no error, the 2572-A will lower command busy after the PLC lowers the command trigger and the 2572-A module has successfully completed the command. If there is an error, the 2572-A will raise the error bit. In this case, it will not lower the command busy bit until the PLC sets the error acknowledge bit. When the command busy bit is lowered, the command cycle is complete and the 2572-A can accept another command in the command slot.

C14 is set here when Command Busy bit comes on

C15 is set here when Command Busy bit goes off, after C14 is on, indicating a complete command cycle

On

Command Busy Bit

Command Error Bit

Time
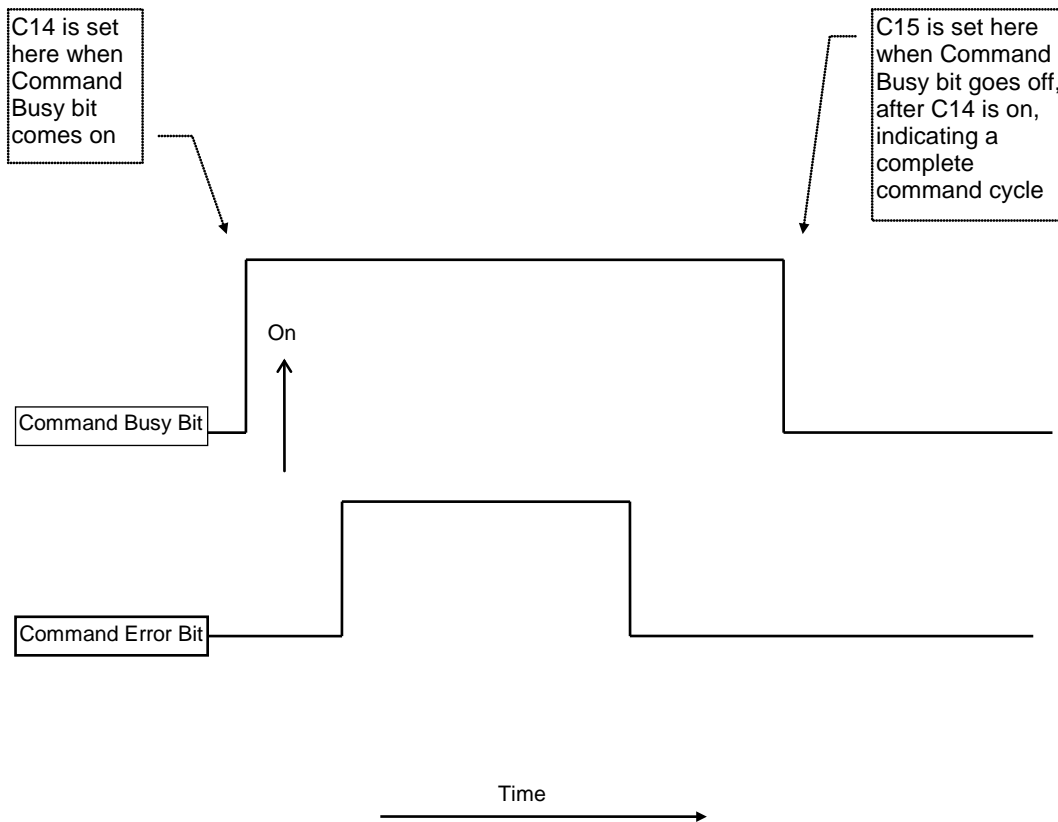
Please refer to APPENDIX C. PLC COMMAND INTERFACE for detailed information regarding the timing of the trigger, command busy and command error bits. C14 is used to latch the beginning of a command cycle. When the command busy bit is lowered after C14 has been set, C15 is set. When C15 is set, the command cycle has been completed.

Error recovery is a required component of any application utilizing network communications. The example error recovery is simple, but typical of what you might do.

When executing the Start Network Server command, any error usually indicates an invalid command block. The error must be manually corrected. Therefore, any errors that occur while attempting this command are not logged nor is the error word cleared.

When performing other commands (such as memory transfer), you may encounter errors that are caused by the network or the remote device with which you are attempting to communicate. For example, the remote device may go off-line. In most cases, the practical error recovery is to log the error and retry.

This example simply copies the last error to a V memory location and retries the command. The retry will repeat until the command is successful. You may wish to modify the error logic to count the number of errors/retries and to set an alarm when an error persists. You might also choose to store a set of most recent errors in a table.

Rung 5 contains error recovery specific to TCP. If the connection to the remote device is lost (due to network or remote device problems), the logic must re-establish the connection. This is accomplished by comparing the command error word of the Memory Transfer command to the value of 166. This is the error code that would be returned if the TCP connection were lost. When the command error word is equal to 166, the logic will attempt to establish the connection again.

The logic recognizes three states:

1. The Network Server application has not been started (thus the IP address has not been set) and WX1.3 is on. C1 is on; C12 and C13 are off.

2. The Network Server is active but a client network connection has not been established. Control relay C12 is turned on in this state; C1 and C13 are off.

3. The network connection has been successfully established and data transfer can commence. Control relay C13 is on in this state; C1 and C12 are off.

> *NOTE:*
> *This example assumes you are starting the network server (and setting the IP address) using PLC logic. If you choose to automatically start the network server using network parameters in EEPROM, your logic will never "see" WX1.3 come on. Therefore, you will need to modify the logic accordingly. See the 2572-A Installation and Operation Guide for information on startup methods.*

Client Ladder Logic Example: Part 1

```
  WX1.3    C2              ┌──────────┐              C1
  ──┤├──────┤/├────────────│   LDC    │──────────────( SET )
   │                       │  A: WY5  │              C12
   │                       │  N = 100 │              ─( RST )
   │                       └──────────┘              C13
   │                                                 ─( RST )
   │                                                 C14
   │                                                 ─( RST )
   │                                                 C15
   │                                                 ─( RST )
   │                                                 C19
   │                                                 ─( SET )
   │
   │ WX1.3                                           C2
   │──┤├────────────────────────────────────────────(   )
   │
   │ WX2.3                                           C14
   │──┤├────────────────────────────────────────────( SET )
   │                                                 C15
   │                                                 ─( RST )
   │
   │ C14      WX2.3                                  C15
   │──┤├───────┤/├───────────────────────────────────( SET )
   │                                                 C14
   │                                                 ─( RST )
```

Rung 1 - If the Net Cfg bit (WX1.3) is on and C2 is not on, then load Command Slot 1 (WY5) with the V memory address of the Start Network Server command block (V100). Set C1 to indicate that Network Server has not been started, reset the control relays used to indicate logic state, and set the command trigger (C19).

Rung 2 - When WX1.3 is on, turn on C2. This will keep the rung above from executing on subsequent scans while WX1.3 is high. This eliminates double triggering.

Rung 3 - Captures the fact that Command Busy (WX2.3) went high by setting C14. C15 is reset. This indicates we have started a command cycle.

Rung 4 - - C15 captures the fact that Command Busy (WX2.3) went low after C14 was set. This indicates that a command cycle has been completed. This rung also resets C14.

Client Ladder Logic Example: Part 2

```
   C1     C15        ┌─────────┐                              C12
───┤├─────┤├─────────┤  LDC    ├──────────────────────────────( SET )
                     │  A: WY5 │                               C1
 V140 + 166          │  N = 120│                              ─( RST )
──┤ = INT ┤──────────└─────────┘                               C15
                                                              ─( RST )
                                                               C19
                                                              ─( SET )


   C12    C15        ┌─────────┐                              C13
───┤├─────┤├─────────┤  LDC    ├──────────────────────────────( SET )
                     │  A: WY5 │                               C12
                     │  N = 140│                              ─( RST )
                     └─────────┘                               C15
                                                              ─( RST )


  C100    C13                                                  C19
───┤├─────┤├──────────────────────────────────────────────────( SET )
```

Rung 5 - If the command completed successfully while C1 is on, this means the Network server is started. Sets C12 and resets C1 to indicate new state. Loads command slot 1 (WY5) with the address of the Create Socket command block. Resets C15 to start a new command cycle and sets the trigger bit (C19) to execute the new command.

If the TCP Connection is lost, as indicated by error code 166 in V140, the Create Socket command will be re-triggered to attempt to create the connection again.

Rung 6 - If the command completed successfully while C12 is on, this means the Create Socket command completed successfully. Sets C13 and resets C12 to indicate new state. Loads command slot 1 (WY5) with the address of the Memory Transfer command block. Resets C15 to start a new command cycle.

Rung 7- This sets the trigger after you have successfully completed the Create Socket command (C13 is on) and C100 is on. C100 represents the event which would cause you to execute the memory transfer.

Client Ladder Logic Example: Part 3

```
   C19    WX2.3                                         WY4.2
 ──┤├──────┤/├──────┌─────────┐ ┌─────────┐─────────────( )──
                    │  LDC    │ │  LDC    │              WY4.3
   WY4.3            │ A: V120 │ │ A: V140 │             ──( )──
 ──┤├──             │  N = 0  │ │  N = 0  │
                    └─────────┘ └─────────┘               C19
                                                        ─(RST)─

   WX2.1   C12     ┌─────────┐                           C18
 ──┤├──────┤├──────│  MOVW   │─────────────────────────( )──
                   │ A: V120 │
                   │ B: V400 │
                   │  N = 1  │
                   └─────────┘

   WX2.1   C13     ┌─────────┐                           C18
 ──┤├──────┤├──────│  MOVW   │─────────────────────────( )──
                   │ A: V140 │
                   │ B: V401 │
                   │  N = 1  │
                   └─────────┘

   WX2.1                                                WY4.1
 ──┤├────────────────────────────────────────────────( )──
```

Rung 8 - This is the command trigger for Command Slot 1. When C19 is set and Command Busy(WX2.3) is low, the Command Mode (WY4.2) and Command Trigger (WY.4.3) bits are turned on . These are held high by WY4.3 until command busy goes high. C19 is reset and must be explicitly set again before another command will execute. The LDC boxes clear the error words.

Rung 9 - If an error occurs while attempting to Create a Network Connection (C12 on), this stores the error word in V400.

Rung 10 - If an error occurs while attempting the memory transfer command (C13 on), this stores the error word in V400.

Rung 11 - When the command error bit is on, raise the error acknowledge bit. This will cause the module to clear the error and lower command busy.

CHAPTER 6. MODBUS TCP SERVER

6.1. Configuration

The Modbus TCP server starts automatically using TCP Port 502 . There is no configuration or startup logic required.

6.2. Variable Mapping

Modbus TCP uses a different nomenclature than the SIMATIC® 505 to describe data elements. The following table provides a cross reference.

Modbus Variable	505 PLC Equivalent Variable
Coil	Control Relay (C)
(Discrete) Input	Discrete Input (X)
Holding Register	User Variable Memory (V)
Input Register	Word Input (WX)

Modbus data elements are referenced to 0, while 505 data elements are referenced to 1. Thus, the first Modbus Holding Register is Register 0, while the first 505 V memory location is V1.

> *NOTE:*
> *Some Modbus TCP client software may start with holding register 0. To be sure how your client will work, you should test your application.*

6.3. Supported Modbus Function Codes (FC)

The following Function Codes are supported by the Modbus/TCP Server function.

FC (dec)	FC (hex)	Function Codes	505 Variable	Comments
01	01	Read Coil Status	C	Max number of coils = 2000
02	02	Read Input Status	X	Max number of inputs = 2000
03	03	Read Holding Register	V	Max = 125
04	04	Read Input Register	WX	Max = 125
05	05	Write Single Coil	C	
06	06	Write Single Register	V	
07	07	Read Exception Status	C	TBD. This returns Y1-8 or C1-8 in 2573-MOD.
15	0F	Write Multiple Coils	C	Max = 800
16	10	Write Multiple Registers	V	Max = 100

6.4. Modbus Exception Codes

The following Modbus Exception codes may be returned to the Modbus Client in case of an error.

Code	Name	Description
01	Illegal Function	Unsupported Function code
02	Illegal Data Address	Requested data address not included in the PLC configuration
03	Illegal Data Value	Typically indicates a problem in the query structure
04	Slave Device Failure	Unrecoverable error occurred while processing the request

6.5. Diagnostic Statistics

A full set of diagnostic statistics is maintained for the Modbus/TCP server. These may be accessed by a web browser by setting the URL to the IP address of the module. From the main menu page, select Module Diagnostics and the Modbus/TCP Server.

CHAPTER 7. Ethernet/IP Server

7.1. Overview

Firmware versions 2.00 and above provide support for Ethernet/IP server functions. Using Ethernet/IP, controllers such as the Allen Bradley Control Logix can read data from and write data to 505 PLCs.

General Description

The 2572-A Ethernet I/P (EIP) server allows an EIP client to access data in a SIMATIC® 545 or 555 PLC. The EIP Server supports reading data from V memory using a CIP DATA TABLE READ message and writing data to V memory using a CIP DATA TABLE WRITE message. V memory values can be accessed as 16 bit unsigned integers, 16 bit signed integers, 32 bit signed integers, or 32 bit floating point numbers.

V Memory Concepts

Variable (V) memory consists of a block of 16 bit registers. The interpretation of the V memory register contents depends on the application accessing the register. V memory registers can be interpreted as a field of 16 bits, an unsigned 16 bit decimal number, a signed 16 bit decimal number, or a set of ASCII characters.

In addition, two consecutive registers can be combined and interpreted as a 32 bit number (signed integer or floating point number). For example, if you were writing a block of 2 floating point numbers to V memory starting with V memory 100, the registers would contain the following data.

V Memory Address	Data
100	Floating Point Number 1
101	
102	Floating Point Number 2
103	

Tag Names

Tag Names are used to specify the type of memory to be accessed, the format of the data, and the memory locations where the data is stored. A Tag Name consists of a Tag Type and a numeric address. The Tag Type specifies the PLC data element type (e.g. V memory) and the data format. The numeric address specifies the address of the first data register to be accessed.

For example, the Tag Type VS would be used to access one or more V memory locations as 16 bit signed integer values. The complete Tag Name VS100 would be used to access V memory address 100 as a signed integer value.

7.2. Tag Types Supported

The following table lists the Tag Types supported by the 2572-A EIP server.

Tag Type	Description	Tag Name Example
VS	V Signed: Accesses a V memory register as a 16 bit signed integer	VS2
VU	V Unsigned: Accesses a V memory register as a 16 bit unsigned integer. *NOTE: The Control Logix processor does not support 16 bit unsigned integer as a data type. (See VE Tag Type below)*	VU335
VF	V Float: Accesses a pair of V memory registers as a 32 bit floating point number	VF650
VL	V Long: Accesses a pair of V memory registers as a 32 bit signed integer	VL50
VE	V Extended: Converts between a V memory 16 bit unsigned integer and a 32 bit signed integer CIP data element. *NOTE: This Tag Type is specifically for controllers that do not support 16 bit unsigned integers See the following section for more information.*	VE1000

Figure 10. V memory Tag Types

V Extended (VE)

VE is a special Tag Type created for controllers that do not support the 16 bit unsigned integer data type. For Data Table Read operations, it converts unsigned integers stored in a V memory register to a 32 bit signed integers that can be read by the client controller. For Data Table Write operations, it converts one or more 32 bit signed integers sent by the client to a 16 bit unsigned integers, each stored in a single V memory location.

The following restrictions are placed on data written to V memory using this Tag Type:
1. The value must be a positive number or 0.
2. The maximum value is 65,535 (0xFFFF).

Values that do not meet these requirements will be rejected by the 2572-A EIP server.

7.3. 2572-A Configuration

The EIP Server starts automatically when the module is started up. No additional configuration is required.

7.4. Application Example

The following example illustrate how to configure a Control Logix system to communicate with the 2572-A. The example reads unsigned integers stored in V memory and writes a block of signed integers to V memory.

The following steps are required to configure the Control Logix system:

1. Define Control Logix tag names that you want to use to hold the data you will read from the 505 PLC and data you will write to the 505 PLC. For accessing multiple V memory locations, you will need to dimension the tag as an array.

2. Create Message Blocks in your Control Logix program.

3. Configure each Message Block by selecting the following:
   - Message Type: CIP Data Table Read or CIP Data Table Write
   - Source Element: For a read operation, this is the 505 Tag Name. For a Write operation this is the Control Logix Tag Name.
   - Number of Elements: Select the number of data elements to read or write
   - Destination Element: For a read operation, this is the Control Logix Tag Name. For a write operation, this is the 505 Tag Name.

4. Specify the Communication options for each Message Block. This includes the path to the target 2572-A module.

Defining the Control Logix Data Tags

First, we will need to define some Control Logix tags. We will define two tags, one to hold the data read from the 505 PLC and the other for the data we will write to the 505 PLC. Different formats are used for the read and the write operations to illustrate the difference in accessing signed and unsigned V memory data.

P	Tag Name	Alias For	Base Tag	Type	Style	Description
	⊞-Local:1:C			AB:1756_DO_DC...		
	⊞-Local:1:I			AB:1756_DO_DC...		
	⊞-Local:1:O			AB:1756_DO:O:0		
	⊞-Message_1			MESSAGE		
	⊞-Message_2			MESSAGE		
▶ □	⊞-myarray			DINT[4,4,4]	Decimal	
	mytag	VMEMWRITE[0].2	VMEMWRITE[0].2	BOOL	Decimal	
□	⊞-VMEMREAD			DINT[100]	Decimal	Data Read from 505 PLC
	⊞-VMEMWRITE			INT[50]	Decimal	Data Written to 505 PLC
* □						

Scope: test_CTI(controller) Show: Show All Sort: Tag Name

The tag named VMEMREAD will be used to store the data read from the 505 PLC. The tag data type is defined as a 32 bit signed integer. This is done because we want to read unsigned integers from the PLC, whose values may exceed the maximum that can be stored in a 16 bit signed integer (+32,767). *Note that the Control Logix processor does not support unsigned integer tags*. This tag is dimensioned to hold 100 values.

