CTI 2572 Send/Receive Application Example

Application

A CTI 2500 Series or Simatic® 505 PLC is used to update a Siemens® S7 PLC with process information. When the S7 receives the information, it sends status information back to the Simatic® 505 PLC.

Assumptions

- The Simatic® 505 PLC uses the 2572 as a network TCP/IP interface.
- The S7 uses a CP343-1 TCP/IP interface.
- The 2572 will be configured as the Passive partner
- The S7 will be configured as the Active partner
- The IP address of the 2572 is 192.168.1.2 (Dotted hexadecimal is C0.A8.01.02) and is loaded from ladder logic using the Start Network Server command.
- The TSAP for the Simatic® 505 connection endpoint is “PLCA”. This TSAP string is stored at V500 in the Simatic® 505 PLC.
- The IP address of the CP343 interface is 192.168.1.3
- The TSAP for the S7 connection endpoint is “S701”. This TSAP string is stored at V510 in the Simatic® 505 PLC.
- The 2572 will send 100 words of data obtained from V1000 – V1099.
- The S7 will reply with 10 words of status information, which will be written to V1200 – V1209.
- The 2572 module is logged into the PLC at WX1.
- No router is used on the network.

Before the 2572 module can communicate on an Ethernet network, it must first be started as a network server and given network parameters, such as, IP address, port number, etc. Network parameters can be loaded into EEPROM on the module with the utility software, IPSET or with CTIDiag software. The module dipswitches can then be set for Auto Start and the module will automatically start up at power up. Network parameters can also be loaded from the PLC using the **Start Network Server** command. This is the most commonly used method. The main advantage for loading the network parameters from the PLC is that the network information for the 2572 stays with the PLC allowing quick substitution of the module if needed. This application example uses the Start Network Server command to load network parameters to the 2572 module. Refer to the ***SIMATI®C 505 Ethernet TCP/IP Communication Processor User Manual, Chapter 2.4*** for complete information on starting the network server from the PLC.

Active and Passive Partners

Send/Receive requires a point-to-point TCP connection between the communications partners. One partner is responsible for initiating the connection request while the other is responsible for accepting or rejecting the request. The partner responsible for ***initiating*** the request to establish the connection is called the ***Active*** partner. The partner that ***responds*** to the connection request is called the ***Passive*** partner. To establish a peer-to-peer connection one partner must be Active and the other Passive. In this application example, the 2572 is the passive partner and the CP343-1 TCP/IP adapter in the S7 system is the active partner. The CP343-1 is responsible for initiating the connection. The 2572 must initiate an Open Passive command on startup initialization. Once an Open Passive command has been initiated, the 2572 will respond to a connection request from the S7 Active partner.

2572 Command Blocks

Start Network Server Command

Address	Description	Hex	Decimal
V50	Error Word	0000	0
V51	Command Code	0004	4
V52	Connection Number	4B62	19298
V53	Protocol Manager Number	0023	35
V54	Startup Option Bits	0000	0
V55	TCP Keep Alive Interval (0 = default = 60 seconds)	0000	0
V56	IP Address of this Module (High 16 bits) 192 = C0 (hex) 168 = A8 (hex)	C0A8	49320
V57	IP Address of this Module (Low 16 bits) 1 = 01 (hex) 2 = 02 (hex)	0102	258
V58	TCP/UDP Port Number	05E1	1505
V59	IP Address of Default Router (High 16 bits)	0000	0
V60	IP Address of Default Router (Low 16 bits)	0000	0
V61	Max Number of TCP Connections (0 = default = 8)	0000	0
V62	Subnet Mask (High 16 bits) Note: Enter 0 to allow the module to set the correct subnet mask for the IP address class entered in offsets 6 and 7.	0000	0
V63	Subnet Mask (Low 16 bits) Note: Enter 0 to allow the module to set the correct subnet mask for the IP address class entered in offsets 6 and 7.	0000	0
V64-65	Unused	0000	0

