Cat. No. W465-E1-16

SYSMAC CS and CJ Series
CS1W-EIP21/EIP21S (100Base-TX)
CJ1W-EIP21/EIP21S (100Base-TX)
CJ2H-CPU6□-EIP (100Base-TX)
CJ2M-CPU3□ (100Base-TX/10Base-T)
CJ3M-CPU3□ (100BASE-TX)

EtherNet/IP™ Units

OPERATION MANUAL

OMRON

© OMRON, 2007

NOTE

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, mechanical, electronic, photocopying, recording, or otherwise, without the prior written permission of OMRON.

No patent liability is assumed with respect to the use of the information contained herein. Moreover, because OMRON is constantly striving to improve its high-quality products, the information contained in this manual is subject to change without notice. Every precaution has been taken in the preparation of this manual. Nevertheless, OMRON assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained in this publication.

Trademarks

- Sysmac and SYSMAC are trademarks or registered trademarks of OMRON Corporation in Japan and other countries for OMRON factory automation products.
- CX-One is a registered trademark for Programming Software made by OMRON Corporation.
- Microsoft, Windows, Excel, Visual Basic, and Microsoft Edge are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
- EtherCAT® is a registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany.
- ODVA, CIP, CompoNet, DeviceNet, EtherNet/IP, and QuickConnect are trademarks of ODVA.
- The SD and SDHC logos are trademarks of SD-3C, LLC.

Other company names and product names in this document are the trademarks or registered trademarks of their respective companies.

Copyrights

- Microsoft product screen shots used with permission from Microsoft.
- This product incorporates certain third party software. The license and copyright information associated with this software is available at https://www.fa.omron.co.jp/product/tool/nx-info/index_en.html, https://www.fa.omron.co.jp/product/tool/cj-info/index_en.html.

CS1W-EIP21/EIP21S (100Base-TX)
CJ1W-EIP21/EIP21S (100Base-TX)
CJ2H-CPU6□-EIP (100Base-TX)
CJ2M-CPU3□ (100Base-TX)
CJ3M-CPU3□ (100BASE-TX)
EtherNet/IP Units

Operation Manual

Revised October 2026

Notice:

OMRON products are manufactured for use according to proper procedures by a qualified operator and only for the purposes described in this manual.

The following conventions are used to indicate and classify precautions in this manual. Always heed the information provided with them. Failure to heed precautions can result in injury to people or damage to property.

⚠DANGER Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. Additionally, there may be severe property damage.

⚠WARNING Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury. Additionally, there may be severe property damage.

⚠Caution Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury, or property damage.

OMRON Product References

All OMRON products are capitalized in this manual. The word “Unit” is also capitalized when it refers to an OMRON product, regardless of whether or not it appears in the proper name of the product.

The abbreviation “Ch,” which appears in some displays and on some OMRON products, often means “word” and is abbreviated “Wd” in documentation in this sense.

The abbreviation “PLC” means Programmable Controller. “PC” is used, however, in some Programming Device displays to mean Programmable Controller.

Visual Aids

The following headings appear in the left column of the manual to help you locate different types of information.

Note Indicates information of particular interest for efficient and convenient operation of the product.

1,2,3... 1. Indicates lists of one sort or another, such as procedures, checklists, etc.

TABLE OF CONTENTS

PRECAUTIONS xxvii

1 Intended Audience xxviii
2 General Precautions xxviii
3 Safety Precautions xxix
4 Operating Environment Precautions xxxii
5 Application Precautions xxxii
6 Conformance to EMC and Electrical Safety Regulations xxxv
7 Software Licenses and Copyrights xxxv

SECTION 1
Overview of EtherNet/IP 1

1-1 EtherNet/IP Unit Features 2
1-2 Devices Required for Constructing a Network 5
1-3 Support Software Required to Construct a Network 5
1-4 Communications Services Overview 7
1-5 Network Configurator Overview 13

SECTION 2
Unit Specifications 15

2-1 EtherNet/IP Unit and Built-in EtherNet/IP Port Specifications 16
2-2 Nomenclature and Functions 31
2-3 Selecting the Network Devices 39

SECTION 3
Installation and Initial Setup 43

3-1 Overview Initial Setup Procedures 44
3-2 Switch Settings 47
3-3 Mounting to a PLC 49
3-4 Network Installation 52
3-5 Connecting to the Network 56
3-6 Creating I/O Tables 58
3-7 Setting the Local IP Address 63
3-8 TCP/IP and Link Settings 66
3-9 Tag Data Link Parameters 74
3-10 User Authentication Settings 78
3-11 Other Parameters 79
3-12 Communications Test 90

SECTION 4
Memory Allocations 93

4-1 Overview of Memory Allocated to the EtherNet/IP Unit 94
4-2 CIO Area Allocations 96

TABLE OF CONTENTS

4-3 DM Area Allocations 114
4-4 User Settings Area 117
4-5 Auxiliary Area Data 120

SECTION 5
Determining IP Addresses 123
5-1 IP Addresses. 124
5-2 IP Addresses in FINS Communications 126
5-3 Private and Global Addresses 138

SECTION 6
Tag Data Link Functions. 143
6-1 Overview of Tag Data Links 144
6-2 Setting Tag Data Links 153
6-3 Ladder Programming with Tag Data Links 220
6-4 QuickConnect 225

SECTION 7
Message Communications Functions. 227
7-1 Overview. 228
7-2 FINS Message Communications 230
7-3 Explicit Message Communications. 232
7-4 Message Communications Specifications 233
7-5 Message Communications Error Indications 234
7-6 Message Communications Errors 235

SECTION 8
FINS Communications 237
8-1 Overview of FINS Communications 238
8-2 FINS/UDP Method 240
8-3 FINS/TCP Method 242
8-4 Routing Tables 247
8-5 Using FINS Applications 251
8-6 Communicating between OMRON PLCs 260
8-7 Precautions on High Traffic in FINS Communications 272

SECTION 9
Message Communications. 273
9-1 Sending Explicit Messages. 274
9-2 Receiving Explicit Messages 287

TABLE OF CONTENTS

SECTION 10
Communications Performance and Communications Load 305

10-1 Communications System 306
10-2 Adjusting the Communications Load 313
10-3 I/O Response Time in Tag Data Links 328
10-4 Message Service Transmission Delay 337

SECTION 11
FTP Server 345

11-1 Overview and Specifications 346
11-2 FTP Server Function Details. 347
11-3 Using the FTP Server Function 349
11-4 FTP Server Application Example 351
11-5 Using FTP Commands 353
11-6 Checking FTP Status 359
11-7 Using File Memory 360
11-8 FTP File Transfer Time 365
11-9 Host Computer Application Example 366

SECTION 12
Automatic Clock Adjustment Function 369

12-1 Automatic Clock Adjustment. 370
12-2 Using the Automatic Clock Adjustment Function 371
12-3 Automatic Clock Adjustment Switch 374
12-4 Automatic Clock Adjustment Error Processing 374

SECTION 13
Security Functions 377

13-1 Overview of Security Functions 378
13-2 Secure Communications 380
13-3 User Authentication 385
13-4 Opening and Closing the Port 403
13-5 IP Packet Filtering. 408
13-6 Operation Log. 415
13-7 General Security Use Cases 424
13-8 Protective Measures to Prevent Security Threats 427

SECTION 14
Socket Services. 429

14-1 Overview of Socket Services 431
14-2 Overview of Socket Communications from Ethernet Units. 434

TABLE OF CONTENTS

14-3 Protocol Overview 435
14-4 Socket Service Function Guide 438
14-5 Using Socket Services by Manipulating Dedicated Control Bits 442
14-6 Using Socket Services with CMND/CMND2 465
14-7 Details on the Socket Service Using with Function Block 484
14-8 Precautions in Using Socket Services 488

SECTION 15
Modbus Server Function 493
15-1 Modbus Server Function Overview 494
15-2 Modbus Server Settings 496
15-3 Example of Using the Modbus Server 498
15-4 Modbus Command Response Details 500