The tag named VMEMWRITE will be used to store the data that will be written to the 505 PLC. Since we are writing signed 16 bit integers to the 505 PLC, this tag type is defined as a signed 16 bit integer. This tag is dimensioned to hold 50 values.

Adding Message Blocks to the Logic

There are two message blocks added to the logic. One block is used to read the data and one to write the data. The following sections will illustrate how to configure these blocks.
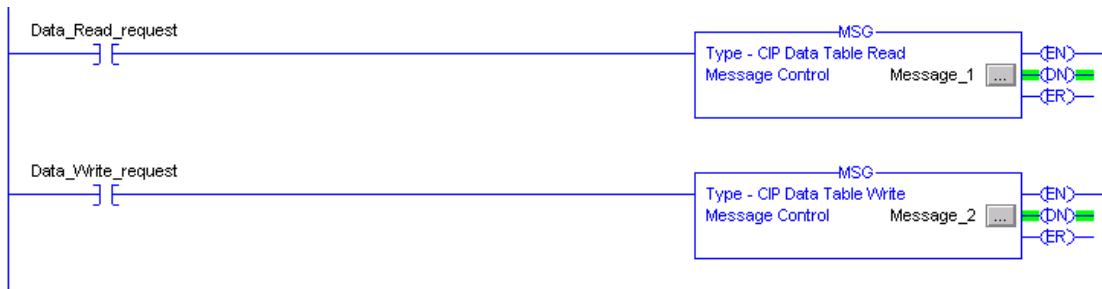
> **NOTE:**
> *Your logic should use a timer (or similar means) to initiate the message block. Allowing the message to execute every scan could create excessive loading on the 2572-A modules.*

Configuring the Read Message Block

This message will read 100 unsigned integers from V memory starting at V501. Clicking on the ellipsis button will display the configuration dialog box.

Configuration Tab

The configuration tab is used to define the message contents.
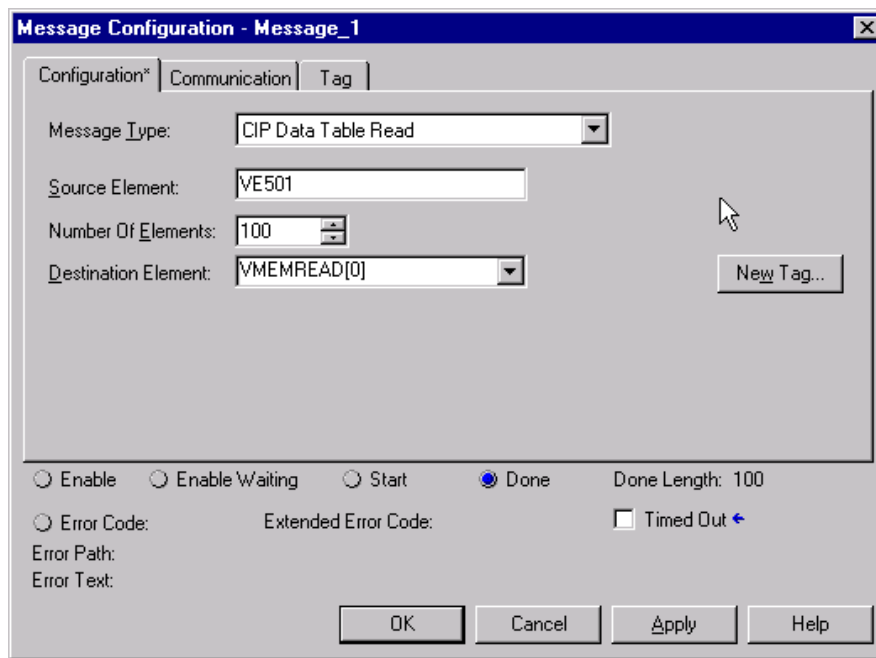
The SOURCE ELEMENT specifies the 505 PLC Tag Name. We want to read a 16 bit unsigned integer into a 32 bit signed Control Logix tag, so we will use the tag type VE. Since we want to start reading at V memory location 501, the complete Tag Name is VE501.

We want to read a block of 100 registers, so the NUMBER OF ELEMENTS will be set to 100.

The DESTINATION ELEMENT specifies the Control Logix tag that will store the results of the read message. This is the tag we defined earlier. Since this is an array, we will specify that first value returned will be stored in array element 0. Additional values will be stored in subsequent array elements.

Communication Tab

The Communication Tab is used to specify the message routing and destination IP address.
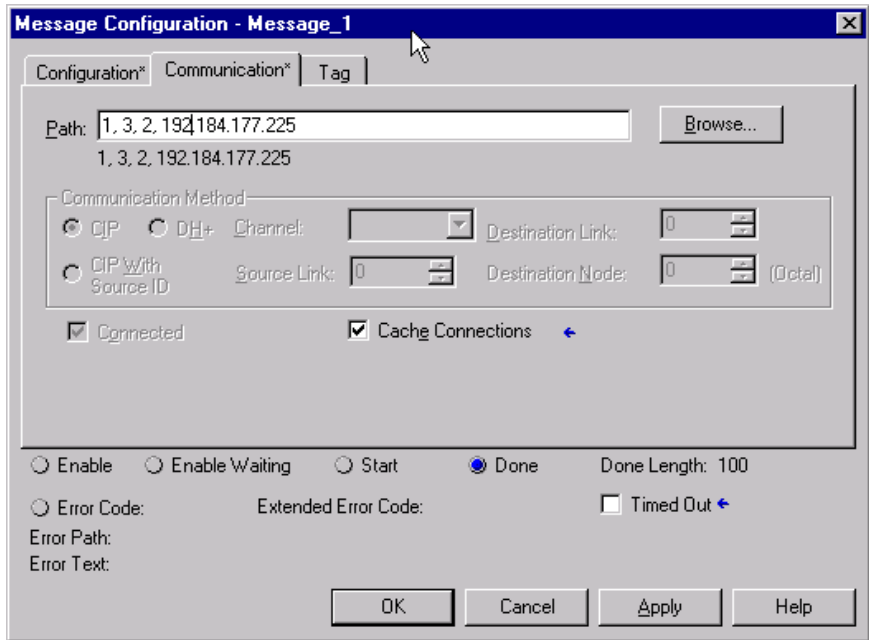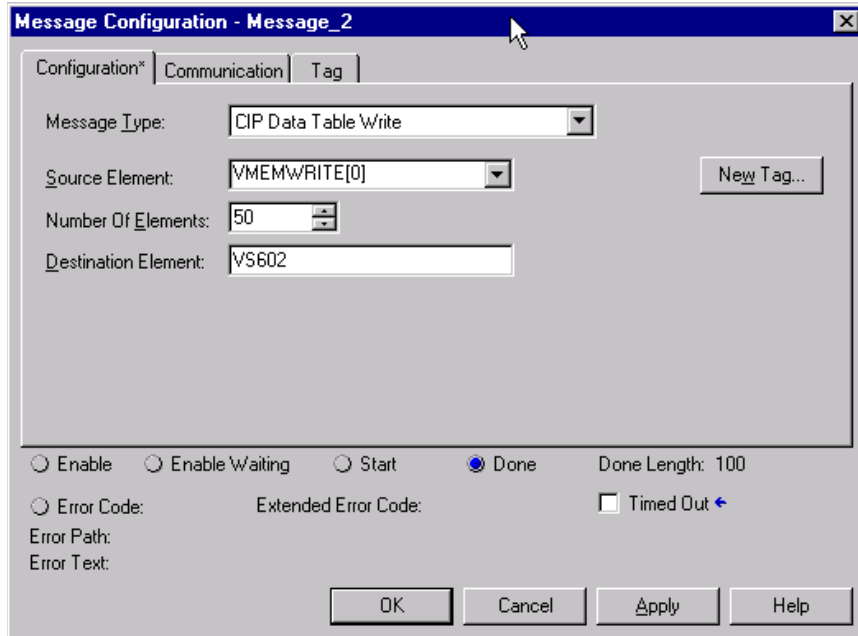
The path specifies the route from the controller to the destination. In this case, we will send the message to the backplane (1), to the Ethernet module located in slot 3, out the Ethernet port (2), to the 2572-A module whose IP address is 192.184.177.225.

The CACHE CONNECTIONS box is checked to keep the TCP connection established after the message is completed. If you don't check this box, the Control Logix will close the TCP connection after each message transaction is complete. Continually opening and closing the TCP connection adds unnecessary overhead and reduces performance.

Configuring the Write Message Block

Configuration Tab

The SOURCE ELEMENT specifies the Control Logix tag that will contain the data to be written to the 505 PLC. We defined this tag in the first section. Since this is an array, we will specify that first value to be written is array element 0. Subsequent elements will be written up to the value specified in the Number of Elements box.

Since we want to write a block of 50 registers, the NUMBER OF ELEMENTS will be set to 50.

The DESTINATION ELEMENT specifies the 505 PLC Tag Name. We want to write 16 bit unsigned integers, so we will use the tag type VS. Since we want to start reading at V memory location 601, the complete Tag Name is VS601.

Communication Tab

The communication tab defines the path to the target 2572-A. See the dialog box for Message -1 above.

CHAPTER 8. TROUBLESHOOTING

This section provides information that you may find useful in diagnosing and correcting problems you may encounter with using the 2572-A module.

8.1. Troubleshooting Aids

There are several troubleshooting aids that may be used to determine the cause of problems. They include:

LED Indicators
The module LEDs provide a visual indication of the status of the module components. APPENDIX A. 2572-A LED INDICATORS provides a complete description of the LED usage.

Event Log
The Event Log is a new diagnostic facility provided by the CTI 2572-A module. It is a collection of entries, created by the module software, that document significant or unusual module events. The log is maintained in non-volatile (battery backed) RAM within the module, so that the records are preserved when power is removed. Each log event includes a timestamp, a text description, and various codes that may be useful to CTI support personnel. The most recent event is listed first and the least recent event is listed last.

> *NOTE*
> *The timestamp is based on the module time of day clock, which is set to the PLC time of day clock, each time the module starts up. If the PLC clock is inaccurate, the event log timestamp will be also.*

The Event Log is the one of the primary troubleshooting tools provided by the module. It is especially useful in diagnosing problems during startup, program download, and other similar activities. When the TCP/IP interface is operational, the event log may be accessed using a standard web browser.

Point your browser to the main 2572-A Menu page by entering http://xxx.xxx.xxx.xxx, where xxx represents the current IP address of the module. For example, http:/192.168.177.55 would point to the web page of the 2572A module with IP address 192.168.177.55. From the main menu, select the Diagnostic Menu, then the Event Log link.

SYSLOG Facilities
Event log messages may be directed to a PC running a SYSLOG server. This provides a means to store the Event Log messages on a hard disk drive for subsequent analysis. SYSLOG server software is available from network software providers, often for a nominal charge.

The SYSLOG facility can be enabled via the Module Configuration web page. See the following illustration.

Event Log

Event Log Size	100	Records
SYSLOG Server IP Address	0 . 0 . 0 . 0	
SYSLOG Server Port	0	(default 514)
SYSLOG Enable	☐	

[Update Module]　　[Restore Initial Values]

Module Diagnostic Objects

The module maintains a set of diagnostic objects, which provide information about the various module facilities. The information includes current operating status and counts of various module activities. The diagnostic objects may be especially useful in diagnosing problems with network performance, PLC access, and similar activities. The diagnostic objects are accessible using a standard web browser.

Other Troubleshooting Tools

CTIDiag

CTI provides a software program (CTIDiag) that can be used to perform some diagnostic activities. Although many of the 2572 based functions of CTIDiag are no longer supported by the 2572-A, it can be used for such functions as setting the module IP address via the serial port and for generating CAMP message traffic to test the 2572-A server. CTIDiag may be downloaded from the CTI web site (www.controltechnology.com).

Network Analysis Software

Network analysis software captures Ethernet traffic on a network segment. Once the packets have been captured, the software decodes the packet information, allowing you to observe the packet content. In addition, since the packets include a timestamp, you can determine the rate at which packets are arriving. The network analysis software is especially useful in diagnosing situations where communications cannot be established or performance is degraded.

8.2. General Troubleshooting Techniques

If you are experiencing problems with using the 2572-A, you should note the general category of the problem you are encountering:

- The module has not started up properly. If the Module Status LED is not Steady Green or the Network Status LED is Off or Steady Red, a problem has been encountered during startup.
- The module is operational, but is not communicating with a client application.
- The module is communicating with a client application but performance is substandard.
- The PLC is unable to initiate a client connection to another CTI Ethernet module (2572- A or 2572 module).

8.3. Module Startup Problems

Before the module can communicate with other TCP/IP hosts, it must complete startup operations. If the MS LED Steady Green and the NS LED is Steady Green, the module has successfully completed startup. Otherwise, a problem has been encountered during module startup. See the table below to determine that cause of the problem.

SYMPTOM	PROBABLE CAUSE	CORRECTIVE ACTION
No LEDs are illuminated.	No Power to Module.	Ensure that power is supplied to the rack and that the module is securely inserted.
	Defective Module.	Cycle the power. If the problem persists, contact CTI.
The module does not execute the Lamp Check Sequence.	The bootloader software did not start. It may be corrupted.	Reset the module. If the problem persists, contact CTI.
MS LED is Steady Red. NS LED is flashing Red.	The module application firmware is corrupted. The module was unable to download new firmware because the information needed to download the firmware cannot be obtained from EEPROM.	Start the module using DHCP after configuring DCHP to provide the boot file and TFTP server path. See APPENDIX E. USING DHCP for details on configuring a DHCP server. Once this is done, the module will automatically download new application firmware.
MS LED is Steady Red. NS LED is Steady Red.	The module application software is missing or corrupted. The module was unable to download new software because of one of the following conditions: 1) the TFTP server could not be contacted, 2) A valid software file could not be found, 3) An unrecoverable error was during file download.	Reset the module to retry the operation. Observe the transient states of the NS LED. If NS LED does not become solid green at some time (indicating that a file download is in progress), then server or file cannot be located. Ensure the following: - Module is connected to the network. - The TFTP server is present and can be accessed via the network (try pinging the server IP address). - The software files are installed in the correct directory on the TFTP server. Else, ensure that all required files are in the correct directory. If files are missing, replace all of the files. Also, check the network and server loading. It is possible that heavy loading can cause a timeout error while downloading files.
MS is Steady Red, NS is Off	The module application software is corrupted. A new program was successfully downloaded but could not be written to flash.	Reset the module to retry the operation. If this problem persists, contact CTI.
MS is Flashing Red NS is Steady Red	Unable to read the Ethernet MAC ID from EEPROM.	Reset the module to retry the operation. If the problem persists, contact CTI.

SYMPTOM	PROBABLE CAUSE	CORRECTIVE ACTION
MS is Flashing Red NS is Flashing Red	Unable to obtain the IP parameters from EEPROM.	Use CTIDiag to manually enter the IP parameters via the serial port and reset the module. OR configure a DHCP server with the required IP information (see APPENDIX E. USING DHCP) and set the Module ID switches to the appropriate setting. Then reset the module. OR Set the module startup switch to the PLC Start position and use the PLC interface to set the IP parameters (see *Section 4.2. Start Network Server Command Block)*
MS LED is Steady Green, NS LED is Off	The module is waiting on the PLC to start the network server.	Ensure the PLC is in run mode and that the 2572-A is properly entered in the PLC I/O configuration. Check the PLC logic. See *Section 8.7. PLC Logic Problems.*

8.4. Communications Problems

If the module operational (properly started up) but it will not respond to network clients, refer to the table below for help in diagnosing the cause.