Open Passive Connection

Address	Description	Hex	Decimal
V100	Error Word	0000	0
V101	Command Code (Passive connection)	2E02	11778
V102	Connection Number	4B15	19221
V103	Protocol Manager Number	002E	46
V104	IP address of Partner – High 16 bits	C0A8	49320
V105	IP address of Partner – Low 16 bits	0103	259
V106	Flags	0000	0
V107	Length of local TSAP (in bytes)	0004	4
V108	Start V-memory address of local TSAP	01F4	500
V109	Length of remote TSAP (in bytes)	0004	4
V110	Start V-memory address of remote TSAP	01FE	510
V111-115	Unused	0000	0

Local and Remote TSAPs

The local TSAP chosen for the application is '**PLCA**'. This TSAP string is stored in the Simatic® 505 PLC starting at V500 as shown in the table below:

Address	Description	Hex	Decimal
V500	ASCII Characters **P** and **L**	504C	20556
V501	ASCII Characters **C** and **A**	4341	17217

The remote TSAP chosen for the application is '**S701**'. This TSAP string is stored in the Simatic® 505 PLC starting at V510 as shown in the table below:

Address	Description	Hex	Decimal
V510	ASCII Characters **S** and **7**	5337	21303
V511	ASCII Characters **0** and **1**	3031	12337

Send Data Command Block

Address	Description	Hex	Decimal
V140	Error Word	0000	0
V141	Command Code (SEND)	2E03	11779
V142	Connection Number (matches open)	4B15	19221
V143	Command Flags	0000	0
V144	Number of words to transfer	0064	100
V145	Send Block V-memory Address	03E8	1000
V146-155	Reserved	0000	0

Receive Data Command Block

Address	Description	Hex	Decimal
V120	Error Word	0000	0
V121	Command Code (Receive)	2E04	11780
V122	Connection Number (matches open)	4B15	19221
V123	Command Flag	0000	0
V124	Maximum Data Block Size (in words)	000A	10
V125	Receive Block V-memory address	04B0	1200
V126	Command Timeout (0 = default) Max = 60 seconds	0001	1
V127 -135	Reserved	00000	0

Simatic® 505 Logic

This rung looks for the Network Cfg bit (WX1.3) to be high and loads command slot 1 (WY5) with the pointer to the V memory location where the Start Network Server command is located. The Command Control bits (WY4) are cleared and control relays used in logic control are initialized. C19 is set to trigger logic below to initiate a command cycle and start the network server.

```
      !WX1.3  C2    LDC-----------+   LDC-----------+             C1
1     [-] [---]/[---!             !---!             !----------*-(SET )
      !             ! A:WY5       !   ! A:WY4       !          !
      !             ! N=50        !   ! N=0         !          !  C12
      !             !             !   !             !          [-(RST )
      !             +-------------+   +-------------+          !
      !                                                        !  C13
      !                                                        [-(RST )
      !                                                        !
      !                                                        !  C14
      !                                                        [-(RST )
      !                                                        !
      !                                                        !  C15
      !                                                        [-(RST )
      !                                                        !
      !                                                        !  C19
      !                                                        +-(SET )
```

This rung locks out the first rung so that the Start Network Server command is only executed once.

```
      !WX1.3                                                      C2
29    [-] [-----------------------------------------------------(    )
```

When the module turns ON the Command Busy bit (WX2.3), C14 is set and C15 is reset to indicate that a command cycle has started.

```
      !
      !WX2.3                                                      C14
33    [-] [----------------------------------------------------*-(SET )
      !                                                        !
      !                                                        !  C15
      !                                                        +-(RST )
```

When C14 is ON and the module turns OFF Command Busy (WX2.3), C15 is set and C14 is reset to indicate that a command cycle has finished.

```
      ! C14  WX2.3                                                C15
42    [-] [---]/[----------------------------------------------*-(SET )
      !                                                        !
      !                                                        !  C14
      !                                                        +-(RST )
      !
```