SECTION 16
Modbus Client Function 509
16-1 Modbus Client Function Overview 510
16-2 Example of Using the Modbus Server 512

SECTION 17
Maintenance and Unit Replacement 515
17-1 Maintenance and Replacement 516
17-2 Simple Backup Function 517
17-3 Using the Backup Tool 522
17-4 Replacing Target Nodes during Communications 523
17-5 Unit Initialization 526

SECTION 18
Troubleshooting and Error Processing 527
18-1 Checking Status with the Network Configurator 528
18-2 Using the LED Indicators and Display for Troubleshooting 535
18-3 Connection Status Codes and Error Processing 548
18-4 Error Log Function 554
18-5 Troubleshooting 559
18-6 Troubleshooting with FINS Response Codes 572
18-7 What to Do If Communications Are Not Possible Due to Security Functions 576

A
CS/CJ-series Ethernet Unit Function Comparison 605

B
Ethernet Network Parameters 607

C
TCP Status Transitions 609

D

TABLE OF CONTENTS

CIP Message Communications 611
E
FINS Commands Addressed to EtherNet/IP Units or Built-in EtherNet/IP Ports 621
F
EDS File Management 671
G
Precautions for Using Windows XP or Later Windows OS 675
H
Setting Example for Using Tag Data Links with the CJ2M-CPU3□ 679
I
IP Packet Filter Settings 681
J
Security Use Cases 685
K
Tag Data Link Settings with Generic Devices 689
L
Function Blonk for Socket Service 695
M
Function Block for Modbus Client 719

Index 743

Revision History 753

TABLE OF CONTENTS

About this Manual:

This manual describes the operation of the CS/CJ-series EtherNet/IP Units and the built-in EtherNet/IP ports on a CJ2/CJ3 CPU Unit for constructing applications and includes the sections described below.

Please read this manual carefully and be sure you understand the information provided before attempting to install or operate the EtherNet/IP Unit or built-in EtherNet/IP port. Be sure to read the precautions provided in the following section.

Precautions provides general precautions for using the CS/CJ-series EtherNet/IP Units and built-in EtherNet/IP ports.

Section 1 introduces the functions and protocols used in EtherNet/IP Unit or built-in EtherNet/IP port communications services.

Section 2 provides the specifications of EtherNet/IP Units and introduces recommended network configuration devices.

Section 3 explains how to install and make the initial settings required for operation of the EtherNet/IP Unit or built-in EtherNet/IP port.

Section 4 describes the words allocated in the CIO Area and the DM Area for EtherNet/IP Units or built-in EtherNet/IP ports.

Section 5 explains how to manage and use IP addresses.

Section 6 describes tag data link functions and related Network Configurator operations.

Section 7 describes message communications using FINS messages and explicit messages.

Section 8 provides information on communicating on EtherNet/IP Systems and interconnected networks using FINS commands. The information provided in the section deals only with FINS communications in reference to EtherNet/IP Units or built-in EtherNet/IP ports.

Section 9 describes message communications using FINS commands sent from the ladder program in the CPU Unit of the PLC.

Section 10 describes the communications performance in an EtherNet/IP network, and shows how to estimate the I/O response times and transmission delays.

Section 11 describes the functions provided by the FTP server.

Section 12 provides an overview of the automatic clock adjustment function, including details on specifications, required settings, operations from CX-Programmer, and troubleshooting.

Section 13 describes the security functions provided by CS1W/CJ1W-EIP21S EtherNet/IP Units and CJ3M-CPU3□ built-in EtherNet/IP port.

Section 14 describes the functionality provided by the Ethernet Unit via the socket services.

Section 15 describes cleaning, inspection, and Unit replacement procedures, as well as the Simple Backup Function.

Section 16 describes error processing, periodic maintenance operations, and troubleshooting procedures needed to keep the EtherNet/IP network operating properly. We recommend reading through the error processing procedures before operation so that operating errors can be identified and corrected more quickly.

Appendices provide information on EtherNet/IP network parameters, the buffer configuration, TCP status transitions, ASCII characters, maintenance, and inspections.

Relevant Manuals

The following table lists manuals that contain information relevant to EtherNet/IP Units or built-in EtherNet/IP ports.

Manual number	Model	Name	Contents
W465	CS1W-EIP21 CJ1W-EIP21 CJ2H-CPU6□-EIP CJ2M-CPU3□ CJ3M-CPU3□ CS1W-EIP21S CJ1W-EIP21S	EtherNet/IP™ Units Operation Manual (this manual)	Provides information on operating and installing EtherNet/IP Units, including details on basic settings, tag data links, and FINS communications. Refer to the *Communications Commands Reference Manual* (W342) for details on FINS commands that can be sent to CS-series and CJ-series CPU Units when using the FINS communications service. Refer to the *Ethernet Units Operation Manual Construction of Applications* (W421) for details on constructing host applications that use FINS communications.
W420	CS1W-ETN21 CJ1W-ETN21	Ethernet Units Operation Manual Construction of Networks	Provides information on operating and installing 100Base-TX Ethernet Units, including details on basic settings and FINS communications. Refer to the *Communications Commands Reference Manual* (W342) for details on FINS commands that can be sent to CS-series and CJ-series CPU Units when using the FINS communications service.
W421	CS1W-ETN21 CJ1W-ETN21	Ethernet Units Operation Manual Construction of Applications	Provides information on constructing host applications for 100Base-TX Ethernet Units, including functions for sending/receiving mail, socket service, automatic clock adjustment, FTP server functions, and FINS communications.
W495	CJ1W-EIP21 CJ1W-EIP21S	CJ-series EtherNet/IP™ Units Operation Manual for NJ-series CPU Unit	Information on using an EtherNet/IP Unit that is connected to an NJ-series CPU Unit is provided. Information is provided on the basic setup, tag data links, and other features. Use this manual together with the *NJ-series CPU Unit Hardware User's Manual* (Cat. No. W500) and *NJ/NX-series CPU Unit Software User's Manual* (Cat. No. W501).
W342	CS1G/H-CPU□□-EV1 CS1G/H-CPU□□H CS1D-CPU□□H CS1D-CPU□□S CJ1H-CPU□□H-R CJ1G-CPU□□ CJ1M-CPU□□ CJ1G-CPU□□P CJ1G/H-CPU□□H CJ3M-CPU3□ CJ2H-CPU6□-EIP CJ2H-CPU6□ CJ2M-CPU□□ CS1W-SCU□□-V1 CS1W-SCB□□-V1 CJ1W-SCU□□-V1 CP1H-X□□□□-□ CP1H-XA□□□□-□ CP1H-Y□□□□-□ CP1L-M/L□□□-□ CP1E-E□□D□-□ CP1E-N□□D□-□ NSJ□-□□□□(B)-G5D NSJ□-□□□□(B)-M3D	Communications Commands Reference Manual	Describes the C-series (Host Link) and FINS communications commands used when sending communications commands to CS-series, CJ-series, CP-series, and SYSMAC One NSJ-series CPU Units.