Symptom	Probable Cause	Corrective Action
The Link Status (LS) LED is Off	Cable between the module and Ethernet hub/switch is not connected.	Plug the opposite cable end into the hub or switch.
	The cable is faulty or the RJ45 connector is improperly wired.	Test cable and replace if faulty. OR Substitute a cable known to be good.
	Defective Ethernet Hub or Switch	Ensure power is applied to the hub/switch. Determine whether other devices are using the hub/switch successfully.
The Link Status (LS) LED is on. Ethernet Receive (RCV) LED does not flash.	There is no traffic on the network segment. If you are attempting to access the module via the network, you should observe the Ethernet RCV LED flash intermittently. NOTE: On most active networks, you will see some traffic on the local segment, even though that traffic is not directed to the module.	Ensure that the Ethernet hub/switch is connected to the network. Using a PC attached to the local network, send a PING to the module IP address. If you observe the Ethernet RCV LED flash, the physical connection is OK.
	If you are using a switch, the switch may be blocking the port for the particular IP address. NOTE: This can occur when you change the port to which the module is connected.	Cycle power to the switch, if possible. OR Wait for up to 5 minutes, for the port to dynamically reassign the port.
Attempt to PING the module using a PC attached to the local network is unsuccessful. Physical network connections are OK.	The IP Address/Subnet Mask of the client PC does not match the local network. NOTE: This might occur is you are using a laptop normally used for other purposes.	Observe the reply to the PING. If you receive a reply such as "Network Unreachable" , the PC IP address does not match. Determine the IP setting of the PC by typing IPCONFIG in the Command Prompt window. Ensure that both the IP address and Subnet Mask are correct.
	The module IP address/Subnet Mask is improperly set.	Using the CTIDiag program, connect to the module serial port and open a serial port connection. Using the "Set Network Parameters" command, read the IP address from the module EEPROM. Then see following troubleshooting activities

Symptom	Probable Cause	Corrective Action
Module IP address is improperly set. Using PLC startup option.	Incorrect data has been entered in the Start Network Server command block.	Review the command block entries. Ensure that the conversion to hexadecimal is correct. Correct entry and reset the module.
Module IP address is improperly set. Using EEPROM startup option.	Incorrect data is stored in EEPROM.	Ensure that the module startup switch is set to the AutoStart position and that the Module ID switches are set to 00.
		Using the CTIDiag program, connect to the module serial port and open a serial port connection. Using the "Set Network Parameters" command, change the IP parameters to the correct values and reset the module.
Module IP address is improperly set. Using DHCP startup option	The Module ID switches are set to the incorrect value.	Ensure that the module startup switch is set to AutoStart and that the Module ID switches are set to the correct value. Make corrections, if necessary, and reset the module.
	The DHCP server is unavailable, IP data is being obtained from EEPROM, which contains the wrong value. NOTE: If backup IP parameters are being used, the NS LED will briefly alternate between Green and Red.	Using CTIDiag, set the IP parameters stored in EEPROM to the correct value. *NOTE: You can verify that this works by temporarily setting the Module ID switches to 00 and resetting the module. Be sure to set them back to the correct value before conducting the next test.* Next, reset the module and use CTIDiag to read the EEPROM again. If the values have not been changed, the DHCP server is not available.
You are able to Ping the module, but the client cannot access the PLC data. Module is installed in a remote rack using a Profibus RBC	2572-A will not function on a Profibus network.	Use Remote I/O network or install in a local rack.
Able to communicate with the 2572-A module on the local network but unable to communicate with the module from a remote network.	Default router not set in 2572-A module	Check the default router IP address and change, if required.
	Firewall is blocking the message.	Contact your network administrator.

8.5. Performance Problems

Symptom	Probable Cause	Corrective Action
Performance is sub-standard at all times.	The module is not getting enough access to the PLC.	Ensure that the number of task codes per scan is set as high as possible (preferably eight). Ensure the module is installed in a local base. Throughput will be degraded in a remote base.
	The network traffic is excessive.	Observe the Collision indicator. If this flashes frequently, the network is busy. Use the module diagnostic capability to analyze the Ethernet traffic measurements. Use a network analyzer to capture network traffic. If you observe a problem you must correct the problem by reducing the traffic load, or segmenting the network using Ethernet switches/routers.
	Network broadcast traffic is excessive. Broadcast traffic consumes processor resources for every station on the network.	Use the module diagnostic facility to capture the count of broadcast traffic. Use a network analysis tool to analyze the broadcast traffic on the network. If a problem is found you must reduce the broadcast traffic by reconfiguring the offending station(s), removing the station(s), or separating them from the local area network via a router. NOTE: Using a simple switch will not reduce the broadcast traffic on an Ethernet segment since the switch sends broadcasts to every port.
	The requested data is highly fragmented in the PLC, requiring many random access transactions.	Copy fragmented data to/from contiguous V memory. This allows efficient block reads and writes.
	You have many clients accessing a single 2572-A causing an excessive transaction load.	Reduce the client poll rate or amount of data requested. Split the load among multiple modules.
	You are making heavy use of the Client function in combination with the Server function.	Don't trigger the Client command more often than required. Split the load among multiple modules.
	Module is located in a remote base. A Special Function module such as the 2572-A is considerably slower in a remote base and may increase scan time considerably.	Place the 2572-A module in a local base.

Symptom	Probable Cause	Corrective Action
Performance is substandard at times, acceptable at other times.	Something is interfering with the Ethernet network.	Observe the Collision indicator for signs of excessive collisions. Use the module diagnostic facility to analyze the Ethernet traffic and error statistics. Use a Network analysis tool to capture network traffic. If you observe a problem you must correct the source of the interference.
	A network station is transmitting an excessive number of broadcasts. Broadcast packets consume processor resources of every station on the network.	Use the module diagnostic facility to capture the count of broadcast traffic. Use a network analysis tool to analyze the broadcast traffic on the network. If a problem is found you must remove the offending station from the local network.

8.6. Serial Communications Problems

The most common sources of signal problems are bad cables or an improperly configured PC serial port. The RCV and XMT indicators can be a valuable aid in troubleshooting these errors. See the table below.

SYMPTOM	PROBABLE CAUSE	CORRECTIVE ACTION
RCV Indicator does not flash when attempting to send data from a device attached to the serial port.	No signal is being received by the 2572. This is probably due to a defective cable, although it could be due to a faulty PC port or configuration.	Check the communications cable wiring. Replace with a known good cable and retry. If failure still occurs, check your PC.
The RCV Indicator flashes but the 2572-A XMT does not flash.	No signal is being transmitted by the 2572-A on this serial port. This is typically a mismatch in the serial port parameters.	Ensure the baud rate for the PC and module are the same. Also , ensure the PC serial port is configured for Data Bits = 7 Parity = Odd Stop Bits = 1
The RCV Indicator flashes AND the 2572-A XMT light flashes, but no signal is received by the PC.	This is probably due to a defective cable. It may be a defective PC	Replace cable with one known to be good. Try an alternate PC.

8.7. PLC Logic Problems

As described previously, the Command Block located in V memory specifies the command to be executed. The Command Slots (WY5-WY8) select which Command Blocks are to be processed. The Command Control bits trigger the execution of the commands. A mistake in setting up and/or manipulating these structures will cause erroneous results. Fortunately, the 2572-A module provides extensive error reporting which should assist you in correcting logic problems. See Appendix A for a complete description and typical solutions to resolving the errors.

Following are some common errors in using the PLC interface to the 2572.

Command Block Errors

When you are first setting up the command blocks in V memory, it is easy to enter incorrect data into the command block or to omit data from the command block. Some mistakes, such as an invalid command or port number will be obvious, because the 2572-A will return an error when they occur.

Command Slot Errors

Other errors can occur if you enter the wrong V memory address for the Command Block or when you omit entering an address. If you enter a V memory address which does not contain a valid command block or enter an address of 0, the 2572-A will raise the PLC ERR bit as well as the CMD ERR bit. No error code will be written, since there is no valid location in which to write one.

> *NOTE:*
> *A command block is considered invalid if offset 2 (Connection Number) does not contain hex 4B is the high byte of the word. This signature byte places all connection numbers are in the range of 19201-19299 decimal (4B01-4B63)*

You might enter a V memory address of a *valid* command block, but it is *not* the command block you want to process. In this case, you will probably not get an error, just the wrong result.

Command Control Errors

One common error in manipulating the Command Control bits is a failure to assert ERR ACK (Error Acknowledge) after the module has raised the CMD ERR (Command Error bit). If you fail to acknowledge the error, the associated command slot will appear to "lock up" on the command slot. In actuality, the module software is waiting on the PLC acknowledgment before proceeding. You can tell that the module is not really locked up by observing the timer value in the lower byte of module WX1 increment and that you have a Command Error by examining the applicable error bit. In addition, if you have triggered other commands, they will continue to operate (unless an error also occurs on these command slots).

Another potential error is failing to observe the timing protocol for coupled mode. You must wait for the module to assert CMD Busy and then lower CMD Trigger. Failure to observe the timing may cause the command slot to appear to "lock up". Actually the module is waiting to see the PLC lower the CMD trigger. See APPENDIX C. PLC COMMAND INTERFACE for timing details.

Errors in manipulating the Command Control bits may cause "multiple triggering," resulting in an error code. Certain commands, such as those to create a connection, must be run only once. Improperly constructed PLC logic may repeatedly trigger the command, resulting in an error code such as 0x00A7 (duplicate connection).

8.8. Development and Debugging Tips

Manual Triggering

You can test your command blocks independently from the PLC logic that actually executes them by manipulating the command control bits manually. First, place the PLC in program mode so that the PLC logic will not be executing. Then you can manipulate the bits as shown below. If you are not familiar with the 2573 PLC Command Interface, you should refer to APPENDIX C. PLC COMMAND INTERFACE.

The command control bits are located in the 4th module word. For example, if you logged the module in starting at Word 1, then the command control bits will be located in WY4. See the *WX/WY Quick Reference* in *Appendix C* of this manual. There are 4 sets of control bits, one set for each command slot. Any command slot can be used in any order.

	Bits 1 -4	Bits 5 - 7	Bits 8 - 11	Bits 12 -16
WY4	Command Control Bits - Slot 1	Command Control Bits - Slot 2	Command Control Bits - Slot 3	Command Control Bits - Slot 4
	Hex 0-F	Hex 0 - F	Hex 0 - F	Hex 0 - F

Within each set of four Command Control bits:
- The first bit is the Error Acknowledge,
- The second bit is the Command Mode bit,
- The third bit is the Command Trigger,
- The fourth bit Abort Trigger.

So a bit pattern of 0110 will set the command mode bit and the command trigger. Similarly, the bit pattern 1000 will set error acknowledge. Using hexadecimal notation is a convenient way to observe and manipulate these bits, because each hexadecimal digit represents 4 bits. Thus, bit pattern when command trigger and command mode are high (0110) is represented by hexadecimal 6 (0+4+2+0). Similarly, an error acknowledge bit high (1000) is represented by hexadecimal 8.

The command status bits written by the module are located at the second module word (WX2 in this example) in a bit grouping that matches the command control word.

	Bits 1 -4	Bits 5 - 7	Bits 8 - 11	Bits 12 -16
WX2	Command Status Bits - Slot 1	Command Status Bits - Slot 2	Command Status Bits - Slot 3	Command Status Bits - Slot 4
	Hex 0-F	Hex 0 - F	Hex 0 - F	Hex 0 - F

Within each set of four Command Status bits:
- The first bit is the Command Error bit,
- The second bit is the PLC Error bit,
- The third bit is the Command Busy bit,
- The fourth bit is the Abort Busy bit.

Therefore, to set a command trigger only (uncoupled mode) for the first command slot, set WY4 to hex 2000. To set the command trigger for the second slot, set the WY4 to hex 0200. To set the error acknowledge for the third Command Slot, set WY4 to hex 0080.

When you are using PLC logic to control the PLC, it is often useful to display the module WX/WY words, parts of the command blocks, and sections of the format specifications as a chart. Following is an example chart.

```
LOCATION      STATUS       LOCATION      STATUS       LOCATION      STATUS
WX1   =       HEX          V100  =       HEX          V300  =       HEX
WX2   =       HEX          V101  =       INTEGER      V301  =       INTEGER
WY3   =       HEX          V102  =       INTEGER      V302  =       INTEGER
WY4   =       HEX          V103  =       INTEGER      V303  =       INTEGER
WY5   =       INTEGER      V104  =       INTEGER      V304  =       INTEGER
WY6   =       INTEGER
WY7   =       INTEGER      V120  =       HEX          V2000 =       INTEGER
WY8   =       INTEGER      V121  =       INTEGER      V2001 =       INTEGER
                          V122  =       INTEGER      V2002 =       INTEGER
                          V123  =       INTEGER      V2003 =       INTEGER
                          V124  =       INTEGER      V2004 =       INTEGER
                                                     V2005 =       INTEGER
```

The above chart allows you to examine at the value of the module status word (WX1), the command status word (WX2), the module control word (WY3), and the command control word (WY4) in hex. It also displays the command slots (WY5-WY8) as integers. V100, V120, and V140 are assumed to contain command blocks you are using; this display shows the first four words, including the error word in hex format. V2000 is assumed to contain data you wish to monitor. Change the display to match your setup.

To trigger a coupled mode command for command slot 1 (Assuming the module is logged at Word 1-8):

1. Enter the Command Block data in V memory.

2. Enter the address of the Command Block in WY5.

3. Change the value of WY4 to hex 6000. WX2 should change to hex 2000, indicating that the module is executing the command.

4. If WX2 changes to hex 2000, set the value of WY4 to hex 0000 (clears the trigger). If WX2 eventually transitions from hex 2000 to hex 0000, the command was executed successfully.

5. If WX2 changes to hex A000, a command error was encountered. Acknowledge the error by changing WY4 to hex 8000; then clear error acknowledge by setting WY4 to hex 0000. Inspect the command error word (Command Block - Offset 0), correct the error, and repeat the operation.

6. If WX2 changes to hex E000, you have entered an incorrect address in WY5 or you have an invalid connection number in the Command Block. Acknowledge the error as described in step 5 above and repeat the operation.

APPENDIX A. 2572-A LED INDICATORS

The 2572A LED indicators provide a visual indication of the status of the module hardware, software, network connection. The following sections describe how to interpret the various states of the LEDs.

Module Status and Network Status LED

The Module Status (MS) LED indicates the condition of the hardware and software. See the following table for general use of the LED.

State	General Condition
Steady Green (SG)	Indicates the module hardware and software are operational.
Flashing Green (FG)	Indicates the module is in a startup state. During this time, the communications facilities of the module are not operational. Assuming no startup errors are encountered, the LED should change to solid green after several seconds.
Flashing Red (FR)	Indicates that a configuration error has been detected. Typically the user must correct the configuration error and restart the module.
Solid Red (SR)	Indicates that the application software is missing or corrupted.
Alternating Green/Red (GR)	Used to indicate special conditions, such as a failed download attempt.

The Network Status (NS) LED indicates the condition of the TCP/IP network. The MS LED and NS LEDs are used together to provide more specific status information.

MS	NS	Condition	Comments
SG	SG	Module OK, Network Server Started	This is the normal operational state
SG	FG	Reserved	Currently unused
SG	FR	Reserved	Currently unused
SG	SR	Duplicate IP Address Detected. There is another network host that is using this address.	You must correct the problem by changing the module IP address or changing the address of the other network host.
SG	G/R	Unable to obtain IP parameters from a DHCP server. The module was started using the address stored in EEPROM.	This is a temporary state to alert the user to this condition when the module is first started.
SG	OFF	Module is waiting on the PLC to start the network server. Meanwhile, the TCP/IP interface is not operational.	If the condition persists, ensure that the PLC is in run mode and that the PLC logic is correct.
FG	SG	The module is downloading new software from the file server.	This is a temporary state that is set during file download.
FG	FG	The module is performing startup activities. The IP parameters have been obtained.	This is a temporary state that is set once the bootloader obtains a valid IP address.
FG	FR	Unable to download the new software file from the file server.	This is a temporary state that is set whenever an unrecoverable error is encountered downloading a file via TFTP

MS	NS	Condition	Comments
FG	SR	TFTP server/file cannot be found.	This is a temporary state that is set whenever the TFTP server cannot be located or the file cannot be found.
FG	OFF	Startup in progress – IP Parameters have not been obtained.	This is a temporary state that is displayed when the bootloader or app code is first started up.
FR	SG	Reserved	
FR	FG	Reserved	
FR	FR	Unable to obtain IP parameters. The required data was not in EEPROM.	This state will be held until the module is reset. You must correct the problem by: 1) manually updating the EEPROM using the serial port or 2) ensure that a properly configured DHCP server is available 3) Using PLC Start mode
FR	SR	Unable to read MAC ID from EEPROM	This state will be held until the module is reset. If the problem persists after several resets, contact CTI.
FR	OFF	Unable to write IP parameters to EEPROM.	This is a temporary state used to alert the user to a problem. Startup will continue even though EEPROM has not been updated.
SR	SG	Reserved	
SR	FG	Reserved	
SR	FR	Module application software is missing or invalid and the module was unable to download new application software because it was unable to obtain the necessary data to download new software.	This state will be held until the module is reset.. You may correct the problem by configuring a DHCP server to provide the necessary data.
SR	SR	Module application software is missing or invalid and the module was unable to download new software because of one of the following conditions: 1) the TFTP server could not be contacted, 2) A valid software file could not be found, 3) An unrecoverable error was during file download.	This state will be held until the module is reset. You may correct the problem by ensuring that that the TFTP file server is functioning properly at the correct IP address, and a valid software file is present in the path specified. Also make sure that the network and computer that is hosting the TFTP server is not overly busy.
SR	OFF	Module application software is missing or invalid and the module was unable to write a new program to flash.	This state will be held until the module is reset. If the problem persists after several retries contact CTI.
		Module application software is missing or invalid. Software download will be attempted.	This is a temporary state that is set when the bootloader first detects that a valid application program is not in flash.
GR	ANY	Alternating green/red – Download Failed – Using old code.	This LED condition will be cleared after the module is reset. Otherwise the module will operate normally.