Command slot #1 (WY5) is loaded with the pointer to the V memory location where the Open Passive command is located (V100) after the Start Network Server command has been executed, as indicated by C1 and C15 both being ON. The command error word for the Open Passive command (V100) is cleared to zero. C12 is set to indicate that the Open Passive command has been initiated. C1 is reset so that this command is not executed again unless the 2572 has gone through a power cycle or a reset. C15 is reset and C19 is set to initiate the command trigger logic.

```
      ! C1    C15   LDC-----------+   LDC-----------+             C12
71    [-] [---] [-*-!             !---!             !----------*-(SET )
      !             ! A:WY5       !   ! A:V100      !          !
      !             ! N=100       !   ! N=0         !          !  C1
      !             !             !   !             !          [-(RST )
      !             +-------------+   +-------------+          !
      !                                                        !  C15
      !                                                        [-(RST )
      !                                                        !
      !                                                        !  C19
      !                                                        [-(SET )
      !
      !
      !
```

Command Slot #1 (WY5) is loaded with the pointer to the V memory location where the Receive Data command is located (V120) after the Open Passive command has been executed and finished, as indicated by C12 and C15 both being ON. C13 is set which initiates the logic at rungs 130 and 134 continuously.

```
      !
      !    C12   C15      LDC-----------+                         C13
95    [----] [---] [------!             !----------------------*-(SET )
      !                   ! A:WY5       !                      !
      !                   ! N=120       !                      !  C12
      !                   !             !                      [-(RST )
      !                   +-------------+                      !
      !                                                        !  C15
      !                                                        +-(RST )
```

Command Slot #2 (WY6) is loaded with the pointer to the V memory location where the Send Data Command is located (V140). Since the 2572 can process commands concurrently on different command slots, we are using command slot #2 for the Send Data command. As long as the input is true (C30 is OFF and C13 is ON) the command will execute continuously. The command trigger bits for Command Slot #2 (WY4.6 and WY4.7) are turned ON and will remain ON until the module turns ON the Command Slot #2 Busy bit (WX2.7). As soon the Command Busy bit goes low again, another command cycle will start.

```
      !
      !    C13      LDC-----------+  WX2.7  LDC-----------+      WY4.6
110   [----] [------!             !-*-]/[---!             !----*-(    )
      !             ! A:WY6       ! !       ! A:V140      !    !
      !             ! N=140       ! !       ! N=0         !    ! WY4.7
      !             !             ! !       !             !    +-(    )
      !             +-------------+ !       +-------------+
      !WY4.7                        !
      [-] [-------------------------+
      !
```

Rungs 130 and 134 control command processing of the Receive Data Command on Command Slot #1. As long as C13 is ON, indicating that the pointer to the Receive Data command has been loaded, the command will execute continuously. The command error word for the Receive Data command (V120) is cleared to zero each time the command is executed.

```
      ! C13                                                       C19
130   [-] [------------------------------------------------------(SET )
      !
      ! C19  WX2.3  LDC-----------+                               WY4.2
134   [-] [-*-]/[---!             !----------------------------*-(    )
      !     !       ! A:V120      !                            !
      !WY4.3!       ! N=0         !                            ! WY4.3
      [-] [-+       !             !                            [-(    )
      !             +-------------+                            !
      !                                                        !  C19
      !                                                        +-(RST )
      !
```

Rung 153 checks if the command error word for the Open Passive command contains an error. If it does, the error word is moved to V399 where it is stored. This needs to be done because the error word is cleared to zero when the command is executed. This way V399 will always contain the last error code that was reported.

```
      !  V100 +0      MOVW----------+                             C23
153   [--]<>  INT[----!             !----------------------------(    )
      !               ! A:V100      !
      !               ! B:V399      !
      !               ! N=1         !
      !               +-------------+
```