Manual number	Model	Name	Contents
W472	CJ3M-CPU3□ CJ2H-CPU6□-EIP CJ2H-CPU6□ CJ2M-CPU□□	CJ-series CJ2/CJ3 CPU Unit Hardware User's Manual	Provides hardware information for the CJ2/CJ3 CPU Units. Information is included on features, system configuration, component names, component functions, installation, setting procedures, and troubleshooting. Use together with the *CJ-series CJ2*/CJ3 *CPU Unit Software User's Manual* (W473).
W473	CJ3M-CPU3□ CJ2H-CPU6□-EIP CJ2H-CPU6□ CJ2M-CPU□□	CJ-series CJ2/CJ3 CPU Unit Software User's Manual	Provides software information for the CJ2/CJ3 CPU Units. Information is included on CPU Unit operation, internal memory, programming, setting procedures, and CPU Unit functions. Use together with the *CJ-series CJ2*/CJ3 *CPU Unit Hardware User's Manual* (W472).
W664	CJ3M-CPU□□	CJ-series CJ3 CPU Unit Hardware User's Manual	Provides software information for the CJ3 CPU Units. Information is included on CPU Unit operation, internal memory, programming, setting procedures, CPU Unit functions, and remedies for errors. Use together with the CJ-series CJ2/CJ3 CPU Unit Software User's Manual (W473).
W474	CJ3M-CPU3□ CJ2H-CPU6□-EIP CJ2H-CPU6□ CJ2M-CPU□□ CJ1G/H-CPU□□H CS1G/H-CPU□□-EV1 CS1D-CPU□□H CS1D-CPU□□S CJ1H-CPU□□H-R CJ1G/H-CPU□□H CJ1G-CPU□□P CJ1M-CPU□□ CJ1G-CPU□□ NSJ□-□□□□(B)-G5D NSJ□-□□□□(B)-M3D	Programmable Controllers Instructions Reference Manual	Provides detailed descriptions of the instructions. When programming, use this manual together with the manuals for your CPU Unit.
W339	CS1G/H-CPU□□H	Programmable Controllers Operation Manual	Provides an outline of, and describes the design, installation, maintenance, and other basic operations for the CS-series PLCs. Information is also included on features, system configuration, wiring, I/O memory allocations, and troubleshooting. Use together with the *Programmable Controllers Programming Manual* (W394).
W393	CJ1H-CPU□□H-R CJ1G/H-CPU□□H CJ1G-CPU□□P CJ1G-CPU□□ CJ1M-CPU□□	Programmable Controllers Operation Manual	Provides an outline of, and describes the design, installation, maintenance, and other basic operations for the CJ-series PLCs. Information is also included on features, system configuration, wiring, I/O memory allocations, and troubleshooting. Use together with the *Programmable Controllers Programming Manual* (W394).
W394	CS1G/H-CPU□□H CS1G/H-CPU□□-V1 CS1D-CPU□□HA/H CS1D-CPU□□SA/S CS1D-CPU□□P CJ1H-CPU□□H-R CJ1G/H-CPU□□H CJ1G-CPU□□P CJ1M-CPU□□ CJ1G-CPU□□ NSJ□-□□□□(B)-G5D NSJ□-□□□□(B)-M3D	Programmable Controllers Programming Manual	Describes programming, tasks, file memory, and other functions for the CS-series, CJ-series, and NS-J-series PLCs. Use together with the *Programmable Controllers Operation Manual* (W339 for CS-series PLCs and W393 for CJ-series PLCs).

Manual number	Model	Name	Contents
W450	CP1H-X40D□-□ CP1H-XA40D□-□ CP1H-Y20DT-D	CPU Unit Operation Manual	Provides hardware information for the CP1H CPU Units. Information is included on features, system configuration, component names, component functions, installation, setting procedures, and troubleshooting.
W451	CP1H-X40D□-□ CP1H-XA40D□-□ CP1H-Y20DT-D CP1L-L10D□-□ CP1L-L14D□-□ CP1L-L20D□-□ CP1L-M30D□-□ CP1L-M40D□-□ CP1L-M60D□-□	CPU Unit Programming Manual	Describes programming, tasks, file memory, and other functions for the CP1-series.
W463	CXONE-AL□□C-V4 CXONE-AL□□D-V4 CXONE-LT□□C-V4	CX-One Setup Manual	Describes the setup procedures for the CX-One. Information is also provided on the operating environment for the CX-One.
W446	CXONE-AL□□C-V4 CXONE-AL□□D-V4	CX-Programmer Operation Manual	Provides information on how to use the CX-Programmer, a Windows-based programming device. Use together with the *Programmable Controllers Operation Manual* (W339 for CS-series PLCs and W393 for CJ-series PLCs), *Programmable Controllers Programming Manual* (W394) and the *Programmable Controllers Instructions Reference Manual* (W474) to perform programming.
W464	CXONE-AL□□C-V4 CXONE-AL□□D-V4	CS/CJ/CP/NSJ-series CX-Integrator Ver. 2.□ Operation Manual	Describes the operating procedures of the CX-Integrator that can be used to set up and monitor networks.

⚠ **WARNING** Failure to read and understand the information provided in this manual may result in personal injury or death, damage to the product, or product failure. Please read each section in its entirety and be sure you understand the information provided in the section and related sections before attempting any of the procedures or operations given.

Terms and Conditions Agreement

Warranty, Limitations of Liability

Warranties

- **Exclusive Warranty**

Omron's exclusive warranty is that the Products will be free from defects in materials and workmanship for a period of twelve months from the date of sale by Omron (or such other period expressed in writing by Omron). Omron disclaims all other warranties, express or implied.

- **Limitations**

OMRON MAKES NO WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, ABOUT NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE PRODUCTS. BUYER ACKNOWLEDGES THAT IT ALONE HAS DETERMINED THAT THE PRODUCTS WILL SUITABLY MEET THE REQUIREMENTS OF THEIR INTENDED USE.

Omron further disclaims all warranties and responsibility of any type for claims or expenses based on infringement by the Products or otherwise of any intellectual property right.

- **Buyer Remedy**

Omron's sole obligation hereunder shall be, at Omron's election, to (i) replace (in the form originally shipped with Buyer responsible for labor charges for removal or replacement thereof) the non-complying Product, (ii) repair the non-complying Product, or (iii) repay or credit Buyer an amount equal to the purchase price of the non-complying Product; provided that in no event shall Omron be responsible for warranty, repair, indemnity or any other claims or expenses regarding the Products unless Omron's analysis confirms that the Products were properly handled, stored, installed and maintained and not subject to contamination, abuse, misuse or inappropriate modification. Return of any Products by Buyer must be approved in writing by Omron before shipment. Omron Companies shall not be liable for the suitability or unsuitability or the results from the use of Products in combination with any electrical or electronic components, circuits, system assemblies or any other materials or substances or environments. Any advice, recommendations or information given orally or in writing, are not to be construed as an amendment or addition to the above warranty.

See http://www.omron.com/global/ or contact your Omron representative for published information.

Limitation on Liability; Etc

OMRON COMPANIES SHALL NOT BE LIABLE FOR SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, LOSS OF PROFITS OR PRODUCTION OR COMMERCIAL LOSS IN ANY WAY CONNECTED WITH THE PRODUCTS, WHETHER SUCH CLAIM IS BASED IN CONTRACT, WARRANTY, NEGLIGENCE OR STRICT LIABILITY.

Further, in no event shall liability of Omron Companies exceed the individual price of the Product on which liability is asserted.

Application Considerations

Suitability of Use

Omron Companies shall not be responsible for conformity with any standards, codes or regulations which apply to the combination of the Product in the Buyer's application or use of the Product. At Buyer's request, Omron will provide applicable third party certification documents identifying ratings and limitations of use which apply to the Product. This information by itself is not sufficient for a complete determination of the suitability of the Product in combination with the end product, machine, system, or other application or use. Buyer shall be solely responsible for determining appropriateness of the particular Product with respect to Buyer's application, product or system. Buyer shall take application responsibility in all cases.

NEVER USE THE PRODUCT FOR AN APPLICATION INVOLVING SERIOUS RISK TO LIFE OR PROPERTY WITHOUT ENSURING THAT THE SYSTEM AS A WHOLE HAS BEEN DESIGNED TO ADDRESS THE RISKS, AND THAT THE OMRON PRODUCT(S) IS PROPERLY RATED AND INSTALLED FOR THE INTENDED USE WITHIN THE OVERALL EQUIPMENT OR SYSTEM.

Programmable Products

Omron Companies shall not be responsible for the user's programming of a programmable Product, or any consequence thereof.

Disclaimers

Performance Data

Data presented in Omron Company websites, catalogs and other materials is provided as a guide for the user in determining suitability and does not constitute a warranty. It may represent the result of Omron's test conditions, and the user must correlate it to actual application requirements. Actual performance is subject to the Omron's Warranty and Limitations of Liability.