Other LEDs

Label	Description	State	Status
LS	Link Status	On	Module is physically connected to an Ethernet hub or switch.
		Off	Module is not physically connected to the network.
100	Ethernet Speed	On	The Ethernet link is operating at 100Mb
		Off	The Ethernet Link is operating at 10Mb
FDX	Duplex Mode	On	The Ethernet link is operating in Full Duplex mode
		Off	The Ethernet Link is operating in Half duplex mode
XMT	Transmit	Flashing	Data is being transmitted
RCV	Receive	Flashing	Data is being received

APPENDIX B. ERROR CODES

When the 2572-A encounters an error condition, it raises the CMD ERR bit and places an error word in Offset 0 of the Command Block. Following is a list of the errors in numerical order. For compatibility, these error codes are identical to the CTI 2572 module error codes.

2572-A System Error Codes

The following error codes may be returned by the 2572-A operating system. They are almost always the result of invalid data in the command block or faulty PLC logic. All system error codes begin with hex 00.

HEX	DEC	DESCRIPTION	SOLUTION
0097	151	INVALID COMMAND The specified command number is invalid.	Correct the Command Number in the Command Block.
009E	158	ALREADY BUSY You attempted to send a command to a function that was already busy executing a previous command.	You can cause this error by using two command slots to send commands to the same connection number. Don't do this.
009F	159	INVALID CONNECTION NUMBER The specified a connection number is out of the valid range.	See the documentation for the particular command block. Correct the connection number as required.
00A5	165	INVALID SYSTEM COMMAND Connection number 19200 (system) was specified in the command block but the command is not a valid system command.	Change the logical port to a valid connection number or the command number to a valid system command.
00A6	166	CONNECTION NOT ACTIVE An attempt was made to send a command to a connection number that has not been created. Note: you could receive this error if you incorrectly entered the connection number in the memory transfer command block.	Check the following for the Create Socket Command: 1) Make sure that the command block contains the correct data, 2) Ensure that the Command Slot points to the proper command block, 3) Ensure that the Command Trigger has been set. 4) Check for reported errors for the Create Connection Command. Check the Memory Transfer command block for an incorrect connection number entry.

HEX	DEC	DESCRIPTION	SOLUTION
00A7	167	DUPLICATE CONNECTION NUMBER An attempt was made to create multiple sockets with the same connection number. or You attempted to Start the 2572-A Network Server and it was already started. or You attempted to Start the 2572-A Network Server after a previous startup error had been returned.	Ensure that all Create Socket commands for serial ports use different connection numbers. Make sure you are not triggering the Start Network Server Command more than once or that you have not already started the network server using the dipswitch AUTOSTART setting. If an error occurs when starting the network server, you must correct it and reset the module.
00A8	168	DUPLICATE CONNECTION NUMBER An attempt was made to start two protocol managers with the same connection number.	Check the Command Blocks for the respective Create Connection commands. Ensure that the Create Connection commands use different connection numbers.
00A9	169	INVALID PROTOCOL MGR NUMBER An invalid protocol manager number was specified in the Command Block.	Review the documentation and correct the command block.
00AA	170	INVALID PORT NUMBER An attempt was made to start a protocol manager with an invalid physical port number for serial ports. This can also occur when you specify an invalid serial port number for the Serial Redirect Command.	This error will occur if you enter an invalid physical port number in the command block. Valid physical port number for the 2572-A serial port is 1. Correct the command block and retry the command.
00AE	174	NETWORK NOT INITIALIZED You attempted to execute a CREATE SOCKET command before the 2572-A network server has been started.	If you are using the PLC Start option, the Start Network Server command was not executed successfully. Check for the proper execution of this command including the command block and PLC logic for this command. If you are using the AutoStart option, ensure that the network parameters are properly stored in EEPROM. You can use the CTI Diag program to examine this.
00AF	175	CONFIGURATION DISABLED WARNING The CONFIGURATION DISABLE switch is ON. You cannot write the configuration to the module.	If you want to write the configuration data, set the CONFIGURATION DISABLE switch to OFF.
00B0	176	EEPROM HARDWARE WRITE ERROR The 2572-A was unable to write data to EEPROM	Retry. If the problem persists, replace the module.
00B1	177	EEPROM HARDWARE READ ERROR The 2572-A was unable to read data from EEPROM	Retry. If the problem persists, replace the module.

General Memory Transfer Error Codes

HEX	DEC	DESCRIPTION	SOLUTION
026F	623	REMOTE MEMORY READ: WORD COUNT ERROR The remote device (PLC) responded with fewer words than requested by the Remote Memory Read command block.	This error usually occurs when the number of words requested in the command block causes the read request to exceed the memory boundary in the remote PLC. In other words, you are trying to read memory that isn't there. You should examine the Command Block and correct either the number of words requested or the starting memory location for the remote device.
0271	625	NUMBER OF WORDS OUT OF RANGE –LOW The Command Block contained a zero or a negative value for number of words. The valid range is 1-256 words.	Correct the value in the Command Block
0272	626	NUMBER OF WORDS OUT OF RANGE –HIGH The Command Block contained a value greater than 256 for number of words. The valid range is 1-256 words.	Correct the value in the Command Block
0273	627	BAD OR MISSING DELIMITER The *receiving* device detected a bad or missing delimiter in the command message	This error usually indicates a transient error in the data link. You should retry the command. If the receiving node is a computer simulating a 2572-A PLC server, ensure that the software is correctly processing the message. If the error persists contact CTI.
0274	628	BAD BLOCK CHECK CHARACTER The *receiving* device found the block check character to be bad.	See error code 0273.
0275	629	INVALID TYPE The *receiving* device reported an invalid TYPE character in the message.	See error code 0273.
0276	630	INVALID DATA CHARACTER The *receiving* device reported an invalid data character. Only characters 0-9 and A-F are allowed.	See error code 0273.
0277	631	ODD NUMBER OF CHARACTERS The *receiving* device reported an odd number of characters in the message. All CAMP messages have an even number of characters.	See error code 0273.
0278	632	INVALID DEVICE CODE The *receiving* device reported an invalid device code in the message.	See error code 0273.
027A	634	INVALID DEVICE CODE The 2572-A detected an invalid device code in the response from the remote device	This error may result from a transient error in the data link. You should retry the command. If the problem persists, check the quality of the data link. If the remote node is a computer simulating a 2572-A PLC server, ensure that the software is correctly creating the response the response message

HEX	DEC	DESCRIPTION	SOLUTION
027B	635	BAD OR MISSING DELIMITER The 2572-A detected a missing delimiter in the response message	See error code 027A.
027C	636	BAD BLOCK CHECK CHARACTER The 2572-A found a bad block check character in the response message.	See error code 027A.
027D	637	INVALID TYPE The 2572-A detected an invalid TYPE character in the message sent from the remote device.	See error code 027A.
027E	638	INVALID DATA CHARACTER The 2572-A detected an invalid data character in the message sent from the remote device. Only characters 0-9 and A-F are allowed.	See error code 027A.
027F	639	ODD NUMBER OF CHARACTERS The 2572-A detected an odd number of characters in the message sent from the remote device. All CAMP messages have an even number of characters.	See error code 027A.
0280	640	UNKNOWN ERROR CHARACTER The response contained an unknown error character.	This error is probably caused by an improperly programmed server node. If the server is a PLC emulating a 2572-A server, review the code and correct as required. If the server is another 2572, contact CTI.
0282	642	INVALID WORD COUNT The response contained an invalid word count	This error is probably caused by an improperly programmed server node. If the server is a PLC emulating a 2572-A server, review the code and correct as required. If the server is another 2572, contact CTI.
0283	643	INVALID ADDRESS The command contained a memory address of 0.	The minimum CAMP address is 1. Enter the correct value for the memory address.
0284	644	INCOMPLETE WRITE The actual number of words written does not match the requested number of words. The actual number of words written is contained in the response message from the remote device.	This error is probably caused by an improperly programmed server node. If the server is a PLC emulating a 2572-A server, review the code and correct as required. If the server is another 2572, contact CTI
028B	651	INVALID IP ADDRESS The command cannot be used with a multicast address.	Change the IP address to a unicast address or change the command to one that supports multicast.
0290	656	INVALID ADDRESS CLASS The address class is not supported by the server	See error 0284 above.
0292	658	MESSAGE ID MISMATCH The response message contained an ID field which did not match the ID field in the command.	This error could be caused by a timeout value which is too short followed by an attempt to re-send. Therefore, by the time the response to the first command arrives, you have already sent a second command. You may correct this condition by increasing the timeout value. This may also be caused by an improperly programmed server. If the server is a PLC emulating a 2572-A server, review the code and correct as required.

HEX	DEC	DESCRIPTION	SOLUTION
029C	668	ETHERNET TRANSMISSION ERROR The Ethernet port was unable to send the packet.	If the problem persists, Contact CTI
029D	669	CMD TIMEOUT ERROR The time to process the requested command exceeded the Command Timeout value. Command processing has been halted. Note that the timeout value may have been explicitly set in the Command Block or the default may have been used (timeout = 0).	If you are using UDP, your *first* attempt to send a message to a newly referenced node may time out while the 2572-A is performing address resolution. Retry the command. In some circumstances, you may occasionally get a timeout error, especially with heavy local network traffic or slow remote data links. In these circumstances, your logic should retry the command. This error may indicate a bad connection (faulty cable, loose connector, etc.). Check all cabling carefully. If the error persists and you have explicitly set the timeout value, it is possible that you have set the timeout value too small. Try increasing the value or using the default value. If you are using multicast, ensure that you are using the Unacknowledged Write command not one of the other Word Transfer commands.
029E	670	ALREADY BUSY ERROR The protocol manager received a new command prior to the completing the previous command.	This error can also be produced by simultaneously triggering two command slots which reference the same command block. If more than one command slot is used, make sure that they reference different command blocks and that the command blocks that they reference have different connection numbers.
02AC	684	MEMORY READ ERROR The 2572-A was unable to read the requested V memory. If this occurs on a WRITE REMOTE command block, it indicates that the 2572-A could not obtain the data from the local PLC V memory. If this occurs on a READ REMOTE command block, it indicates that the memory in the remote device could not be read.	When this error occurs, it is usually due to an invalid memory address specification in the command block. Check the value for Source in Offset 3 and make corrections if necessary. When this error is returned in response to a READ REMOTE command block, it is also possible that there is a problem in the remote PLC which prevents the 2572-A from reading V memory. Retry the command. If the problem persists, check the remote device.
02AD	685	MEMORY WRITE ERROR The 2572-A was unable to write the requested memory. If this occurs on a WRITE REMOTE command block, it indicates that the remote device could not write the data into remote memory. If this occurs on a READ REMOTE command block, it indicates that the local PLC could not write the result from the remote device into local V memory	When this error occurs, it is usually due to an invalid memory address specification in the command block. Check the value for Destination in Offset 5 and make corrections if necessary. When this error is returned in response to a WRITE REMOTE command block, it is possible that there is a problem in the remote PLC which prevents the 2572-A from writing V memory. Retry the command, if the problem persists, check the remote device
02B9	697	UNABLE TO ADD COMMAND TO ACTIVE LIST The module is unable to process this command.	If this occurs, the cause may be a module firmware error. Contact CTI if the error persists.

HEX	DEC	DESCRIPTION	SOLUTION
02BA	698	MINIMUM PRODUCTION INTERVAL OUT OF RANGE The value you specified for the minimum production interval is less than 50 or more than 10,000.	Enter a valid value in the command block and re-execute the command.
02C7	711	COMMAND INPUT QUEUE FULL The target module server queue is full and has rejected the additional command.	This may occur when commands arrive at the 2572 or 2572-A faster than they can be processed through the PLC. More than likely other clients are also sending to the target module. You should check the task codes per scan setting of the PLC containing the target module. For best performance, this should be set to 8. Also, check the scan time to ensure it is not arbitrarily set to a large value. If the preceding steps do not correct the problem you will need to reduce the total transaction loading by slowing down the poll rate from all clients.
02C9	713	UNEXPECTED RESPONSE/BAD EVENT The Unacknowledged Write command received a response from a CAMP server. You are probably attempting to access a CAMP server that does not support the Unacknowledged Write command. An unexpected event occurred.	If you are accessing a 2572-A, you must have firmware version 2.0 or greater. Using the Web browser interface, check the firmware version. If the version is less than 2.0, upgrade the firmware. If you are accessing a 2572 module, the Unacknowledged Write command is not supported. You must use a 2572_ for this application. If you did not intend to use the Unacknowledged Write command, change the command code. If this does not correct the problem, the cause may be a module firmware error. Contact CTI if the error persists.

Server Error Codes

The following error codes may be returned by the PLC server when it is started using PLC logic.

HEX	DEC	DESCRIPTION	SOLUTION
2370	9072	INVALID OPTION BIT The option bit setting is invalid when compared to the other parameters in the command block.	Correct the option bit setting or change the conflicting parameters.
2379	9081	INVALID SUBNET MASK The subnet mask that you entered was invalid for the IP address you have assigned to the module. See appendix D.	Correct the subnet mask entry.
2386	9094	INVALID IP ADDRESS The Start Network Server command block does not contain a valid local IP address.	You cannot use a value of 0000 hex or greater than DFFF hex for the IP address. Correct the entry and retry the command.
2387	9095	INVALID PORT NUMBER The Start Network Server command block contains a value of 0 for the PLC server TCP/UDP port number.	You must select a number greater than 0.

HEX	DEC	DESCRIPTION	SOLUTION
2388	9096	INVALID DEFAULT ROUTER ADDRESS The Start Network Server command block contains an invalid address for the default router.	Correct the entry and retry the command. Note: If you do not have a router on the network, set this value to 0.
238D	9101	# OF CONNECTIONS OUT OF RANGE The number of concurrent TCP server connections you specified in Offset 11 of the command block exceeded the maximum allowable value.	Correct the command block and re-execute the command.
238E	9102	INVALID STARTUP OPTIONS The Startup Options word contains an invalid combination of bits.	Correct the command block and re-execute the command.
2397	9111	UNKNOWN COMMAND The protocol manager received a command number that is not valid.	Ensure that Offset 1 in the Command block contains a valid Command Code. Check that the Command Slot points to the correct V memory Address for the Command Block. Make sure that you have started the correct protocol manager and that you are using the correct connection number.
239E	9118	PROTOCOL MANAGER BUSY The protocol manager received a new command prior to completing the previous command.	You can cause this error by using two command slots to send concurrent commands to the same connection number. Don't do this.
239F	9119	INVALID CONNECTION NUMBER The command block contained an invalid connection number.	Change the connection number in the command block to a valid number. See the documentation on the specific command block.
23AB	9131	SERVER ALREADY STARTED The PLC logic attempted to start another copy of the server on the same physical port. If the error occurs while processing the Start Network Server Command, the Network Server was already started. Only one copy of the server is required to service multiple clients.	This is caused by a PLC logic error. It usually occurs when you are triggering the command more than once. It also may occur when you AutoStart the network server and also try to start the network server from PLC logic.

PLC Client Error Codes

HEX	DEC	DESCRIPTION	SOLUTION
2401	9217	PROTOCOL NOT SUPPORTED The remote device does not support the TCP/IP protocol you are requesting.	The protocol may have been disabled in the startup options of the remote 2572-A Network Server. Check the remote device. Check the network address in the command block. If you are using a PC to emulate a PLC server, ensure that the network parameters are properly set.
2402	9218	SOCKET TYPE NOT SUPPORTED The remote device does not support the socket type you are requesting.	See the previous solution.
2403	9219	NETWORK ADDRESS IN USE The 2572-A cannot obtain the network address.	This may occur when there is a general problem on the network. Check the network address you have specified in the command block. Correct if necessary. Retry the operation. If the problem persists contact your network administrator.
2404	9220	CANNOT ASSIGN ADDRESS The 2572-A cannot assign the requested address.	See above. If the problem persists contact CTI.
2405	9221	NETWORK IS DOWN The network you are attempting to use is down.	This may occur when you are attempting to connect to a remote on another network via a router and the network has been taken out of service. First, make sure that you have specified the correct IP address. Retry the operation. If the problem persists, contact your network administrator.
2406	9222	NETWORK IS UNREACHABLE The network you are attempting to use is unreachable.	You have specified a network address for a network that cannot be found. This probably occurred because you specified an incorrect IP network address. Check the entry in the command block and retry. If you believe that you are using the correct network address, contact your network administrator.
2407	9223	NETWORK CONNECTION ABORTED The remote device (host) aborted the connection.	This may occur if the remote host encountered a problem with TCP data transmission where recovery was not possible. You should attempt to create the connection again. If the problem persists, check the remote host.
2408	9224	CONNECTION RESET BY PEER The remote device has reset the connection.	See error code 2407.
2409	9225	INSUFFICIENT BUFFER SPACE There is insufficient buffer space to hold the message.	This could occur when the remote host has sent more data than the negotiated buffer space. Retry the operation. If the problem persists, contact CTI.
240A	9226	SOCKET NOT CONNECTED The socket you are attempting to use is not connected to the remote host.	The socket may have been previously disconnected from the remote host work by a network error or because the remote host closed the connection. Create the network connection again and retry.
240B	9227	ATTEMPT TO SEND AFTER SOCKET HAS BEEN SHUT DOWN You are attempting to send data to a socket that has been closed	See above.