Rung #162 examines the Command Error Bit for Command Slot #1 (WX2.1) and, if ON, moves the error code word of the Receive Data Command (V120) to V400 for storage. V400 will always contain the last error reported. The Error Acknowledge Bit for Command Slot 1 (WY4.1) is then turned ON to acknowledge the error. When the 2572 module sees the Error Acknowledge bit ON it will turn OFF the Command Error Bit (WX2.1). This must be done before another command cycle can be executed on the command slot.

```
      !WX2.1  MOVW----------+                                     WY4.1
162   [-] [---!             !------------------------------------(    )
      !       ! A:V120      !
      !       ! B:V400      !
      !       ! N=1         !
      !       +-------------+
```

Rung #172 performs the same function as Rung #162 only for Command Slot #2 where the Send Data command is being executed. The error code word for the Send Data command (V140) is moved to V401 for storage.

```
      !WX2.5  MOVW----------+                                     WY4.5
172   [-] [---!             !------------------------------------(    )
      !       ! A:V140      !
      !       ! B:V401      !
      !       ! N=1         !
      !       +-------------+
```

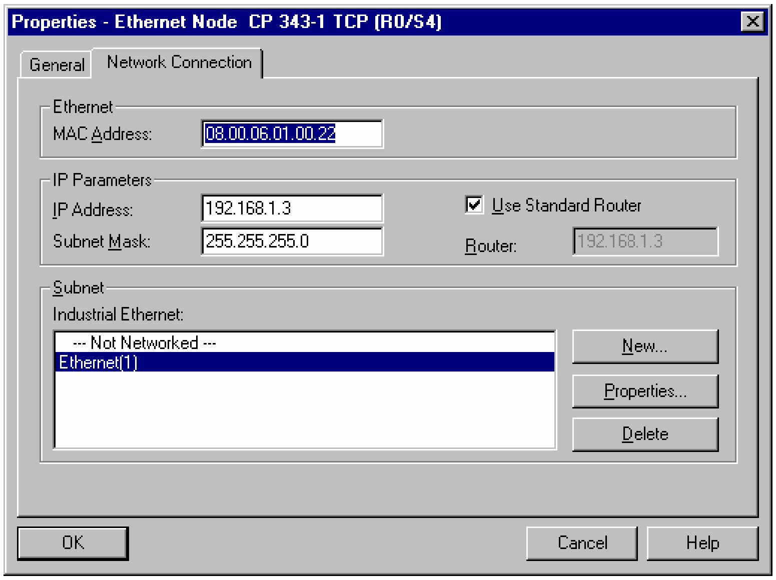
S7 Configuration

Note:
This application note assumes you are familiar with the S7 system, including installing and configuring the CP343-1 Ethernet TCP/IP module, and using the Step 7 software develop application programs. If you have questions about the S7 and related components, please contact your Siemens technical representative.

Using the Step7 configuration program, create an Ethernet subnet consisting of the S7 PLC with a CP343-1 module and an “Other” Station named 2572. Since there is no router on this network, set the subnet default to “No Router”. Then, selecting “Standard Router” under the individual node network properties will automatically select no router.

Configuring the CP343 Ethernet Module

Set the Network Connection properties of the CP343-1 module as shown below. The MAC address is not used in TCP/IP connections, but some versions of Step 7 may require an entry. In this case you may enter any arbitrary value that Step 7 will accept.



Properties - Ethernet Node CP 343-1 TCP (R0/S4)