Change in Specifications

Product specifications and accessories may be changed at any time based on improvements and other reasons. It is our practice to change part numbers when published ratings or features are changed, or when significant construction changes are made. However, some specifications of the Product may be changed without any notice. When in doubt, special part numbers may be assigned to fix or establish key specifications for your application. Please consult with your Omron's representative at any time to confirm actual specifications of purchased Product.

Errors and Omissions

Information presented by Omron Companies has been checked and is believed to be accurate; however, no responsibility is assumed for clerical, typographical or proofreading errors or omissions.

Lot Numbers and Unit Versions of CS/CJ-series

Lot Numbers and Versions

Hardware revisions and unit versions are used to manage the hardware and software in CJ2/CJ3 CPU Units. (Hardware revisions are supported only for CJ3 CPU Units.)

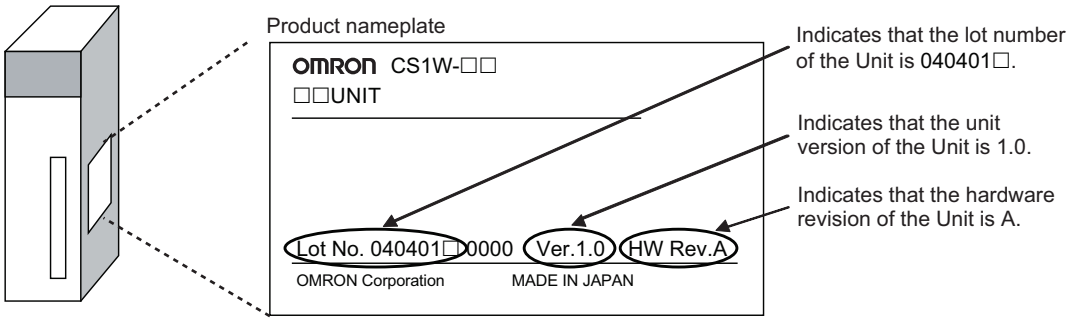
The hardware revision or unit version is updated each time there is a change in hardware or software specifications. Therefore, even if Units have the same model number, they will have functional or performance differences if they have different hardware revisions or unit versions.

The version at the time of shipment and the lot number can be confirmed on the product nameplate or with Support Software.

Notation of Lot Numbers and Unit Versions on Products

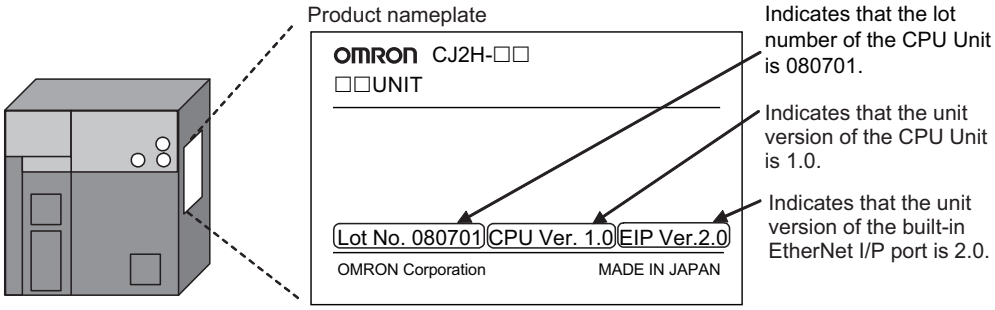
The unit version, hardware revision, and lot number can be confirmed on the nameplate on the side of the product.

■ **CS1W-EIP21/CJ1W-EIP21/EIP21S**



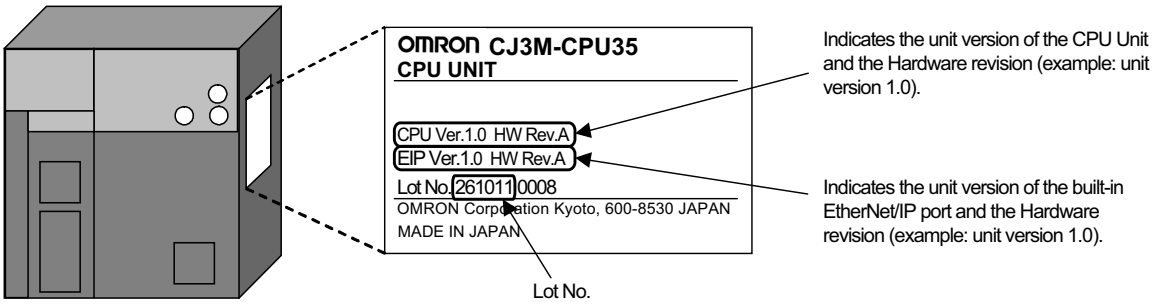
Units with a hardware revision of None do not have a hardware revision indication.

■ **CJ2H-CPU□□-EIP/CJ2M-CPU3□**



■ **CJ3M-CPU3□**

Example: For CJ3M-CPU35



In this manual, the version of the EtherNet/IP port built into the CJ2H-CPU□□-EIP/CJ2M-CPU3□/CJ3M-CPU3□ CPU Unit is given as the unit version.

Confirming Lot Numbers and Unit Versions with Support Software

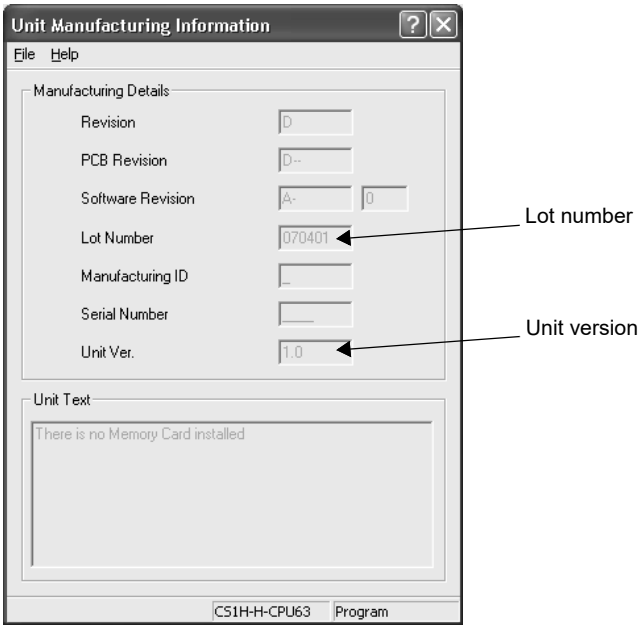
CX-Programmer version 4.0 can be used to confirm the lot number and unit version using the ***Unit Manufacturing Information***.

Note The lot number and unit versions of Pre-Ver.1.0 Units cannot be confirmed in ***Unit Manufacturing Information***. The following dialog box is displayed.



In the *IO Table* Dialog Box, right-click and select ***Unit Manufacturing information - CPU Unit.***

The following *Unit Manufacturing information* Dialog Box will be displayed.



Example The lot number 070401 and the unit version 1.0 will be displayed in the *Unit Manufacturing Information* Dialog Box.

Using Unit Version Label* The following unit version label is provided with the EtherNet/IP Unit.

This label can be attached to the front of the EtherNet/IP Unit to differentiate between EtherNet/IP Units with different unit versions.
* Only the unit version can be identified by the unit version label.

Lot Number Notation

The lot number is printed on the product's nameplate.

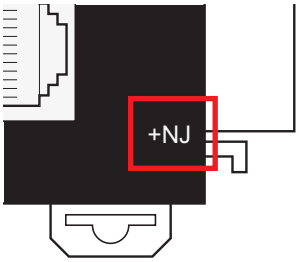
The lot number represents the manufacturing date and can be read as shown in the table below.

Product nameplate	How to read the lot number
Lot number shown to right of the "Lot No."	YYMMDD☐, in which YY indicates the last two digits of the year, MM the month, DD the day, and ☐ for use by OMRON.