HEX	DEC	DESCRIPTION	SOLUTION
240C	9228	CONNECTION TIMED OUT The remote host is not responding to an attempt to connect.	Attempt to create the network connection again. If the problem persists check the status of the remote host. Make sure that all IP addresses are properly set, that the remote host is on line, and that network cables are connected properly.
240D	9229	CONNECTION REFUSED The remote host refused the connection.	If the remote host is a 2572, the maximum number of TCP connections allowed has been exceeded. Wait and try again.
240E	9230	REMOTE HOST IS UNREACHABLE The remote host cannot be found.	This error may occur when the remote host has been taken out of service. It may also occur if you have specified an incorrect IP address.
240F	9231	URGENT DATA RECEIVED The remote host has sent urgent data via TCP. This feature is not supported by the 2572-A.	The remote device has sent you a message format that is not supported. If the remote host is a computer, check to software and network setup. For additional information, see documentation on TCP/IP.
2410	9232	OUT OF BAND DATA RECEIVED You have been sent out of band data via TCP. This feature is not supported by the 2572-A.	See above.
246E	9326	NITP PROTOCOL ERROR When the 2572-A sent an NITP message, the remote device replied with an invalid NITP message. NITP protocol errors include: - Odd number of characters received, - Invalid characters received, - Checksum error, - Incorrect character count field.	This error may occur due to communications error (line noise, etc.) on serial lines. It may also result from an improperly programmed remote device. Retry the operation. If the error persists, check out the remote device.
2470	9328	INVALID OPTION BIT VALUE The option bit setting is invalid when compared to the other parameters in the command block.	Correct the option bit setting or change the conflicting parameters. If you are using TCP, you cannot set the IP Address Location bit to 1.
2473	9331	BAD OR MISSING DELIMITER The *receiving* device detected a bad or missing delimiter in the command message	This error usually indicates a transient error in the data link. You should retry the command. If the receiving node is a computer simulating a 2572-A PLC server, ensure that the software is correctly processing the message. If the error persists contact CTI.
2474	9332	BAD BLOCK CHECK CHARACTER The *receiving* device detected a block check character error in the command message.	See error code 2473
2475	9333	INVALID TYPE The *receiving* device reported an invalid TYPE character in the message.	See error code 2473.
2476	9334	INVALID DATA CHARACTER The *receiving* device reported an invalid data character. Only characters 0-9 and A-F are allowed.	See error code 2473.
2477	9335	ODD NUMBER OF CHARACTERS The *receiving* device reported an odd number of characters in the message. All CAMP messages have an even number of characters.	See error code 2473.

HEX	DEC	DESCRIPTION	SOLUTION
2478	9336	INVALID DEVICE CODE The *receiving* device reported an invalid device code in the message.	See error code 2473.
247A	9338	INVALID DEVICE CODE The 2572-A detected an invalid device code in the response from the remote device	This error may result from a transient error in the data link. You should retry the command. If the problem persists, check the quality of the data link. If the remote node is a computer simulating a 2572-A PLC server, ensure that the software is correctly creating the response the response message
247B	9339	BAD OR MISSING DELIMITER The 2572-A detected a missing delimiter in the response message	See error code 247A.
247C	9340	BAD BLOCK CHECK CHARACTER The 2572-A found a bad block check character in the response message.	See error code 247A.
247D	9341	INVALID TYPE The 2572-A detected an invalid TYPE character in the message sent from the remote device.	See error code 247A.
247E	9342	INVALID DATA CHARACTER The 2572-A detected an invalid data character in the message sent from the remote device. Only characters 0-9 and A-F are allowed.	See error code 247A.
247F	9343	ODD NUMBER OF CHARACTERS The 2572-A detected an odd number of characters in the message sent from the remote device. All CAMP messages have an even number of characters.	See error code 247A.
2480	9344	UNKNOWN ERROR CHARACTER The response contained an unknown error character.	This error is caused by an improperly programmed server node. If the server is a PLC emulating a 2572-A server, review the code and correct as required. If the server is another 2572, contact CTI.
248A	9354	INVALID SERVICE TYPE You specified an invalid value for Type of Service. Must be 1=TCP or 2=UDP.	Correct the value in the Command Block.
248B	9355	INVALID REMOTE IP ADDRESS You specified an invalid value for the remote IP Address.	Correct the value in the Command Block.
2490	9360	INVALID ADDRESS CLASS The address class is not supported by the remote device.	If the server is another 2572, check the firmware version of the module to ensure the latest revision. If the server is a PLC emulating a 2572-A server, review the code and correct as required.

HEX	DEC	DESCRIPTION	SOLUTION
2492	9362	CAMP ID MISMATCH The response did not contain a message ID which matched the command. This can be caused by an improperly programmed remote device. It can also be caused by response delays which exceed the command timeout value. Thus it may be a response to a previous command.	Check the remote device for problems and correct as required. Determine whether you have response delays that exceed the command timeout. You may be able to increase the timeout value so that the command waits longer for a response. You can use network analyzer software to view network traffic. See the *Troubleshooting* Chapter of this manual.
2497	9367	UNKNOWN COMMAND The protocol manager received a command number which is not valid.	Ensure that Offset 1 in the Command block contains a valid Command Code. Check to be sure that the Command Slot points to the correct V memory Address for the Command Block. Make sure that you have specified the correct protocol manager number in the Create Connection command and that you are using the right connection number.
249B	9371	ERROR READING ETHERNET PORT An error was encountered reading from the Ethernet port.	If the problem persists, contact CTI.
249C	9372	ERROR WRITING ETHERNET PORT An error was encountered writing to the Ethernet port.	If the problem persists, contact CTI.
249D	9373	CMD TIMEOUT ERROR The time to process the requested command exceeded the Command Timeout value. Command processing has been halted. Note that the timeout value may have been explicitly set in the Command Block or the default may have been used (timeout = 0).	In some circumstances, you may occasionally get a timeout error, especially with heavy network traffic or remote modem data links. In these circumstances, your logic should retry the command. This error may indicate a bad connection (faulty cable, loose connector, etc.). Check all cabling carefully. If the error persists and you have explicitly set the timeout value, it is possible that you have set the timeout value too small. Try increasing the value or using the default value.
249E	9374	PROTOCOL MANAGER BUSY The protocol manager received a new command prior to completing the previous command.	You can cause this error by using two command slots to send concurrent commands to the same connection number. Don't do this.
249F	9375	INVALID CLIENT CONNECTION NO. The connection number used during Create Socket was out of the valid range. The valid range of connection numbers is 19221 –19228.	Correct the command block data.
24AC	9388	MEMORY READ ERROR The 2572-A was unable to read the requested V memory.	When this error occurs, it is usually due to an invalid memory address specification in the command block. Check the command block and make corrections if necessary. Check to ensure that the PLC you are addressing is configured for the address you are trying to access.
24AD	9389	MEMORY WRITE ERROR The 2572-A was unable to write to the requested PLC memory.	Check the command block to ensure a valid V memory address has been specified.

2572-A Internal Errors

Error codes whose lower byte is greater than C8 hex are internal code errors. If you should experience one of these errors, contact CTI for assistance.

APPENDIX C. PLC COMMAND INTERFACE

General Description

CTI 2572-A modules log into the PLC as 2 WX inputs and 6 WY outputs.   The PLC controls the module by placing values in specific WY words. The PLC obtains status information from the module via the WX words. Areas of V memory called *Command Blocks* are used to store command information.

MODULE WX/ WY   **COMMAND BLOCKS**

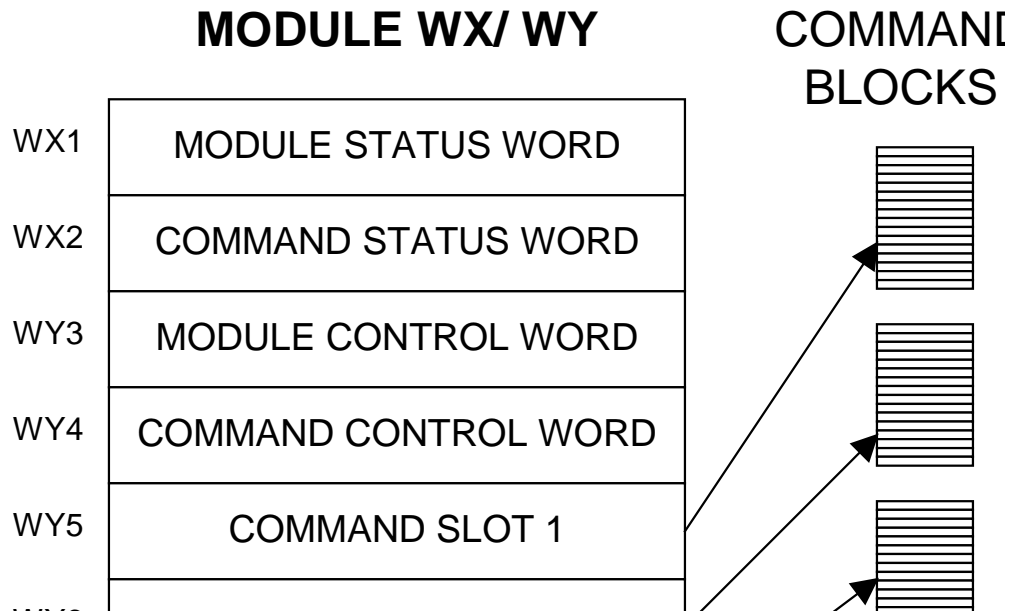|	
WX1	MODULE STATUS WORD
WX2	COMMAND STATUS WORD
WY3	MODULE CONTROL WORD
WY4	COMMAND CONTROL WORD
WY5	COMMAND SLOT 1

Figure 11 illustrates the 2572-A PLC Command Interface. The control structures consist of the module WX/WY words and the Command Blocks. Words WY5-WY8 contain the V memory addresses of the command blocks. Using this command interface, the PLC can initiate up to four commands at one time. The status and control bits for the four commands are located in WX2 and WY4, respectively.

Command Processing Modes

You can specify how the module command execution is synchronized with the PLC logic by setting the Command Mode bit in WY4. The Command Mode bit is described in detail later in this appendix. You can select either *coupled* mode or *uncoupled* mode.

Coupled Mode Processing

Coupled Mode provides for tight "handshaking" between the module and the PLC. When the PLC triggers the command, the module will execute the command *only once*. The module will then wait for acknowledgment from the PLC before allowing the command to be triggered again. Coupled mode is useful for initiating transfers that must be done exactly one time per PLC event (such as Starting the Network Server).

Uncoupled Mode Processing

Uncoupled Mode does not require a handshaking sequence from the PLC. When Uncoupled Mode is selected, the module will read the Command Block when the PLC triggers the command and then execute the command continuously as long as the command trigger is set. Uncoupled mode is useful for providing continuous updates of PLC data.

> *NOTE:*
> *If you make changes to the Command Block, the PLC must clear the command trigger and then reset it before the new Command Block data will be read.*

Command Processing Procedure

Following is the typical procedure used to initiate a module command:

- Set up the Command Block(s) in V memory using your PLC programming software

- Load the command slot(s) with the address of the Command Block(s).

- Set the applicable command trigger and mode bits in WY4.

- Monitor the status of the command processing using WX2.

WX/WY Description

Figure 12 shows the layout of the WX and WY words assigned to the module. WX1 and WY3 are used for global module control and status. The remaining words are used for command processing. Note there are four command slots, which allows the PLC to trigger up to four module commands in one scan. The four sets of bits in WX2 and WY4 correspond to the four command slots.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
Module Status Word																WX1
Command Status Word																WX2
CMD 1 Status Bits				CMD 2 Status Bits				CMD 3 Status Bits				CMD 4 Status Bits				
Module Control Word																WY3
Command Control Word																WY4
CMD 1 Control Bits				CMD 2 Control Bits				CMD 3 Control Bits				CMD 4 Control Bits				
Command Slot 1: V Memory Address of Command Block for CMD1																WY5
Command Slot 2: V Memory Address of Command Block for CMD2																WY6
Command Slot 3: V Memory Address of Command Block for CMD3																WY7
Command Slot 4: V Memory Address of Command Block for CMD4																WY8

Figure 12. WX/WY Map

Module Status Word

The Module Status Word (WX1) is used to communicate the overall status of the module. The module uses the following bit structure:

1	2	3	4	5	6	7	8-15	16
MOD STATUS	RSVD	NET CFG	RSVD	RSVD	LS	RSVD	RSVD	Heart Beat

Bit 1 - MOD STATUS - *Module Status*

This bit is set to 1 whenever the application firmware OK and the network server is started. Note that the 2572 module uses this bit to indicate fatal error.

Bit 2 –RSVD – *Reserved*

This bit is reserved for future use.

Bit 3 -NET CFG - *Network Configuration Required*

This bit is set by the module application code to indicate that the network CAMP server has not been started. The primary use of this bit is to condition PLC ladder logic to trigger the Start Network Server command.

When the PLC Start option is selected, this bit is set to a value of 1 at startup. When the CAMP network server has successfully started, this bit is set to a value of 0.

Bit 4 and 5– RSVD - *Reserved*

These bit positions are reserved for future use.

Bit 6 – LS - *Link Status*

This bit indicates the status of the Ethernet Link. It is set to a value of 1 when the Ethernet port is connected to a functioning Ethernet hub or switch. Otherwise is set to a value of 0.

Bit 7 – 15 RSVD - *Reserved*

These bit positions are reserved for future use.

Bit 16 - HEARTBEAT- *Heartbeat*

The module toggles this bit between 1 and 0 approximately once per second. It is used as an indication that the module software is functioning.

Module Control Word

Module Control Word (WY3)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Mod Rst															

Module Control Bits are contained in WY3. Bit 1 is a module reset bit. **When the bit is set *and* all four abort triggers are set, the module will perform a hardware reset.** This operation resets the processor and initiates a complete module restart. It is available for extreme error cases where simply acknowledging an error or aborting a command does not clear the error.

> *NOTE:*
> *Once the module has reset, your PLC logic must re-execute any commands used to configure the module or to start the network server.*

Command Control and Command Status Words

The command status word and the command control word contains bits that are used to synchronize and control the execution of module commands. The Command Control Word is located in module word WY4 and contains bits that are set by the PLC logic. The Command Status Word is located in WX2 and contains bits that are set by the module.

Since the PLC can send up to four commands to the module per scan, both the Command Control Word and the Command Status Word contain four sets of bits, one set for each possible concurrent command. For example, the first four bits (bits 1-4) in both words relate to command Slot 1, the next four bits (bits 5-8) relate to command Slot 2, etc.

The four command slots execute commands independently. Thus, an error on one command does not affect processing on the other commands than happen to be executing at the same time. The command slots can be triggered at different times or some (or all) may be triggered concurrently.

Command Control Word

The Command Control Word contains bits that are set by the PLC logic. The following illustration indicates how the bits within the word are used.

COMMAND CONTROL WORD (WY4)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ERR Ack	CMD Mode	CMD Trig	Abort Trig	ERR Ack	CMD Mode	CMD Trig	Abort Trig	ERR Ack	CMD Mode	CMD Trig	Abort Trig	ERR Ack	CMD Mode	CMD Trig	Abort Trig
COMMAND 1				COMMAND 2				COMMAND 3				COMMAND 4			

ERROR Ack	*Error Acknowledge.* The PLC sets this bit to acknowledge the error bit which was set by the 2572.
CMD Mode	*Command Mode.* The PLC sets this bit to control how the module command execution is synchronized with the PLC logic:
	0 = Uncoupled mode - The 2572-A command processing is not synchronized with the PLC logic.
	1 = Coupled mode - The 2572-A command processing is synchronized with the PLC logic.
CMD Trig	*Command Trigger.* The PLC sets this bit to initiate a command.
ABORT Trig	*Abort Trigger.* The PLC sets this bit to abort a command in progress. In most applications, use of the abort bit is not required.

Command Status Word

The Command Status Word contains bits that are set by the module. The following illustration indicates how the bits within the word are used.

COMMAND STATUS WORD (WX2)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
CMD Err	PLC Err	CMD Busy	Abrt Busy	CMD Err	PLC Err	CMD Busy	Abrt Busy	CMD Err	PLC Err	CMD Busy	Abrt Busy	CMD Err	PLC Err	CMD Busy	Abrt Busy
COMMAND 1				COMMAND 2				COMMAND 3				COMMAND 4			

CMD Err *Command Error.* The 2572-A sets this bit when it encounters an error while attempting to execute the command. The 2572-A will write an error code into Offset 0 of the command block unless PLC ERR is also set (see below).

PLC Err *PLC Read/Write Error.* The 2572-A sets this bit to indicate that it could not read a valid command block from V memory. Therefore, there is no place to write an error word. This may be caused by loading a value in the Command Slot which is not a valid V memory location (such as 0) or which points to V memory that does not contain a Command Block.

CMD Busy Indicates the module is in the process of executing a command.

ABORT Busy Indicates the module is attempting to abort a command.

Command Slots (WY5-WY8)

Module words WY5, WY6, WY7, and WY8 are called Command Slots. There are four command slots, one for each possible concurrent command. The value in the command slot points to the V memory address of a command block as illustrated below. Addresses of 0 or less are invalid. Addresses greater than 64k cannot be referenced.

COMMAND SLOTS

WY5	Command Slot 1: V Memory Address of Command Block for CMD1
WY6	Command Slot 2: V Memory Address of Command Block for CMD2
WY7	Command Slot 3: V Memory Address of Command Block for CMD3
WY8	Command Slot 4: V Memory Address of Command Block for CMD4

Note that the command slots match up with the command control and command status bits in WY4 and WX2. For example, the command block whose address in Command Slot 1 will be triggered by setting bit 3 in WY4 (Bit 3 is the Command Trigger for Command 1).