Ethernet

MAC Address: 08.00.06.01.00.22

IP Parameters

IP Address: 192.168.1.3

Subnet Mask: 255.255.255.0

☑ Use Standard Router

Router: 192.168.1.3

Subnet

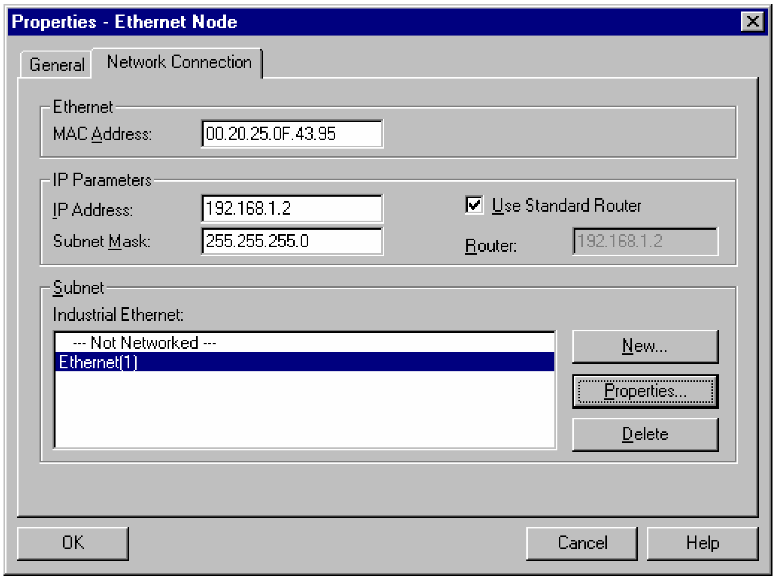
Industrial Ethernet:

--- Not Networked ---

Ethernet(1)

Configuring the Other Station (2572)

Enter the following Network Connection properties for the 2572 module. Again, the MAC ID is not used by TCP/IP, but some versions of Step 7 may require the entry. You may any arbitrary value acceptable by Step 7.



Properties - Ethernet Node

Ethernet

MAC Address: 00.20.25.0F.43.95

IP Parameters

IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

☑ Use Standard Router

Router: 192.168.1.2

Subnet

Industrial Ethernet:

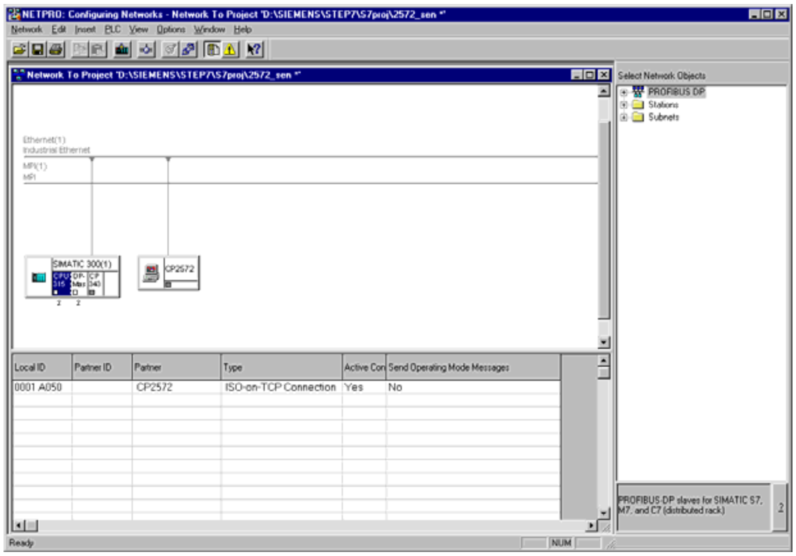
--- Not Networked ---

Ethernet(1)