Lot Numbers of CJ1W-EIP21S and Indication of Mounting Compatibility (Printing at the lower right of the Unit's front panel)

CJ1W-EIP21S with lot number 241001 or later are printed "+NJ" at the lower right of the Unit's front panel. CJ1W-EIP21S with lot number 250401 or later is printed "+CJ/CP/NJ" at the lower right of the Unit's front panel.

Example for "+NJ"



The relationship between the lot number, hardware revision, and indication of mounting compatibility (printing at the lower right of the Unit's front panel) is as follows.

Lot number	Hardware revision	Indication of mounting compatibility (printing at the lower right of the Unit's front panel)
250401 or later	"A"	"+CJ/CP/NJ"
241001 to 250331	None	"+NJ"
240930 or earlier	None	No printing

The printing at the lower right of the Unit's front panel means as follows.

Printing	Mean
CJ	No restrictions for the CJ-series Power Supply Units. (see *Restrictions for Installation (CS1W/CJ1W-EIP21S Only)* in *2-1-2 Unit Specifications*.
CP	Can be connected to the CP1H-series CPU Units.
NJ	Can be connected to the NJ-series CPU Units. (See CJ-series EtherNet/IP Units Operation Manual for NJ-series CPU Unit.)

Unit Version Notation

In this manual, the unit version of an EtherNet/IP Unit is given as shown in the following table.

Product nameplate	Notation used in this manual	Special remarks
Ver. 1.0 or later number shown to right of the lot number	Ethernet Unit Ver. 1.0 or later (See note.)	Information without reference to specific Unit Versions applies to all versions of the Unit.

Note Some Support Software products call the EtherNet/IP Unit version the "revision." "Revision" is also sometimes used in this manual.

Unit Versions of EtherNet/IP Units or Built-in EtherNet/IP Ports

The unit versions of EtherNet/IP Units or Built-in EtherNet/IP ports are shown below.

CS1W-EIP21/CJ1W-EIP21/ CJ2H-CPU□□-EIP

Unit version
Ver. 1.0
Ver. 2.0
Ver. 2.1
Ver. 3.0

CJ2M-CPU3□

Unit version
Ver. 2.0
Ver. 2.1
Ver. 2.2

CJ3M-CPU3□

Unit version
Ver. 1.1

CS1W/CJ1W-EIP21S/ CJ3M-CPU3□

Unit version
Ver. 1.0

The following topics are described below.

- Functions That Are Supported for Each Unit Version
- Applicable CIP Revisions
- Unit Versions and Programming Device Versions

Functions That Are Supported for Each Unit Version

For information on functions that are supported for each unit version of EtherNet/IP Units or built-in EtherNet/IP ports, refer to *Appendix A CS/CJ-series Ethernet Unit Function Comparison*.

The unit versions of EtherNet/IP Units or built-in EtherNet/IP ports and whether they can be connected to NJ-series CPU Units are shown below. For information on connection of the CJ1W-EIP21/EIP21S EtherNet/IP Units to NJ-series CPU Units, refer to the *CJ-series EtherNet/IP Units Operation Manual for NJ-series CPU Unit* (Cat. No. W495).

EtherNet/IP Units Excluding CS1W/CJ1W-EIP21S

	Unit version 1.0	Unit version 2.1 or later	
Models	CS1W-EIP21 CJ1W-EIP21 CJ2H-CPU6□-EIP CJ2M-CPU3□	CS1W-EIP21 CJ2H-CPU6□-EIP CJ2M-CPU3□	CJ1W-EIP21
Connection under an NJ-series CPU Unit	Not supported.	Not supported.	Supported. (See note.)

Note For details, refer to the *CJ-series EtherNet/IP Units Operation Manual for NJ-series CPU Unit* (Cat. No. W495).

CS1W/CJ1W-EIP21S/ CJ3M-CPU3□

Models	CS1W-EIP21S CJ1W-EIP21S	CJ3M-CPU3□
Connection under an Njseries CPU Unit	OK The CJ1W-EIP21S can be connected if the lot number is 241001 or later.	---
Modbus Server	---	OK
LLDP Function	---	OK

Applicable CIP Revisions

The following tables list the CIP revisions that are supported by the different unit versions of the EtherNet/IP Unit.

CS1W-EIP21, CJ1W-EIP21, and CJ2H-CPU□□-EIP

Unit version	CIP revision
Unit version 1.0	Revision 1.01
Unit version 2.0	Revision 2.01 to 2.03
Unit version 2.1	Revision 2.04 or 2.05
Unit version 3.0	Revision 3.01 to 3.03

CJ2M-CPU3□

Unit version	CIP revision
Unit version 2.0	Revision 2.01
Unit version 2.1	Revision 2.02 to 2.06
Unit version 2.2	Revision 2.07

CJ3M-CPU3□

Unit version	CIP revision
Unit version 1.1	Revision 4.02

CS1W/CJ1W-EIP21S

Unit version	CIP revision
Unit version 1.0	Revision 4.01

Unit Versions and Programming Device Versions

The following versions of the CX-Programmer and Network Configuration are required to set EtherNet/IP Units.

CS1W-EIP21, CJ1W-EIP21, and CJ2H-CPU□□-EIP

Unit version	CX-Programmer		
	Ver. 7.1 or lower	Ver. 8.0	Ver. 8.02 or higher
Unit version 1.0	---	OK*1	OK
Unit version 2.0	---	OK	OK*5
Unit version 3.0 or later	---	OK	OK*5

Unit version	Network Configurator for EtherNet/IP
	Ver. 3.00 or higher
Unit version 1.0	OK
Unit version 2.0	OK
Unit version 3.0 or later	OK*6

CJ3M-CPU3□

Unit version	CX-Programmer
	Ver. 9.90 or higher
Unit version 1.0	OK

Unit version	Network Configurator for EtherNet/IP
	Ver. 3.78 or higher
Unit version 1.0	OK

CJ2M-CPU3□

Unit version	CX-Programmer		
	Ver. 9.0 or lower	Ver. 9.1	Ver. 9.2 or higher
Unit version 2.0	---	OK	OK
Unit version 2.1	---	OK*2	OK*5
Unit version 2.2	---	OK*2	OK*5

Unit version	Network Configurator for EtherNet/IP		
	Ver. 3.1 or lower	Ver. 3.20	Ver. 3.21 or higher
Unit version 2.0	---	OK	OK*3
Unit version 2.1	---	OK*4	OK
Unit version 2.2	---	OK*4	OK

CS1W/CJ1W-EIP21S

Unit version	CX-Programmer*7	
	Ver. 9.76 or lower	Ver. 9.81 or higher*8
Unit version 1.0	---	OK

Unit version	Network Configurator for EtherNet/IP	
	Ver. 3.72 or lower	Ver. 3.74a or higher*8
Unit version 1.0	---	OK

Unit version	EIP21S User Management Tool*7
	Ver. 1.00 or higher*8
Unit version 1.0	OK

*1: The most recent version of the common module for CX-One version 3.□□ must be installed.
*2: The most recent version of the common module for CX-One version 4.□□ must be installed.
*3: The settings cannot be downloaded from the computer to the PLC if more than 20 words of tag data links are set.
*4: A maximum of 20 words of tag data links can be set.
*5: For EtherNet/IP Units manufactured in October 2012 or later, you must install CX-Programmer version 9.41 to use the backup functions with the Backup Tool.
*6: The Network Configurator for EtherNet/IP version 3.57 or higher is required.
*7: If the OS of your PC is earlier than Windows 10, you cannot either install the EIP21S User Management Tool or select Secure Comm in the CX-Programmer and the PLC Backup Tool.
If the Windows 10 version is earlier than 1803, you cannot either go online by Secure Comm or use the function derived from Secure Comm.
*8: If you have a CX-One version lower than 4.61, use the auto update function to update it after July 2023. This allows you to update the Support Software to the same version as that included in version 4.61 (DVD).

PRECAUTIONS

This section provides general precautions for using the CS/CJ-series EtherNet/IP Units and built-in EtherNet/IP ports.