WX2 and WY4 Relationships

The following illustrates the relationship between the first four bits in WX2 and WY4. This relationship applies to the other three sets of bits.

Word	Bit 1	Bit 2	Bit 3	Bit 4
WX2	CMD Err	PLC Err	CMD Busy	Abort Busy
WY4	ERR Ack	CMD Mode	CMD Trigger	Abort Trigger

Error Processing Bits

The module will set CMD ERR any time an error occurs in processing a command. The module will also set PLC ERR if a valid Command Block cannot be read from V memory. After setting the error bits, the module will halt processing on this command. The PLC acknowledges the error by setting ERR ACK. When the module sees ERR ACK go high, it aborts the command, clears the error bits, and is ready to accept another command trigger for this slot.
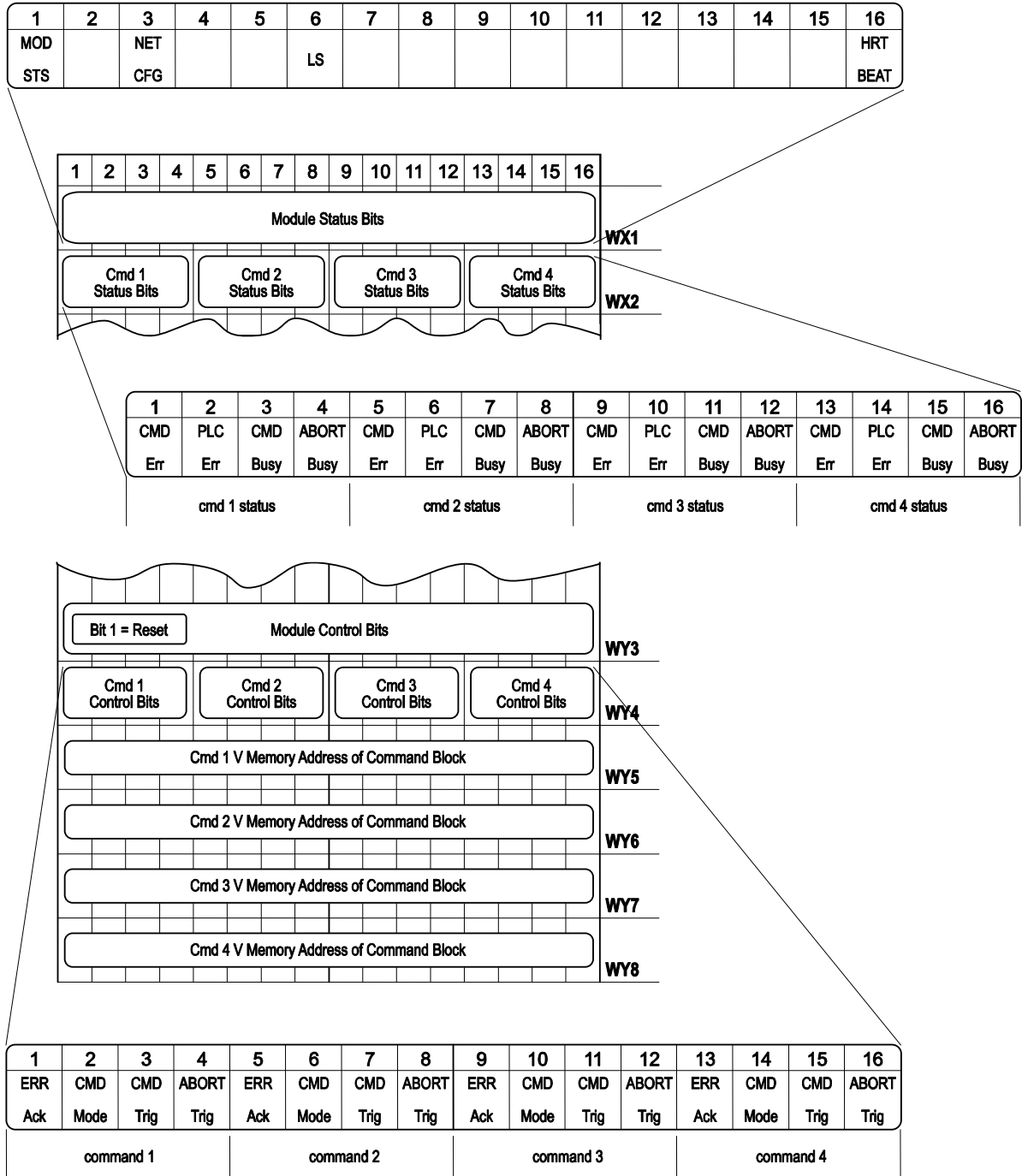
Command Processing Bits

The PLC sets the CMD MODE bit to select whether Coupled Mode or Uncoupled Mode is used. The PLC sets the CMD TRIGGER to initiate the command. When the module begins command processing, it sets the CMD BUSY bit. The CMD BUSY bit will remain on until the module has completed processing the command.

Abort Processing Bits

The PLC can set the ABORT TRIGGER to request the module to abort a command that is in process. When the module starts the process of aborting a command, it raises the ABORT BUSY bit. When the process is complete, it lowers ABORT BUSY (and also CMD BUSY).

The timing diagrams in this appendix describe the interaction of the various Command Control and Command Status bits.

WX/WY Quick Reference

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
MOD STS		NET CFG			LS										HRT BEAT

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Module Status Bits																WX1

| Cmd 1 Status Bits | Cmd 2 Status Bits | Cmd 3 Status Bits | Cmd 4 Status Bits | WX2 |

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
CMD Err	PLC Err	CMD Busy	ABORT Busy	CMD Err	PLC Err	CMD Busy	ABORT Busy	CMD Err	PLC Err	CMD Busy	ABORT Busy	CMD Err	PLC Err	CMD Busy	ABORT Busy
cmd 1 status				cmd 2 status				cmd 3 status				cmd 4 status			

| Bit 1 = Reset | Module Control Bits | WY3 |

| Cmd 1 Control Bits | Cmd 2 Control Bits | Cmd 3 Control Bits | Cmd 4 Control Bits | WY4 |

| Cmd 1 V Memory Address of Command Block | WY5 |

| Cmd 2 V Memory Address of Command Block | WY6 |

| Cmd 3 V Memory Address of Command Block | WY7 |

| Cmd 4 V Memory Address of Command Block | WY8 |

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ERR Ack	CMD Mode	CMD Trig	ABORT Trig	ERR Ack	CMD Mode	CMD Trig	ABORT Trig	ERR Ack	CMD Mode	CMD Trig	ABORT Trig	ERR Ack	CMD Mode	CMD Trig	ABORT Trig
command 1				command 2				command 3				command 4			

Command Blocks

Command Blocks contain information which specifies how the command is to be executed. The standard Command Block consists of 16 contiguous words located in the first 64k of PLC V memory and has the following general structure.

Offset	Contents
0	Error Word
1	Command Code
2	Connection Number
3	Command Parameter 1
4 - 15	Additional parameters

Error Word   Assuming the Command Block is valid, the module will write an error code into this location when it encounters an error in executing the command. The error code can be used during development as an aid to de-bugging logic. It may also be used by the PLC logic as an indication to execute specific error processing logic.

Command Code   The Command Code is a number which uniquely defines the command you wish to execute.

Connection Number   The connection number identifies the instance of the protocol manager with which you are communicating. A connection number is similar to a file handle used in other operating environments. The connection number is established when a CREATE CONNECTION or CREATE SOCKET command is executed. During this process, a specific protocol manager is loaded and associated with a particular physical port or a network socket. If the connection is created using PLC logic, the programmer can assign a connection number. If the connection is automatically created by the module, the module will assign a connection number.

The high byte of the Connection number should always contains hex 4B. The module uses this byte as a Command Block "signature". The use of the signature byte provides a way for the module to verify that the address you loaded in the command slot indeed points to a valid command block and not some arbitrary area of V memory. When the module detects that you have referenced an area of V memory where the high byte of offset 3 does not contain hex 4B, it asserts the CMD Err and PLC Err. Since the module assumes that a block without a signature byte is not a command block but a reference error, it does not attempt to process the block of V memory and does not write any error information back into offset 0 of the block.

Command Parameters   The command parameters provide command execution information. For example, for a Read Command they may specify where to obtain the data, how many words to read, and where to store the results. The number of command parameters required will vary with different commands.

Command Timing Diagrams

Coupled Mode Timing (CMD Mode = 1)

Coupled Mode should be selected when you want to ensure that the module will execute a command only once per trigger. In Coupled Mode the PLC and the module use the CMD TRIG (Command Trigger) and the CMD BUSY (Command Busy) bits in a "handshaking" sequence. The following figure illustrates the timing relationships between CMD TRIG and CMD BUSY for a Coupled Mode command.

The PLC has cleared CMD TRIG (Time A) and the module has cleared CMD BUSY (Time B) indicating that the processing of the previous command is complete.

At Time C, the PLC asserts CMD TRIG to initiate a command. When the module recognizes that CMD TRIG is high, it asserts CMD BUSY (Time D) and samples the CMD MODE bit to determine the command mode. It then retrieves the command block and starts processing the command. Any time after the PLC sees CMD BUSY go high, it may lower CMD TRIG (Time E).
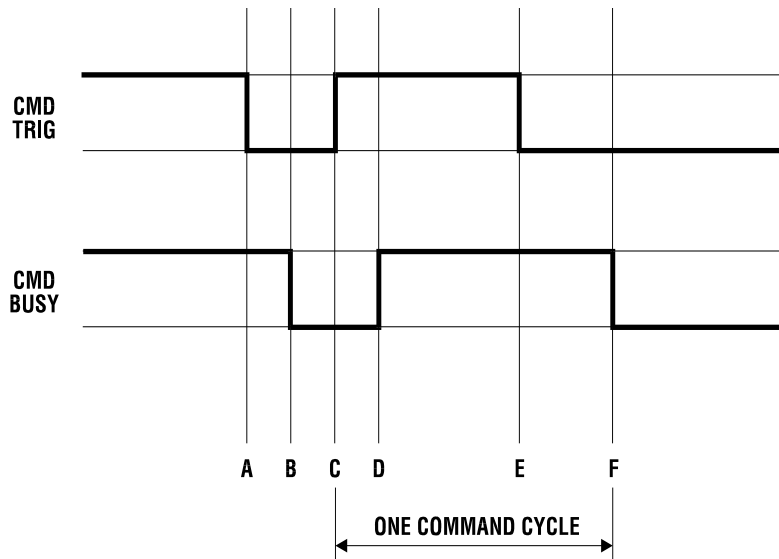
Figure 13. Coupled Mode Timing

Once the module completes processing the command, it samples CMD TRIG. If CMD TRIG is off, the Module will lower CMD BUSY (Time F) and wait for the next trigger. If CMD TRIG is on, the module will hold busy high and wait until CMD TRIG is turned off. Time F will be delayed as required until CMD TRIG is off. At time F (equivalent to time B), both CMD TRIG and CMD BUSY are low and a new cycle can begin whenever the PLC asserts CMD TRIG.
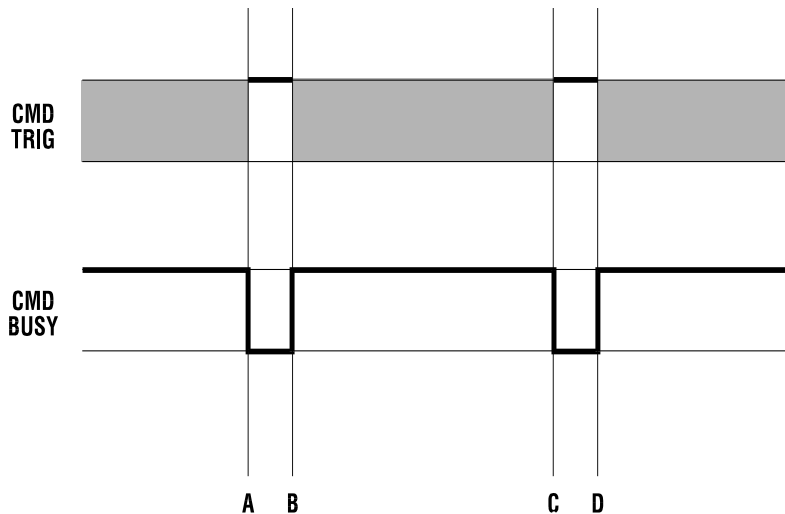
> *NOTE:*
> *The Command Block is subject to access and change by the module anytime after CMD TRIG is asserted (time C) until CMD BUSY is cleared (time F). Thus, the Command Block should not be changed by the PLC at any time between time C and F.*

CTI 2572-A Installation and Operation Guide

Uncoupled Mode Timing (CMD Mode =0)

Uncoupled Mode may be selected when close synchronization between the PLC and the module is not required. In this mode, a single trigger can cause the module to execute a command many times. Uncoupled mode is useful in applications where you want to continuously update the remote PLC. Uncoupled Mode usually takes less PLC logic to implement than Coupled Mode. The following figure illustrates the timing relationships between CMD TRIG and CMD BUSY for an Uncoupled Mode command. The shaded area in the diagram indicates that it does not matter what the status of the bit happens to be (*don't care* condition).

At time A, the module has cleared CMD BUSY, indicating that Command processing is complete. When CMD BUSY is low and CMD TRIG is high the module will assert CMD BUSY (Time B) and begin command processing. CMD BUSY will remain on during the processing of the Command Block. When the processing is complete, the module will lower CMD BUSY (Time C). *Note that in Coupled Mode, the module would wait for the PLC to lower the trigger before clearing CMD BUSY*.

Figure 14. Uncoupled Mode Timing

At the next end of the PLC I/O scan, the module will again sample CMD TRIG. If CMD TRIG is high, the module will raise CMD BUSY and execute the same command again, without re-reading the Command Block from the PLC. Note that the PLC logic is not required to cycle CMD TRIG.

If continuous operation is desired, the PLC can simply leave the CMD TRIG on. The Module will then repeat the command as fast as possible.

> *NOTE:*
> *As long as the 2572-A detects that CMD TRIG is high when CMD BUSY is lowered, it will execute the same command again, It will not re-read the Command Block from the PLC. Therefore, if you wish to change the command to the module, the PLC logic should clear CMD TRIG and ensure CMD BUSY is cleared before changing the contents of the Command Block or the associated Command Slot. Alternately, use Coupled Mode for these applications.*

Command Error Timing

The module provides a mechanism for command execution communicating errors to the PLC. This is accomplished via the CMD ERR bit and the ERROR WORD in the Command Block. The following figure illustrates Command Error timing. Note that the shaded area indicates a "don't care" condition for the particular bit.

At time A, the module has set CMD BUSY and is attempting to retrieve the command block and to process the command.

Some time later, a command processing error occurs. The module writes error information into the error word of the Command Block and asserts CMD ERR at time B. Processing of this command is halted.

If the module cannot write the error word to the Command Block, it also asserts the PLC ERR bit (see the following section). *The error word is valid only when CMD error is asserted and PLC ERR is clear.*
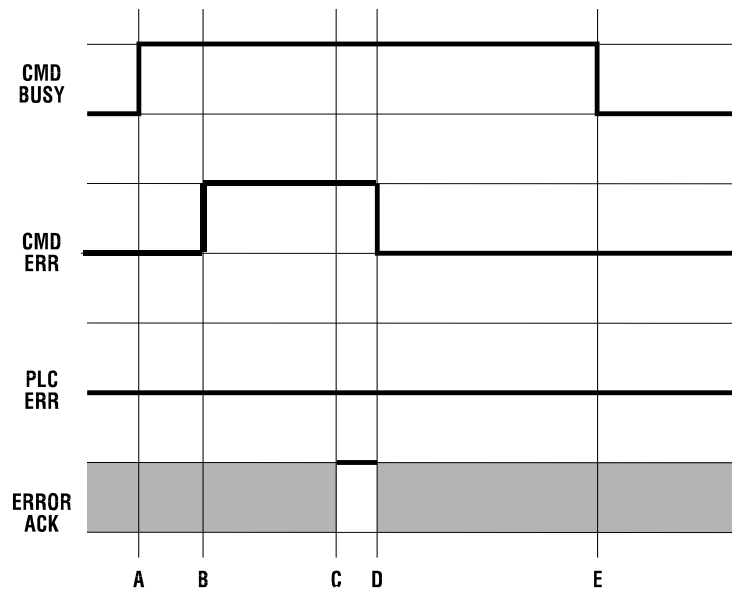
Figure 15. Command Error Timing

At the end of each PLC I/O scan, the module samples the state of ERROR ACK (Error Acknowledge). As soon as the module detects that ERROR ACK is set (Time C), it will turn off CMD ERR (and PLC ERR if on) at Time D and proceed with the error recovery.

After error recovery is completed, the module will clear CMD BUSY (Time E). This may or may not be the in the same PLC I/O scan. CMD ERR will never be asserted unless CMD BUSY is asserted. CMD ERR is always cleared prior to or at the same time as the release of the CMD BUSY signal (Time D is always before or the same as time E).

> *NOTE:*
> *The contents of the error word in the Command Block is valid only when CMD ERR is asserted and PLC ERR is clear.*

Since the ERROR ACK signal is sampled only when CMD ERR or PLC ERR is asserted, PLC logic can leave the ERROR ACK bit on, if you wish to ignore all errors.