Configuring the ISO on TCP Connection

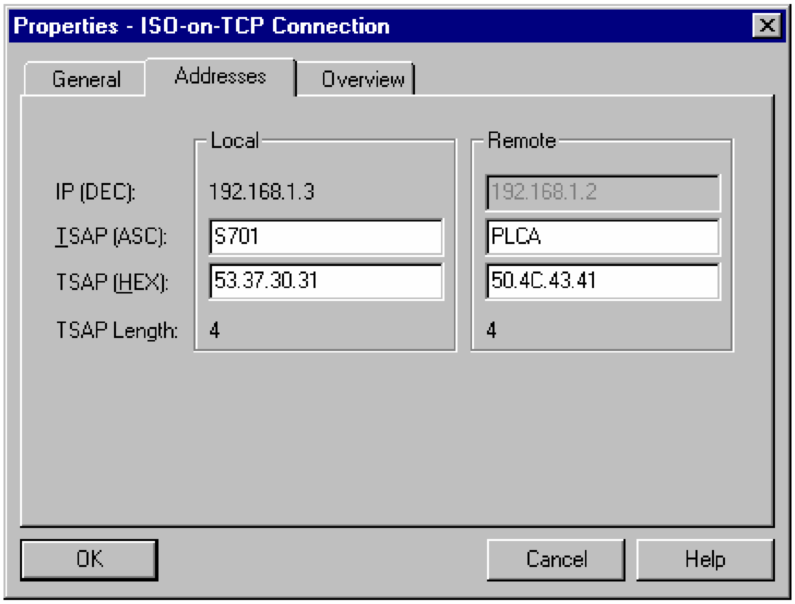
Create a new connection to the 2572 as shown below.

Note: Configure the 2572 as the Passive partner by changing the Yes to NO under the “Active Con” column below.


NETPRO: Configuring Networks - Network To Project 'D:\SIEMENS\STEP7\S7proj\2572_sen *'
Network Edit Insert PLC View Options Window Help
Network To Project 'D:\SIEMENS\STEP7\S7proj\2572_sen *'
Select Network Objects
PROFIBUS DP
Stations
Subnets
Ethernet(1)
Industrial Ethernet
MPI(1)
MPI
SIMATIC 300(1)
CPU 315
DP-Mas
CP 343
CP2572
PROFIBUS-DP slaves for SIMATIC S7, M7, and C7 (distributed rack)
Ready
NUM

Local ID	Partner ID	Partner	Type	Active Con	Send Operating Mode Messages
0001 A050		CP2572	ISO-on-TCP Connection	Yes	No

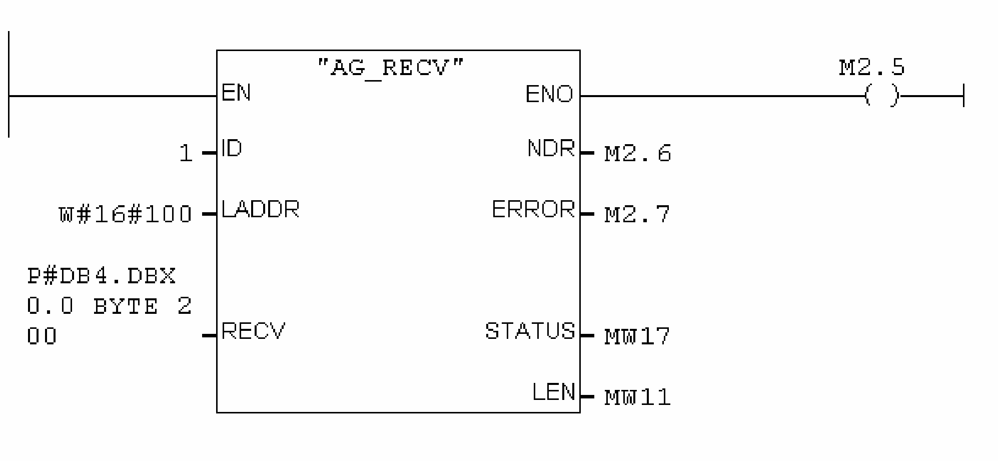
Enter the following TSAP information.