The information contained in this section is important for the safe and reliable application of EtherNet/IP Units or built-in EtherNet/IP ports. You must read this section and understand the information contained before attempting to set up or operate an EtherNet/IP Unit or built-in EtherNet/IP port.

1 Intended Audience xxviii
2 General Precautions xxviii
3 Safety Precautions xxix
4 Operating Environment Precautions xxxii
5 Application Precautions xxxii
6 Conformance to EMC and Electrical Safety Regulations xxxv
Concepts xxxv
7 Software Licenses and Copyrights xxxv

1 Intended Audience

This manual is intended for the following personnel, who must also have knowledge of electrical systems (an electrical engineer or the equivalent).

- Personnel in charge of installing FA systems.
- Personnel in charge of designing FA systems.
- Personnel in charge of managing FA systems and facilities.

2 General Precautions

The user must operate the product according to the performance specifications described in the operation manuals.

Before using the product under conditions which are not described in the manual or applying the product to nuclear control systems, railroad systems, aviation systems, vehicles, combustion systems, medical equipment, amusement machines, safety equipment, and other systems, machines, and equipment that may have a serious influence on lives and property if used improperly, consult your OMRON representative.

Make sure that the ratings and performance characteristics of the product are sufficient for the systems, machines, and equipment, and be sure to provide the systems, machines, and equipment with double safety mechanisms.

This manual provides information for programming and operating the Unit. Be sure to read this manual before attempting to use the Unit and keep this manual close at hand for reference during operation.

⚠ **WARNING** It is extremely important that a PLC and all PLC Units be used for the specified purpose and under the specified conditions, especially in applications that can directly or indirectly affect human life. You must consult with your OMRON representative before applying a PLC System to the above-mentioned applications.

3 Safety Precautions

⚠ **WARNING** Do not attempt to take any Unit apart while the power is being supplied. Doing so may result in electric shock.

⚠ **WARNING** Do not touch any of the terminals or terminal blocks while the power is being supplied. Doing so may result in electric shock.

⚠ **WARNING** Do not attempt to disassemble, repair, or modify any Units. Any attempt to do so may result in malfunction, fire, or electric shock.

⚠ **WARNING** Provide safety measures in external circuits (i.e., not in the Programmable Controller), including the following items, to ensure safety in the system if an abnormality occurs due to malfunction of the Programmable Controller or another external factor affecting the operation of the Programmable Controller. “Programmable Controller” indicates the CPU Unit and all other Units and is abbreviated “PLC” in this manual.

- Emergency stop circuits, interlock circuits, limit circuits, and similar safety measures must be provided in external control circuits.
- The PLC will turn OFF all outputs when its self-diagnosis function detects any error or when a severe failure alarm (FALS) instruction is executed. As a countermeasure for such errors, external safety measures must be provided to ensure safety in the system.
- The PLC will turn OFF all outputs when its self-diagnosis function detects any error or when a severe failure alarm (FALS) instruction is executed. Unexpected operation, however, may still occur for errors in the I/O control section, errors in I/O memory, and other errors that cannot be detected by the self-diagnosis function. As a countermeasure for all such errors, external safety measures must be provided to ensure safety in the system.
- Provide measures in the computer system and programming to ensure safety in the overall system even if errors or malfunctions occur in data link communications or remote I/O communications.

⚠ **WARNING** **Anti-virus protection**

Install the latest commercial-quality antivirus software on the computer connected to the control system and maintain to keep the software up-to-date.

⚠ **WARNING** **Security measures to prevent unauthorized access**

Take the following measures to prevent unauthorized access to our products.

- Install physical controls so that only authorized personnel can access control systems and equipment.
- Reduce connections to control systems and equipment via networks to prevent access from untrusted devices.
- Install firewalls to shut down unused communications ports and limit communications hosts and isolate control systems and equipment from the IT network.
- Use a virtual private network (VPN) for remote access to control systems and equipment.
- Adopt multifactor authentication to devices with remote access to control systems and equipment.
- Set strong passwords and change them frequently.
- Scan virus to ensure safety of USB drives or other external storages before connecting them to control systems and equipment.

⚠ **WARNING** **Data input and output protection**

Validate backups and ranges to cope with unintentional modification of input/output data to control systems and equipment.

- Checking the scope of data
- Checking validity of backups and preparing data for restore in case of falsification and abnormalities
- Safety design, such as emergency shutdown and fail-soft operation in case of data tampering and abnormalities

⚠**WARNING** **Data recovery**
Backup data and keep the data up-to-date periodically to prepare for data loss.

⚠**WARNING** When using an intranet environment through a global address, connecting to an unauthorized terminal such as a SCADA, HMI or to an unauthorized server may result in network security issues such as spoofing and tampering.
You must take sufficient measures such as restricting access to the terminal, using a terminal equipped with a secure function, and locking the installation area by yourself.

⚠**WARNING** When constructing an intranet, communication failure may occur due to cable disconnection or the influence of unauthorized network equipment.
Take adequate measures, such as restricting physical access to network devices, by means such as locking the installation area.

⚠**WARNING** When using a device equipped with the SD Memory Card function, there is a security risk that a third party may acquire, alter, or replace the files and data in the removable media by removing the removable media or unmounting the removable media.
Please take sufficient measures, such as restricting physical access to the Controller or taking appropriate management measures for removable media, by means of locking the installation area, entrance management, etc., by yourself.

⚠**Caution** Execute online editing only after confirming that no adverse effects will be caused by extending the cycle time. Otherwise, the input signals may not be readable.

- Emergency stop circuits, interlock circuits, limit circuits, and similar safety measures must be provided in external control circuits.

⚠**Caution** Fail-safe measures must be taken by the customer to ensure safety in the event of incorrect, missing, or abnormal signals caused by broken signal lines, momentary power interruptions, or other causes. Serious accidents may result from abnormal operation if proper measures are not provided.

⚠**Caution** Confirm safety at the destination node before changing or transferring to another node the contents of a program, the PLC Setup, I/O tables, I/O memory, or parameters. Changing or transferring any of these without confirming safety may result in injury.

⚠**Caution** Tighten the screws on the terminal block of the AC Power Supply Unit to the torque specified in the operation manual. The loose screws may result in burning or malfunction.

⚠ **Caution** When using the power OFF detection time with a CJ1W-EIP21S or CS1W-EIP21S EtherNet/IP Unit, use the Power Supply Unit and power supply voltage specified in this manual. If you use a non-specified Power Supply Unit, the CJ1W-EIP21S or CS1W-EIP21S EtherNet/IP Unit may malfunction and fail to start.

4 Operating Environment Precautions

⚠ **Caution** Do not operate the control system in the following locations:

- Locations subject to direct sunlight.
- Locations subject to temperatures or humidity outside the range specified in the specifications.
- Locations subject to condensation as the result of severe changes in temperature.
- Locations subject to corrosive or flammable gases.
- Locations subject to dust (especially iron dust) or salts.
- Locations subject to exposure to water, oil, or chemicals.
- Locations subject to shock or vibration.

⚠ **Caution** Take appropriate and sufficient countermeasures when installing systems in the following locations:

- Locations subject to static electricity or other forms of noise.
- Locations subject to strong electromagnetic fields.
- Locations subject to possible exposure to radioactivity.
- Locations close to power supplies.

5 Application Precautions

Observe the following precautions when using the EtherNet/IP Unit or built-in EtherNet/IP port.

⚠ **WARNING** Always heed these precautions. Failure to abide by the following precautions could lead to serious or possibly fatal injury.

- Always connect to a ground of 100 Ω or less when installing the Units. Not connecting to a ground of 100 Ω or less may result in electric shock.
- Always turn OFF the power supply to the CPU Unit and Slaves before attempting any of the following. Not turning OFF the power supply may result in malfunction or electric shock.
  - Mounting or dismounting Power Supply Units, I/O Units, CPU Units, Memory Packs, or Master Units.
  - Assembling the Units.
  - Setting DIP switches or rotary switches.
  - Connecting cables or wiring the system.
  - Connecting or disconnecting the connectors.