CTI 2572-A Installation and Operation Guide

PLC Error Timing

A PLC error occurs when the module cannot read a valid Command Block from the PLC V memory or it cannot write back to this location. The following diagram illustrates timing for the PLC ERR bit. Note that the shaded area indicates a "don't care" condition for the particular bit.

At time A, the module has set CMD BUSY and attempts to retrieve the command block from V memory. At time B, the module determines it cannot retrieve a valid command block and asserts the CMD ERR and the PLC ERR bit. Since a valid command cannot be retrieved, the module halts processing of this command.

At time C the module samples the ERROR ACK bit and determines that it is asserted, indicating that the PLC has acknowledged the error. Some time later the module clears the CMD ERR and PLC ERR bits (Time D) and the CMD BUSY bit (Time E). The error bits will always be cleared prior to or at the same time as CMD BUSY.
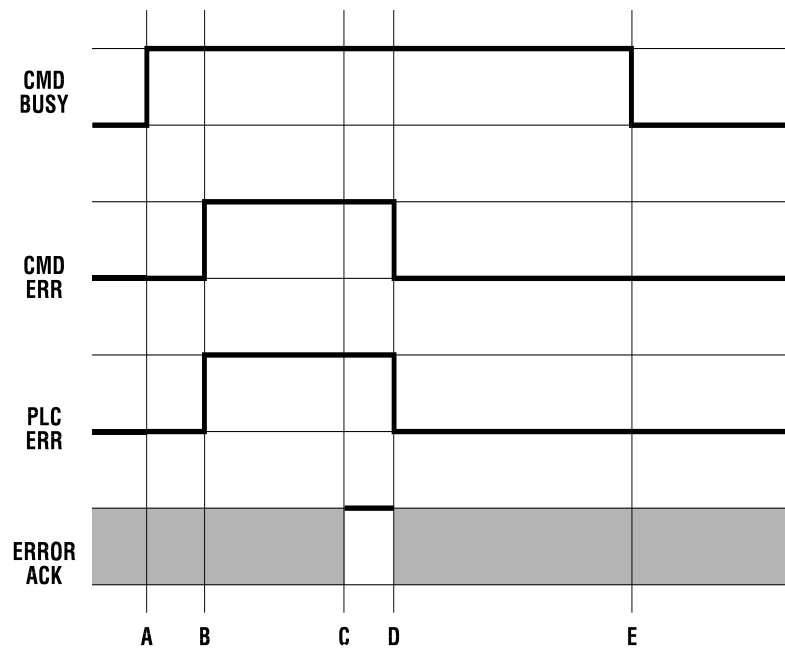
Figure 16. PLC Error Timing

Note that, in this example, no error code is written to the command block. Since a Command Block could not be read, the module does not attempt to write an error code into the V memory location indicated in the command slot.

NOTE:
When the PLC ERR bit is set, it is almost always the result of:
1) an invalid address in the Command Slot (WY5, WY6, WY7, or WY8) or
2) a command block connection number that does not have hex 4B in the high byte
*If the PLC ERR bit is on, you should check your PLC logic carefully!*

Command Abort Timing

There may be rare occasions when you need to abort a command that is in progress. For example, if you triggered a READ REMOTE command with an infinite timeout and the data was never returned, the protocol manager would wait forever, blocking further execution in the command slot. Figure 17 illustrates abort timing.

Assume the module is busy processing a command (Time A). At time B, the PLC asserts ABORT TRIG to stop the ongoing command processing. When the module recognizes that ABORT TRIG is high, the module will assert ABORT BUSY (Time C).

After detecting ABORT BUSY, the PLC should clear ABORT TRIG (Time D). When the Module has completed abort processing, it clears ABORT BUSY(Time E).

After ABORT BUSY is cleared, the module will clear CMD BUSY (Time F). Time F may be on the same scan or on a later scan than time D. ABORT BUSY will never be asserted unless CMD BUSY is also asserted.
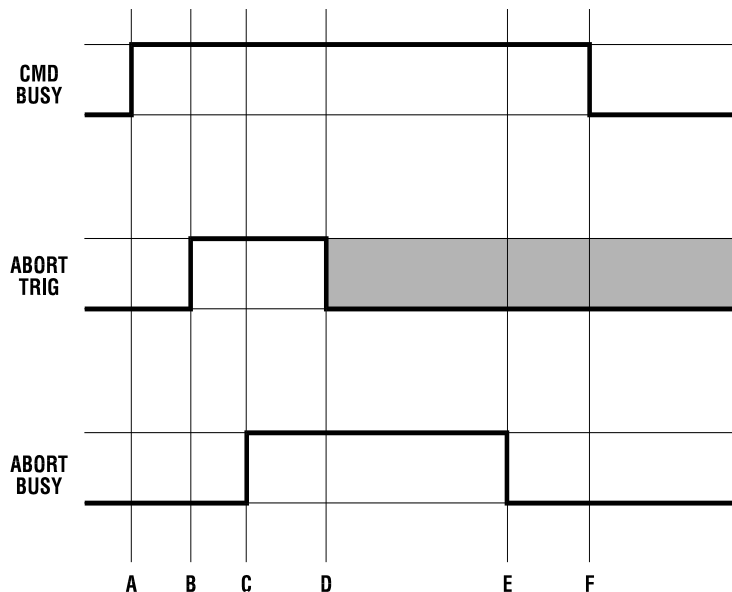
Figure 17. Command Abort Timing

NOTE:
ABORT BUSY will be cleared even if the ABORT TRIG is still active. If the PLC does not clear ABORT TRIG, no further commands will be processed for the Command slot.

Depending upon the nature of the command and circumstances of execution, some commands cannot be aborted.

NOTE:
Setting all four abort triggers and asserting the module reset bit in WY3 will cause the module to perform a complete reset.

General Command Considerations

When designing your PLC logic you should be aware of the following:

- The Command Trigger is ignored for a command if the associated Abort Trigger is set.

- In Uncoupled Mode, the PLC may not see CMD BUSY go low in between command cycles. After you lower the trigger, the module may execute the command additional times.

- If ERR ACK is set and left high, the associated CMD ERR bit may be set and cleared without the PLC detecting it.

- With the notable exception of Module Reset (all four abort triggers are set along with the module reset bit) the command slots are totally independent. Unless the commands are directed to a common resource, the command slots should have no effect on each other.

APPENDIX D. IP ADDRESS INFORMATION

IP Address Nomenclature

Every host interface on a TCP/IP network is identified by a unique IP address. This address is used to uniquely identify the host and the network to which the node belongs.

Each IP address consists of 32 bits, divided into four 8 bit bytes (called *octets*). An IP address is usually expressed in *dotted notation,* with each octet expressed as its decimal equivalent. See the example below.

Notation	Byte 1	Byte 2	Byte 3	Byte 4
Binary	11000000	11011111	10110001	00000001
Decimal	192	223	177	1

Although an IP address is a single value, it contains two pieces of information: the *Network ID* and the *Host ID*. The Network ID identifies a group of computers and other devices that are all located on the same logical network. In internetworks (networks formed by a collection of local area networks), there is a unique network ID for each network. The Host ID identifies a specific device within a particular network.

The Internet community has defined address classes to accommodate networks of varying sizes. Each network class can be discerned from the first octet of its IP address. The following table summarizes the relationship between the first octet of a given address and its Network ID and Host ID fields. It also identifies the total number of Network IDs and Host IDs for each address class that participates in the Internet addressing scheme. This sample uses w.x.y.z to designate the bytes of the IP address.

Class	w values*	Network ID	Host ID	Number of networks	Number of hosts per net
A	1-126	w	x.y.z	126	16,777,214
B	128-191	w.x	y.z	16,384	65,534
C	192-223	w.x.y	z	2,097,151	254

* Inclusive range for the first octet in the IP address. The address 127 is reserved for loopback testing and inter-process communication on the local computer; it is not a valid network address. W values 224 – 239 are used for Class D - IP multicast.

Private IP Addresses

If you are planning on connecting to the 2572-A modules via the Internet, you *must* obtain a set of IP addresses from the Internet Assigned Numbers Authority (IANA). Contact you network administrator or point your browser to http://www.isi.edu/div7/infra/iana.html. to obtain more information.

If you are certain that you do not need to connect to the Internet, you can use a block of 'private' addresses specified in RFC 1597. The private addresses are:

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

These addresses will not be forwarded by the Internet backbone routers. For more details see the Web site at http://www.cis.ohio-state.edu/rfc/rfc1597.txt

Subnet Mask

Although the address class concept provides a standard way to determine the network portion of the IP address there are times that you may wish to further divide an assigned network ID among several local networks. For example, you may wish to install routers to segment network traffic. The Subnet Mask provides the means to accomplish this.

The Subnet Mask is a collection of 32 bits that distinguish the network ID portion of the IP address from the host ID. Subnet masks are determined by assigning 1's to bits that belong to the network ID and 0's to the bits that belong to the host ID. Once the bits are in place, the 32-bit value is converted to dotted decimal notation. See the example below.

Bits for Subnet Mask				Subnet Mask
11111111	00000000	00000000	00000000	255.0.0.0
11111111	11111111	11110000	00000000	255.255.240.0
11111111	11111111	11111111	00000000	255.255.255.0

For example: when the IP address is 128.54.177.97 and the subnet mask is 255.255.255.0, the Network ID is 128.54.177 and the Host ID is 97.

> *NOTE:*
> *All computers on a physical network segment should use the same subnet mask and network ID; otherwise, addressing and routing problems may occur.*

The Subnet Mask must correspond to the address class of the IP Address.

- For a Class A network, at least the first 8 bits must set to 1.

- For a Class B network, at least the first 16 bits must be set to 1.

- For a Class C network, at least the first 24 bits must be set to 1.

The subnet mask must allow at least two bits of host address. This translates into the requirement that that the subnet mask must contain at least two zeroes. In addition, a subnet mask which causes the derived host address to be 0 or a broadcast address (all bits set to 1) is invalid.

Port Number

The *Port Number* identifies a particular process or service offered by the host. Some services, such as echo server, are provided via standard "well known" port numbers. For the 2572-A PLC Network Server facility, you can configure the TCP/UDP port number.

> *NOTE:*
> *The examples in CTI documents use 1505 (decimal) as the PLC Network Server port number. Unless you have a specific reason for using another number, you should use 1505.*

APPENDIX E. USING DHCP

DHCP Overview

DHCP (Dynamic Host Configuration Protocol) provides an automated method of configuring devices on a TCP/IP network. DHCP was popularized by Microsoft Windows. Because of the rapid increase in personal computers using TCP/IP, DHCP has become commonplace in the office environment.

DHCP is built around the client-server model in which networked computers (clients) contact a centralized server for configuration parameters. Although the most common use of DHCP is to assign IP addresses, network masks, and default router addresses, the protocol is capable of providing other information, such as the path to application programs or configuration files.

The DHCP server provides two methods for assigning IP addresses to devices, dynamic assignment and static assignment. Both may be used concurrently.

Dynamic Assignment

Using the dynamic assignment method, the DCHP server assigns an IP address to a device from a pool of available IP addresses based on rules established by the network administrator. The IP address is leased to the device for a specified period of time. When the lease time expires, the lease may be renewed or a new IP address may be assigned to the device. If not renewed, an IP address with an expired lease goes back into the pool of IP addresses available for assignment. The dynamic assignment is method is commonly used for PC workstations, whose operation is unaffected by a change in the IP address. It is especially popular for assigning IP addresses to portable "laptop" computers that may move from network to network.

Static Assignment:

Using the static assignment method, the DHCP server assigns a fixed IP address to the device, based on a unique identifier supplied by the device.. The network administrator configures the DHCP server to associate the unique identifier with a specified IP address and other network parameters.

> *NOTE:*
> *The Microsoft DHCP Server refers to static entries as reservations.*

The static assignment method is used for devices whose function must be tied to a fixed IP address. In the office environment, devices requiring a fixed IP address are typically network servers that provide file, printing, and application services to the PC workstation clients. These devices require an unchanging IP address that must be known by client PCs seeking data or services from the server.

> *NOTE:*
> *On the plant floor, devices such as the 2572-A act as servers and require a fixed IP address.*

The host characteristic most commonly used to associate a fixed IP address with a device is the hardware address of the network interface, also referred to as the link layer address or the MAC ID. For Ethernet networks, the MAC ID is assigned at the factory by the manufacturer of the Ethernet product. The disadvantage of using the MAC ID as a means of assigning an IP address surfaces when the device must be replaced. Because the new device will have a new MAC ID, the DHCP server must be re-configured. For devices administered by the information services personnel, reconfiguring the DHCP server is usually acceptable. For plant floor devices, the requirement to reconfigure a DHCP server when a device is replaced by maintenance can be problematic.

An alternate method allows the use of a user-specified field known as a Client Identifier (Client ID) for this purpose. The 2572-A module uses a patent-pending technique to generate a Client ID by concatenating the value of the module ID switches with a fixed value representing the CTI Ethernet manufacturer ID (assigned by IEEE) and the first four digits of the product number as shown below.

CTI Manufacturer ID	Product Number	Module ID
002025	2572	01 thru FE

For example, if you set the Module ID switches to a value of 56, the generated client ID would be 002025257256.

Once you configure the DHCP server to associate this Client ID with a fixed IP address and set the Client ID switches accordingly, the module will automatically obtain its IP address and other network parameters from the DHCP server when it starts up. Should you need to replace the module for any reason, the only configuration required of the replacement module is to set the module option switches and Module ID switches to match the previous module.

Configuring a DHCP Server

There are several alternatives for implementing a DHCP server. The most common alternative is to use the DHCP server that is included with Microsoft server software. This example assumes that you are using the Microsoft DHCP manager in Windows 200 Advanced Server. Other DHCP servers provide similar features, but the terminology may vary slightly. This example assumes that you are starting with a fresh instance of a DHCP server. If you are adding the 2572-A to an existing DHCP server, you may be able to skip some of these steps.

Create a Scope

A Scope identifies a range of IP addresses that will be managed by the DHCP server. If a scope has not been defined, you will need to create one. Figure 18 illustrates the dialog box for specifying the scope range and associated subnet mask. In this example, a pool of addresses from 192.168.1.20 through 192.168.1.200 is included in the scope.
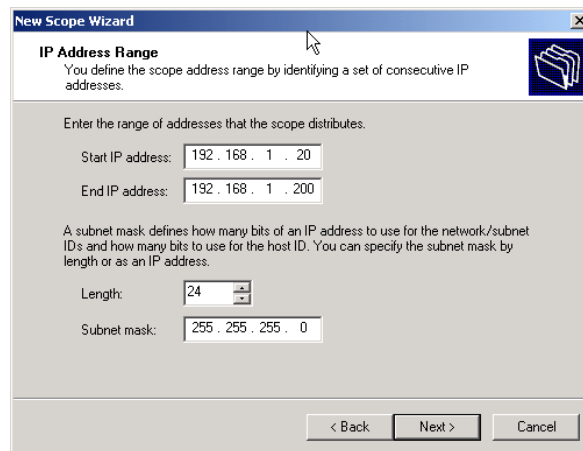

Figure 18. DHCP Scope Range

You may also exclude IP addresses within the scope range using the Add Exclusions dialog box. In the example, the IP addresses from 192.168.1.100 through 192.168.1.120 are excluded.

It is important to make sure that all addresses on the subnet that are specified by some other method (such as manual configuration) be excluded from the scope. If these are not excluded, the DHCP server may attempt to assign these addresses to another network station, resulting in duplicate IP address assignments.
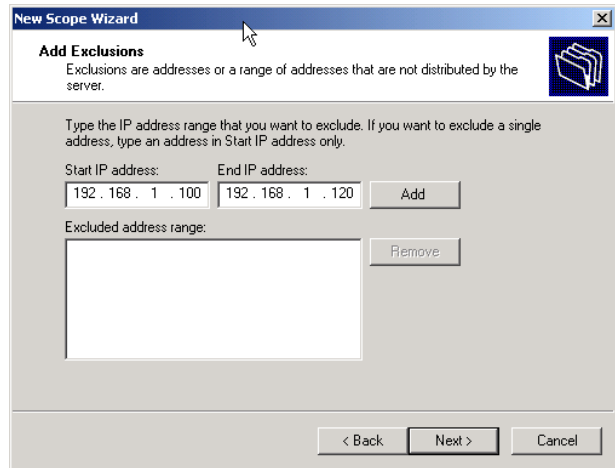
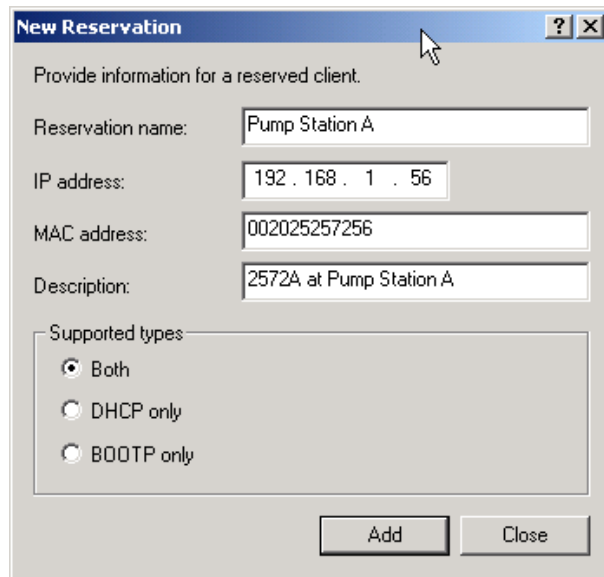*Figure 19. DHCP Scope Exclusions*

Establish Reservations

The reservations facility allows you to specify a fixed IP address that will be assigned to a particular network station.