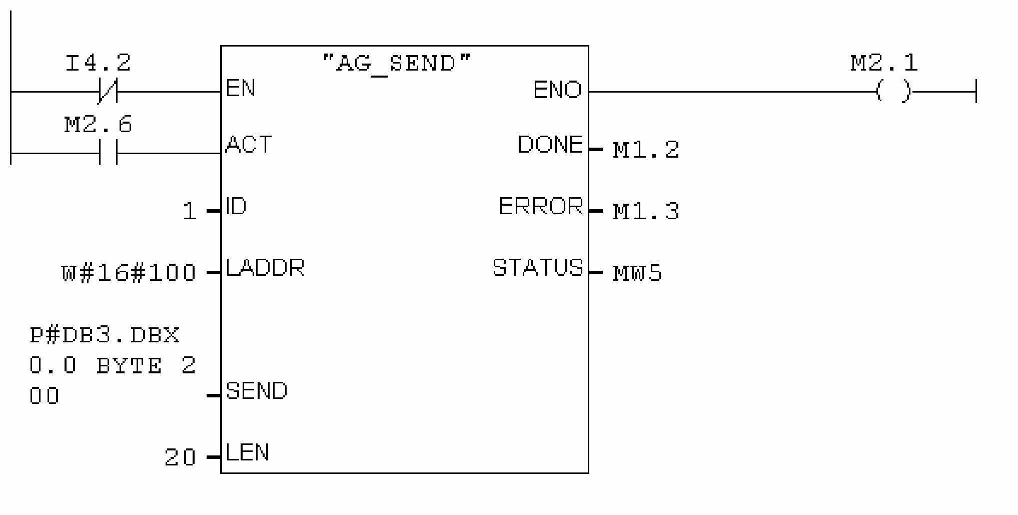
	Local	Remote
IP (DEC):	192.168.1.3	192.168.1.2
TSAP (ASC):	S701	PLCA
TSAP (HEX):	53.37.30.31	50.4C.43.41
TSAP Length:	4	4

S7 Logic

The following S7 Function Block (FC6) receives data from the 2572 module. ID must correspond to the "Connection ID" in the S7 Ethernet setup. LADDR must correspond to the value shown in "Block Parameters". RECV is memory block where the S7 writes the received data. Your S7 logic should execute this function block on a regular basis to check for input from the Simatic® 505 PLC.



The following S7 Function Block (FC5) sends data to the Simatic® 505 PLC. ID must correspond to the "Connection ID" in the S7 Ethernet setup. LADDR must correspond to the value shown in "Block Parameters". SEND is memory block where the S7 obtains data to be transmitted. Your S7 logic should execute this block after receiving a message from the Simatic® 505 PLC.



Error Codes

The following codes may be returned by this protocol manager in the Command Block error word.

HEX	DEC	Description	Possible Corrective Action
2E01	11777	TSAP length too long(>10 bytes)	Ensure the entry is correct
2E02	11778	Out-of-range connection number	Use a number between 19221 and 19228
2E03	11779	Local TSAP specified is already in use	Select another TSAP name
2E04	11780	Remote TSAP specified is already in use for the remote IP address.	Select another TSAP name. You may need to set up another TSAP in the partner PLC.
2E05	11781	Local TSAP Length = 0	Correct the command block entry.
2E06	11782	Local TSAP V memory address = 0	Correct the command block entry.
2E07	11783	Remote TSAP Length = 0	Correct the command block entry.
2E08	11784	Remote TSAP V memory address = 0	Correct the command block entry.
2E09	11785	Local TSAP V memory address exceeds PLC maximum	Correct the command block entry.
2E0A	11786	Remote TSAP V memory address exceeds PLC maximum	Correct the command block entry.
2E0B	11787	Duplicate attempt to create a Passive connection	Check the logic used to trigger the command block. You are probably triggering the command more than once.
2E0C	11788	Reserved	Not Used
2E0D	11790	Attempted to send packet with no data (word count = 0)	Correct the command block entry.
2E0E	11791	V memory address in SEND or RECEIVE command = 0	Correct the command block entry.
2E0F	11792	Number of words to transfer exceeds 512	Correct the command block entry.
2E10	11793	Remote IP address is the same as the local 2572 IP address	Correct the command block entry.
2E20	11808	Connection lost: TCP Keep Alive timeout	Retry the Send or Receive command. The module will automatically attempt to re-establish the connection. If the problem persists, check the network and partner.
2E21	11809	Partner PLC explicitly closed the connection.	Partner PLC must open a new connection before you can continue.
2E22	11810	The specified partner supports ISO on TCP (Port 102) but Open connection request was denied.	This error is probably due to an incorrect TSAP entry.
2E23	11811	Open Active connection failed to open a TCP connection on port 102 at the specified IP address. The PLC address exists but the target does not support ISO on TCP.	Ensure that you have specified the correct IP address. If the target is a Simatic® 505 PLC using a 2572 module, ensure that the firmware supports the Send/Receive feature. *Note: Port 102 availability can be verified by using a Windows Telnet application. Configure telnet to access port 102 rather than the default telnet port, and then attempt to connect to the remote IP. If the message box "connect Failed" does not appear, the port 102 is available on the remote machine*.
2E24	11812	A RECEIVE command was issued on a Passive connection that has not yet been	Correct the application logic.