⚠ **Caution** Failure to abide by the following precautions could lead to faulty operation of the EtherNet/IP Unit, built-in EtherNet/IP port, or the system, or could damage the Ethernet Unit. Always heed these precautions.

- Interlock circuits, limit circuits, and similar safety measures in external circuits (i.e., not in the Programmable Controller) must be provided by the customer.
- Always use the power supply voltages specified in the operation manuals. An incorrect voltage may result in malfunction or burning.
- Take appropriate measures to ensure that the specified power with the rated voltage and frequency is supplied. Be particularly careful in places where the power supply is unstable. An incorrect power supply may result in malfunction.
- Install external breakers and take other safety measures against short-circuiting in external wiring. Insufficient safety measures
- Make sure that all the Backplane mounting screws, terminal block screws, and cable connector screws are tightened to the torque specified in the relevant manuals. Incorrect tightening torque may result in malfunction.
- Do not allow scraps and chips of wire to enter the Unit. Doing so may result in burning, failure, or malfunction. Take measures such as covering the Unit, in particular, during installation.
- Do not insert foreign matter from any opening of the Unit. Doing so may result in burning, electric shock, or failure.
- Use crimp terminals for wiring. Do not connect bare stranded wires directly to terminals. Connection of bare stranded wires may result in burning.
- Observe the following precautions when wiring the communications cable.
  - Separate the communications cables from the power lines or high-tension lines.
  - Do not bend the communications cables past their natural bending radius.
  - Do not pull on the communications cables.
  - Do not place heavy objects on top of the communications cables.
  - Always lay communications cable inside ducts.
  - Use appropriate communications cables.
- Make sure that the terminal blocks, expansion cable connectors, and other items with locking devices are locked in place.
- Wire all connections correctly according to instructions in this manual.
- Double-check all wiring and switch settings before turning ON the power supply. Incorrect wiring may result in burning.
- Mount terminal blocks and connectors only after checking the mounting location carefully.
- Check the user program (ladder program and other programs) and parameters for proper execution before actually running it on the Unit. Not checking the program may result in unexpected operation.

- Confirm that no adverse effect will occur in the system before attempting any of the following. Not doing so may result in an unexpected operation.
  - Changing the operating mode of the PLC.
  - Force-setting/force-resetting any bit in memory.
  - Changing the present value of any word or any set value in memory.
- After replacing a Unit, resume operation only after transferring to the new CPU Unit, Special I/O Unit, or CPU Bus Unit the contents of the DM Area, HR Area, programs, parameters, and other data required for resuming operation. Not doing so may result in an unexpected operation.
- Before touching a Unit, be sure to first touch a grounded metallic object in order to discharge any static build-up. Not doing so may result in malfunction or damage.
- When transporting the Unit, use special packing boxes and protect it from being exposed to excessive vibration or impacts during transportation.
- CPU Bus Units will be restarted when routing tables are transferred from a Programming Device to the CPU Unit. Restarting these Units is required to read and enable the new routing tables. Confirm that the system will not be adversely affected before allowing the CPU Bus Units to be reset.
- When the settings (IP address or tag data link settings) of the EtherNet/IP Unit or built-in EtherNet/IP port are transferred from a Programming Device, all of the destination EtherNet/IP Units or built-in EtherNet/IP ports (nodes) will be reset in order to enable the transferred settings. Transfer settings to the EtherNet/IP Units or built-in EtherNet/IP ports only after verifying that restarting the Units will not cause any problems in the system.
- If a repeater hub is used for EtherNet/IP tag data links (cyclic communications), the network's communications load will increase, data collisions will occur frequently, and stable communications will be impossible. Always use a switching hub when using tag data links in the network.
- Before resetting a CPU Bus Unit or Special I/O Unit, always verify that restart the Unit will not cause any problems in the system.
- If incorrect tag data link parameters are set, it may cause equipment to operate unpredictably. Even when the correct tag data link parameters are set, make sure that there will be no effect on equipment before transferring the data.
- Do not connect any devices other than a personal computer to the USB port.
- CJ3M CPU Unit has no battery.
  - If you use the clock data in the user program and turn OFF the power supply for a long time, use a Battery (CJ1W-BAT01) which is sold separately. The Battery is not mounted when the product is at factory setting. The clock data is retained by the built-in capacitor. The capacitor is charged while the power is supplied and discharged while the power is not supplied. If the power OFF time rate is high, the clock data is initialized and malfunctions may occur in the program for which the clock data is used.

- If you use the Battery, connect the CX-Programmer and set the Battery-related error detection to “Detect”. The Battery-related error detection is set to Do not use at the factory setting because the Battery is not built in. If the Battery-related er-ror detection is set to “Not Detect”, an error cannot be detected when the Battery is exhausted and malfunctions may occur in the program for which the clock data is used.

6 Conformance to EMC and Electrical Safety Regulations

Concepts

OMRON products are industrial electrical devices that are incorporated into various types of machines and manufacturing equipment. The products conform to the relevant standards so that the machines and equipment incorporating the OMRON products can comply with EMC and Electrical Safety Regulations more easily.

Refer to the OMRON website (www.ia.omron.com) or ask your OMRON representative for the most recent standards to which our products conform.

■ Conformance to EMC regulations

This product complies with EMC regulations when assembled in a PLC system or Machine Automation Controller.

To ensure that your machine or equipment complies with EMC regulations, please observe the following precautions.

- This product is defined as an in-panel device and must be installed within a control panel.
- This product complies with the emission standards. For the radiated emission requirements, in particular, please note that the actual emission varies depending on the configuration of the control panel to be used, the connected devices, and wiring methods. Therefore, customers themselves must confirm that the entire machine or equipment conforms to EMC regulations, even you are using a device that conforms to EMC regulations.
- You must use reinforced insulation or double insulation for the DC power supplies connected to DC Power Supply Units and I/O Units.

Caution:

This equipment is not intended for use in residential environments and may not provide adequate protection to radio reception in such environments.

■ Conformance to Electrical Safety regulations

This product complies with Electrical Safety regulations required by specific laws and regulations such as the EU Directives and UKCA.

For precautions for each product, see the instruction manual included with the product.

7 Software Licenses and Copyrights

This product incorporates certain third party software. The license and copyright information associated with this software is below.

CS1W/CJ1W-EIP21S:

https://www.fa.omron.co.jp/product/tool/nx-info/index_en.html
CJ3M-CPU3□:
https://www.fa.omron.co.jp/product/tool/cj-info/index_en.html

- OpenSSL

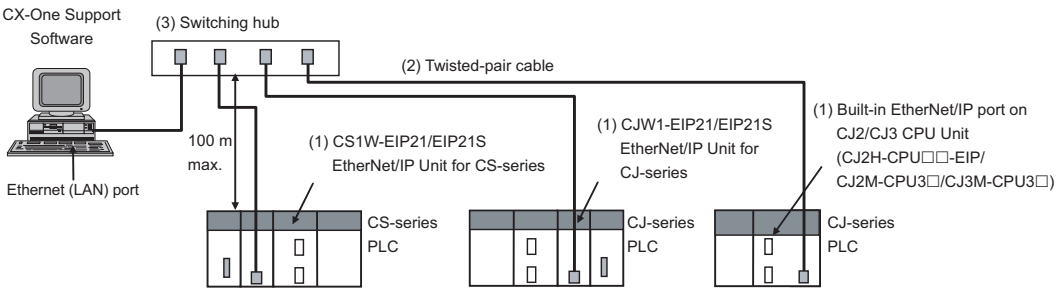
This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit
(http://www.openssl.org/).
Copyright (C) 1998-2019 The OpenSSL Project. All rights reserved.
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.
This product includes cryptographic software written by Eric Young
(eay@cryptsoft.com)

SECTION 1
Overview of EtherNet/IP

This section introduces the functions and protocols used in EtherNet/IP Unit or built-in EtherNet/IP port communications services.