NOTE:
Every 2572A that uses DHCP should have a unique reserved IP address

Figure 20 shows an example of creating a reservation. In the IP address box, enter the IP address which you want to assign to the module. In the example, the IP address is set to 192.168.1.56.

In the MAC Address box, enter 0020252572 followed by the value to which the Module ID switch will be set. In the example, the Module ID switch will be set to 56.

In this example, when you startup a 2572-A module with the Module ID set to 56, the IP address of 192.168.1.56 will

Figure 20. DHCP Reservation Dialog Box

automatically be assigned to it. Also, the subnet mask of the scope (255.255.255.0) will be assigned.

NOTE:
In the above example, the value of the last octet of the IP address matches the Module ID value. Although this direct correspondence is not required, it is a helpful method in keeping track of module IP assignments.

DHCP Options

DHCP options are used to assign other module parameters. An option may be applied globally (all scopes), to a scope, or to an individual reservation. If you want to use the module default values, you are not required to configure the option in the DHCP server. The default values for the options used by the 2572-A module are:

Parameter	Default Value
Default Router	0.0.0.0 (No routing)
CAMP Server Port Number	1505
CAMP Server Maximum TCP Connections	16
TCP KeepAlive	60 Seconds
TFTP Server	Value Stored in Module EEPROM
Boot File Name	Value stored in Module EEPROM

If you wish to change the default values, you will need to configure the corresponding option in the DHCP Server.

The most common DHCP Option is the Default Router option. A default router is required if you wish to allow access to the module from other networks. Figure 16illustrates the dialog box used to add a default router option to the scope. Although multiple routers may be configured, the 2572A will use only the first one in the list.

The 2572A also supports the following standard DHCP options:

Number	Description
038	Keep Alive Interval
067	Boot File Name

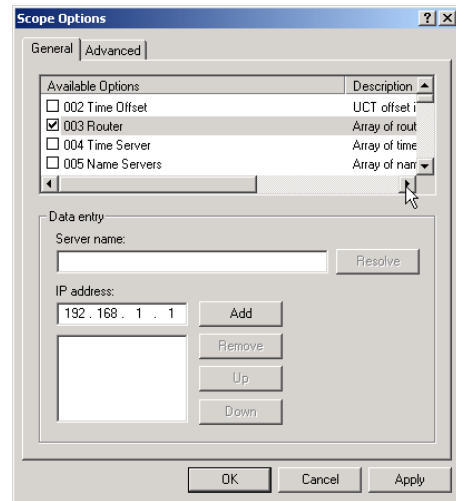**Figure 21. DHCP Router Option**

You can also add the following CTI options to the DHCP server options:

Number	Description	Format
130	CAMP Server Port Number	Word
131	CAMP Server Maximum TCP Connections	Long
132	TFTP Server Address	IP Address
133	Multicast IP Address	IP Address

Once added, the CTI Options can be configured the same as a standard option.

> *NOTE:*
> *Unless you want **all** modules to listen to a single multicast address, you should assign the multicast IP address for each reservation.*

APPENDIX F. Updating Firmware

Overview

The 2572-A stores all firmware in flash memory. This allows the firmware to be upgraded in the field, eliminating the need to replace physical PROMS. There are two types of firmware used with the 2572-A, the application firmware and the boot loader firmware.

The application firmware performs all of the primary module functions, including the PLC server, PLC client, and Web server tasks. When new features are added to the module, the application firmware will change.

The bootloader is a small section of code that performs module startup functions (including DHCP) and manages the firmware download functions. Because most of the bootloader functions are generic, it may not change when new functions are added.

When you are upgrading the 2572-A module firmware, you must choose which type of firmware you are downloading. During the download process, the firmware will be checked to ensure that it is the correct type and that it is compatible with the version of the 2572-A hardware you are using.

Update Preparation

Obtain TFTP Server Software

The 2572-A module uses the Trivial File Transfer Protocol (TFTP) to copy the firmware files from a hard drive to the module. The module will need network access to a TFTP server, which is a small program that can run on your local PC.

TFTP servers are available for free download from several sources. One such source is Solar Winds, a provider of network analysis software. Point your browser to:
http://support.solarwinds.net/updates/SelectProgramFree.cfm# to access the download page. Once you have installed the TFTP software on your PC, start the TFTP server and set the TFTP root directory. You will place the new firmware files in the directory.

> *NOTE:*
> *If you are using Windows XP SP2 or above, you may have a local firewall enabled. Also, you may have a local firewall installed by virus scanning software such as McAfee Personal Firewall. If this is the case, you must open port 69 on the firewall or disable the firewall entirely in order to use the TFTP server. For Windows XP, you can accomplish this using the "Windows Firewall" application in Control Panel. For other local firewalls, refer to the vendor documentation accompanying the software.*

Obtain New Firmware

2572-A firmware may be downloaded from the following URL:
ftp://www.controltechnology.com/public/Download/2572A/
The firmware is stored as a self extracting zip file. See the readme file in the download directory or contact your CTI support representative for the name of the file to download. After downloading the applicable file(s) to a folder on your hard drive, run the program. This will extract several files to the target directory you select. Make sure these file are placed in the root directory of the TFTP server.

Updating 2572-A Firmware

Point your browser to the IP address of the module. From the Main Menu web page, select the Firmware Download option. Unless you have bypassed password protection, you will be prompted for a user name and password. The default factory user name and password are both `download`. The actual password is user configurable. Once the module has validated the user name and password, the following web page will be displayed.

If you are downloading new application firmware, go to the DOWNLOAD APPLICATION FIRMWARE section, enter the IP address of the computer running the TFTP server software, verify that Command File Path contains the name of the command download file (enildr.cmd), and click on the Download button. The module should reset and begin downloading new application firmware.

If you are downloading a new bootloader, go to the DOWNLOAD BOOTLOADER FIRMWARE section, enter the IP address of the computer running the TFTP server, and click on the Download button. The module should reset and begin downloading new bootloader firmware.

> *NOTE:*
> *The TFTP Server must be on the same IP subnet as the 2572-A module.*
> *NOTE:*
> *Avoid updating the 2572-A while HMI or other clients are attempting to communicate with the module. This will slow the file download considerably and may cause the download process to terminate without completion.*

Firmware Update Process

The update process consists of two phases. In phase one, the firmware files are downloaded from the TFTP server, verified, and stored in the module RAM. If all downloaded firmware files are successfully verified, phase two replaces the current firmware stored in flash with the newly downloaded firmware. This two phase procedure minimizes the possibility of corrupting the existing firmware during the download process.

Phase One

After you click on the download button the module will reset. Once the LED test sequence is complete, the MS LED will begin blinking green. Once the file download from the TFTP server starts the NS LED will illuminate. If you are downloading application firmware, this process will take about 60 seconds. If you are downloading new bootloader code, this should take about 15 seconds.

If phase one does not complete successfully, the application firmware currently stored in flash will be restarted. To alert you of this condition, the MS LED will flash green and red. You should access the event log to determine the cause of the problem, make corrections, and the reinitiate the download process. See the section on Troubleshooting Download Problems

Phase Two

Once the downloaded file has been verified, the firmware stored in flash will be overwritten by the newly downloaded firmware. If you are downloading application firmware this should take about 30 seconds. If you are downloading new bootloader code, this will take only a couple of seconds.

To indicate that the module is updating flash, the MS and NS LEDs will each alternate between green and red after each sector is written. Once the flash has been completely updated, the module will reset and start up with the new firmware.

Once the module has restarted, you should confirm that the desired version of firmware has been loaded by accessing the Module Information web page. The event log will also contain messages that indicate the download completed successfully.

If you should corrupt the existing application firmware by interrupting the flash update, the module will stop with both the MS and NS steady red. To attempt recovery, reset the module. Once reset, the module will attempt to download new application firmware from the same location used the previous time.

Troubleshooting Firmware Update Problems

If you encounter an error in phase one of the download process, you should access the event log to determine the cause of the problems. The table below identifies the messages you may see and indicates potential corrective actions.

Event Log Message	Possible Cause	Corrective Action
Unable to Locate TFTP server	A temporary problem has occurred.	Retry the download procedure
	The IP address of the TFTP server has been entered incorrectly.	Verify that the IP address you entered matches the PC containing the TFTP server. Correct, if necessary, and retry the download.
	The PC containing the TFTP server is offline or not connected to the network.	Ensure the PC is running and connected to the network.
	The PC containing the TFTP server is not on the same subnet as the module. See Appendix D for a further explanation of subnets.	Verify that the IP addresses are on the same subnet. If this is not the case, you must change the IP address of the server or of the module.
No response from TFTP server when requesting command file	The TFTP server is not active	Start the TFTP server
	The IP address that you entered is not the PC containing the TFTP server	Change the IP address to the correct one.
Command file not found	The file is not present.	Ensure that the file is in the root directory of the TFTP server.
	You entered the wrong name for the command file.	The correct name for the 2572-A is ENILDR.CMD
Error Parsing command file	The command file contains invalid records.	Replace all the 2572-A firmware files code in your TFTP Server root directory and retry the download
TFTP timeout during command file download	The PC containing the TFTP server is too busy to keep up.	Retry the operation. If the problem persists use another PC or reduce loading on the current PC.
	Heavy network traffic is causing records to be lost.	Retry the operation. If the problem persists use a less loaded network connection.

Event Log Message	Possible Cause	Corrective Action
No response from TFTP server when requesting sector file	The TFTP server has been closed during file download.	Start the TFTP server and retry the download operation.
Code file for sector n not found	One of the sector files is missing.	Ensure that you replace all the code in your TFTP Server directory with a completely new set of files.
	The module is unable to maintain communications with the TFTP server because HMI and/or PLC clients are attempting to communicate with it during download.	Eliminate the client activity and retry.
Bad code file for sector n	The sector file contains invalid records	Replace all the code in your TFTP Server root directory with a new set of firmware and retry the download process.
Checksum error for sector n	The file was corrupted during download or the file itself contains erroneous data.	Retry the download operation. If the problem persists, replace all the 2572-A firmware files in your TFTP Server root directory with a new set of files and retry the download process.
Invalid version number for sector n	The version number of this file does not match the expected firmware version number. Firmware files from more than one version have been intermixed.	Ensure that you replace all the code in your TFTP Server directory with a completely new set of files.
Hardware Model not valid	The file was corrupted during download or the file itself contains erroneous data.	Retry the download operation. If the problem persists, replace all the 2572-A firmware files in your TFTP Server root directory with a new set of files
	The firmware is not for a 2572-A module	Contact CTI
Hardware Version not valid	The file was corrupted during download or the file itself contains erroneous data.	Retry the download operation. If the problem persists, replace all the 2572-A firmware files in your TFTP Server root directory with a new set of files
	The firmware is not compatible with the version of your 2572-A hardware	Contact CTI
TFTP Timeout during code file download	The PC containing the TFTP server is too busy to keep up.	Retry the operation. If the problem persists use another PC or reduce loading on the current PC.
	Heavy network traffic is causing records to be dropped. This may be due to clients attempting to communicate with the module during the download process.	Retry the operation. If the problem persists, eliminate the client traffic to the module or use a less busy network connection.

HARDWARE SPECIFICATIONS

Ethernet Port:

 1 ea.   RJ-45 style connector ANSI/EIA/TIA – 568-B.2 Category 5E. IEEE 802.3 10BaseT
         and 100BaseTX (half/full duplex). IEEE 802.3 auto-negotiation of speed and duplex
         mode.

Serial Communications Port:

 1 ea.   Male DB9 connector providing a subset of RS-232C DTE electrical interface (TxD,
         RxD, and SG signals only). 1500 VDC isolation (channel to PLC).

Data Rate	1200,2400,9600,19200 Baud (switch selectable)
Data Bits	7
Parity	Odd
Stop Bits	1

LED Indicators:

1 ea.	Module Status (MS)	Bicolor Red/Green
1 ea.	Network Status (NS)	Bicolor Red/Green
1 ea.	Collision (COL)	Yellow
1 ea.	Link Status (LS)	Green
1 ea.	100 Mb Operation (100)	Green
1 ea.	Full Duplex (FDX)	Green
2 ea.	Transmit Data (XMT)	Yellow
2 ea.	Receive Data (RCV)	Yellow

Module Size: Single Wide 505 I/O

Backplane Power Consumption: 2.5 watts @ 5 VDC

Operating Temperature: 0º to 60º C (32º to 185º F)

Storage Temperature: -40º to 85º C (-40º to 185º F)

Humidity: 0% to 95%, non-condensing

LIMITED PRODUCT WARRANTY

CTI warrants that this CTI Industrial Product shall be free from defects in material and workmanship for a period of one (1) year after purchase from CTI or from an authorized CTI Industrial Distributor. This CTI Industrial Product will be newly manufactured from new and/or serviceable used parts which are equal to new in the Product.

Should this CTI Industrial Product fail to be free from defects in material and workmanship at any time during this (1) year warranty period, CTI will repair or replace (at its option) parts or Products found to be defective and shipped prepaid by the customer to a designated CTI service location along with proof of purchase date and associated serial number. Repair parts and replacement Product furnished under this warranty will be on an exchange basis and will be either reconditioned or new. All exchanged parts or Products become the property of CTI. Should any Product or part returned to CTI hereunder be found by CTI to be without defect, CTI will return such Product or part to the customer.

This warranty does not include repair of damage to a part or Product resulting from: failure to provide a suitable environment as specified in applicable Product specifications, or damage caused by an accident, disaster, acts of God, neglect, abuse, misuse, transportation, alterations, attachments, accessories, supplies, non-CTI parts, non-CTI repairs or activities, or to any damage whose proximate cause was utilities or utility like services, or faulty installation or maintenance done by someone other than CTI.

Control Technology Inc. reserves the right to make changes to the Product in order to improve reliability, function, or design in the pursuit of providing the best possible Product. CTI assumes no responsibility for indirect or consequential damages resulting from the use or application of this equipment.

THE WARRANTY SET FORTH ABOVE IN THIS ARTICLE IS THE ONLY WARRANTY CTI GRANTS AND IT IS IN LIEU OF ANY OTHER IMPLIED OR EXPRESSED GUARANTY OR WARRANTY ON CTI PRODUCTS, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR OF FITNESS FOR A PARTICULAR PURPOSE AND IS IN LIEU OF ALL OBLIGATIONS OR LIABILITY OF CTI FOR DAMAGES IN CONNECTION WITH LOSS, DELIVERY, USE OR PERFORMANCE OF CTI PRODUCTS OR INTERRUPTION OF BUSINESS, LOSS OF USE, REVENUE OR PROFIT. IN NO EVENT WILL CTI BE LIABLE FOR SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES.

SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU.

THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH MAY VARY FROM STATE TO STATE.

REPAIR POLICY

In the event that the Product should fail during or after the warranty period, a Return Material Authorization (RMA) number can be requested orally or in writing from CTI main offices. Whether this equipment is in or out of warranty, a Purchase Order number provided to CTI when requesting the RMA number will aid in expediting the repair process. The RMA number that is issued and your Purchase Order number should be referenced on the returning equipment's shipping documentation. Additionally, if the product is under warranty, proof of purchase date and serial number must accompany the returned equipment. The current repair and/or exchange rates can be obtained by contacting CTI's main office at 1-800-537-8398.

When returning any module to CTI, follow proper static control precautions. Keep the module away from polyethylene products, polystyrene products and all other static producing materials. Packing the module in its original conductive bag is the preferred way to control static problems during shipment. Failure to observe static control precautions may void the warranty. For additional information on static control precautions, contact CTI at 1-800-537-8398.

WX / WY Quick Reference

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
MOD STS		NET CFG			LS										HRT BEAT

Module Status Bits — WX1

| Cmd 1 Status Bits | Cmd 2 Status Bits | Cmd 3 Status Bits | Cmd 4 Status Bits | WX2 |

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
CMD Err	PLC Err	CMD Busy	ABORT Busy	CMD Err	PLC Err	CMD Busy	ABORT Busy	CMD Err	PLC Err	CMD Busy	ABORT Busy	CMD Err	PLC Err	CMD Busy	ABORT Busy

| cmd 1 status | cmd 2 status | cmd 3 status | cmd 4 status |

Bit 1 = Reset   Module Control Bits — WY3

| Cmd 1 Control Bits | Cmd 2 Control Bits | Cmd 3 Control Bits | Cmd 4 Control Bits | WY4 |

Cmd 1 V Memory Address of Command Block — WY5

Cmd 2 V Memory Address of Command Block — WY6

Cmd 3 V Memory Address of Command Block — WY7

Cmd 4 V Memory Address of Command Block — WY8

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ERR Ack	CMD Mode	CMD Trig	ABORT Trig	ERR Ack	CMD Mode	CMD Trig	ABORT Trig	ERR Ack	CMD Mode	CMD Trig	ABORT Trig	ERR Ack	CMD Mode	CMD Trig	ABORT Trig

| command 1 | command 2 | command 3 | command 4 |