HEX	DEC	Description	Possible Corrective Action
		established.	
2E25	11813	A SEND command was issued on a Passive connection that has not yet been established.	Correct the application logic.
2E26	11814	Remote system attempted to open a connection on a TSAP locally configured as an Active connection.	Correct the application logic.
2E27	11815	Logic attempted to create an active TCP connection when the TCP connection is already established.	Correct the application logic.
2E28	11816	Connection has been lost. Protocol manager is attempting to re-establish the connection.	Continue to retry. If the problem persists, check the network and partner PLC.
2E30	11824	A command is already in process for this connection number.	Correct the application logic.
2E31	11825	Reserved	Not Used in this release
2E32	11826	No data available to Receive command. Occurs when timeout value of 0 is specified and no data is currently available to be read.	Retry the command. If the problem persists check the partner PLC.
2E33	11827	Error writing to local V memory during Receive command	Retry the command. If the problem persists check the PLC I/O configuration and applicable Command Block entries.
2E34	11828	Error reading from V memory during Send command	Retry the command. If the problem persists check the PLC I/O configuration and applicable Command Block entries.
2E35	11829	The partner controller is not accepting additional data. TCP window size has been set to 0 by the partner.	Ensure that the partner controller is running logic (in Run mode). Reduce the rate at which messages are sent to the partner.
2E40	11840	Incoming packet data length is 0.	Check partner PLC configuration.
2E41	11841	Incoming packet data length is longer than the data length specified in the command block.	This is a warning message that you can use in your application logic. You may choose to ignore the error and use the truncated data.
2E64 - 2E96	11876 - 11926	System Errors.	Contact CTI.
2E97	11927	Invalid command code.	Correct Command Block Entry.
2E98 - 2EFF	11928 - 12031	System errors	Contact CTI.

0.1. Diagnostic Statistics

Diagnostic Statistics may be a valuable tool for troubleshooting problems. The following diagnostic information may be obtained from the 2572 module using the CTIDiag application (version 1.1 and above).

Statistic	**Comments**
These statistics are kept per connection instance	
Instance Identifier	Connection Number
Local TSAP (1st 10 bytes)	
Remote TSAP (1st 10 bytes)	
Connection Type	0x0000 = Undefined (not instantiated) 0x0001 = Active 0x0002 = Passive
Count of Message Send Attempts	Attempts by logic to send
Count of Messages Sent	Successfully transmitted messages
Count of Messages Received	Buffered at Module
Count of Messages Read by PLC	Read by PLC
Count of Message Read – Empty Buffer	Buffer Reads with no data present
Current Connection Status	0x0000 = Undefined 0x0001 = Not Connected 0x0002 = Connected 0x0003 = Attempting to Connect 0x0004 = Waiting on Connection 0x0005 = Processing Connection Request 0xFFFF = Unknown
Count of Connection Attempts	Incremented each time an attempt to connect is initiated or received (both success and non-success are counted).
Count of Rejected Connections	Incremented each time a connection attempt is explicitly rejected.
Count of Closed Connections	Incremented each time an explicit TCP close is initiated or received
Count of KeepAlive Timeouts	Incremented each time a connection is closed because of KeepAlive timeout.