1-1 EtherNet/IP Unit Features 2
1-2 Devices Required for Constructing a Network 5
1-3 Support Software Required to Construct a Network 5
1-4 Communications Services Overview 7
1-5 Network Configurator Overview 13
1-5-1 Overview 13
1-5-2 Network Configurator Requirements 13
1-5-3 Precautions When Using the Network Configurator 14

1-1 EtherNet/IP Unit Features



EtherNet/IP System Configuration Example

EtherNet/IP is an industrial multi-vendor network that uses Ethernet components. The EtherNet/IP specifications are open standards managed by the ODVA (Open DeviceNet Vendor Association), just like DeviceNet.

EtherNet/IP is not just a network between controllers; it is also used as a field network. Since EtherNet/IP uses standard Ethernet technology, various general-purpose Ethernet devices can be used in the network. The EtherNet/IP Unit and built-in EtherNet/IP port have the following features.

High-speed, High-capacity Data Exchange through Data Links

The EtherNet/IP protocol supports implicit communications, which allows cyclic communications (called tag data links in this manual) with EtherNet/IP devices. Data can be exchanged at high speed between Controllers and devices, using high-volume tag sets (up to 640 words for the CJ2M-EIP21 and up to 184,832 words for other CPU Units) between PLCs.

Tag Data Link (Cyclic Communications) Cycle Time

Tag data links (cyclic communications) can operate at the cyclic period specified for each application, regardless of the number of nodes. Data is exchanged over the network at the refresh cycle set for each connection, so the communications refresh cycle will not increase even if the number of nodes is increased, i.e., the synchronicity of the connection's data is preserved.

Since the refresh cycle can be set for each connection, each application can communicate at its ideal refresh cycle. For example, a processes interlocks can be transferred at high speed while the production commands and the status monitor information are transferred at low speed.

Note The communications load to the nodes must be within the Units' allowed communications bandwidth.

Communicating with FINS Messages (FINS/TCP and FINS/UDP)

Data can be exchanged with other OMRON FA devices using SEND, RECV, and CMND instructions from the ladder program, because EtherNet/IP supports OMRON's standard FINS message communications services.

There are two kinds of message services, using UDP/IP and TCP/IP (called FINS/UDP and FINS/TCP), allowing flexible data exchange for different applications.

Note There are no particular restrictions when sending FINS messages to OMRON Ethernet Units (CS1W-ETN21 or CJ1W-ETN21) in an Ethernet network.

Network Connections with Controller Link

Mutual connections of Controller Link and EtherNet/IP are also supported (using the FINS communications service). The Controller Link connection allows a PLC on the Controller Link network to be monitored from a PLC on the EtherNet/IP network. Conversely, data can be exchanged with a PLC on the EtherNet/IP network from a PLC on the Controller Link network.

FTP Server

A built-in FTP server is provided to enable transferring files in the PLC to and from a host computer. This enables transferring large amounts of data from a client without any additional ladder programming.

Automatic PLC Clock Adjustment

The clocks built into PLCs connected to Ethernet can be automatically adjusted to the time of the clock in the SNTP server. If all of the clocks in the system are automatically adjusted to the same time, time stamps can be used to analyze various production histories.

Note A separate SNTP server is necessary to automatically adjust the PLC clocks.

Manage the Network with an SNMP Manager

Internal status information from the EtherNet/IP Unit or built-in EtherNet/IP port can be passed to network management software that uses an SNMP manager.

Note A separate SNMP manager is necessary for network management.

Specify Servers with Host Names

DNS client functionality allows you to use host names instead of IP addresses to specify SNTP servers and SNMP managers. This is useful, for example, when server IP addresses change for system revisions because the IP addresses are automatically found when host names are used.

Note

(1) A separate DNS server is necessary to use host names with the DNS client.

(2) The DNS server is specified directly using its IP address.

Set Classless IP Address with CIDR

A subnet mask can be set to use classless IP addresses, allowing more flexibility in address settings.

Support for QuickConnect™ (Originator Only)

Equipment replacement during network operation is possible.

Note This function is supported by the CS1W/CJ1W-EIP21S, CJ3M-CPU3□.

Plentiful Troubleshooting Functions

A variety of functions are provided to quickly identify and handle errors.

- Self-diagnosis at power ON
- PING command to check the connection with another node
- Error Log functions record the time of occurrence and other error details

Security Functions Including User Authentication and IP Packet Filter

Security functions to reduce the risk of misappropriation and tampering of customer assets are provided.

For information on the security functions, refer to *SECTION 13 Security Functions*.

Note This function is supported by the CS1W/CJ1W-EIP21S, CJ3M-CPU3□.

Communications by UDP/IP and TCP/IP (Socket Service Functions)

The standard Ethernet protocols, UDP/IP and TCP/IP, are supported, making it possible to communicate with a wide range of devices, workstations, computers, and Ethernet Units from other manufacturers.

Up to eight ports can be used for various protocols, enabling the use of various applications.

Note This function is supported by the CS1W/CJ1W-EIP21S, CJ3M-CPU3□.

Simplified Socket Services

Without using the CMND(490) or CMND2(493) instruction, the socket service functions for TCP or UDP can be simplified by presetting parameters and using dedicated bits. In addition, the size of received data accumulated in the reception buffer is stored, and a Data Received Flag is supported. These new features eliminate the need for ladder programs to monitor the timing for completion of instructions and socket service processing, and thus reduce the amount of labor required for program development.

The performance of sending and receiving has been improved using optional settings for the TCP or UDP socket services using specific bits in memory. Also, a linger socket option can be used with the TCP socket services. Specifying this option enables open processing immediately with the same port number without having to wait (approximately 1 min.) until the port number opens after the socket closes.

Note This function is supported by the CS1W/CJ1W-EIP21S, CJ3M-CPU3□.

Modbus TCP/UDP Server Function

Allocating Modbus addresses in the I/O memory of the CPU Unit enables reading and writing in the I/O memory of the CPU Unit from a host PC, host PLC, HMI, or other Modbus client device. A Modbus TCP server and Modbus UDP server are supported, and a Modbus TCP server can be connected with up to eight clients.

Note This function is supported by the CJ3M-CPU3□.

Modbus TCP/UDP Client Function

As a Modbus client, it can issue Modbus commands to Modbus devices. The reading and writing of Modbus coils and registers can be performed with function blocks using the socket service functions. A Modbus TCP client and Modbus UDP client are supported, which can each be connected with up to eight servers.

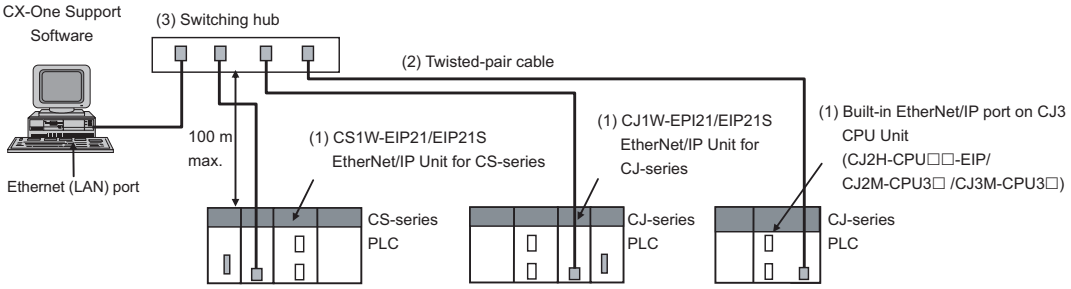
Note This function is supported by the CJ3M-CPU3□, CJ1W-EIP21S.

Note The CIP (Common Industrial Protocol) is a shared industrial protocol for the OSI application layer. The CIP is used in networks such as EtherNet/IP, ControlNet, and DeviceNet. Data can be routed easily between networks that are based on the CIP, so a transparent network can be easily configured from the field device level to the host level.
The CIP has the following advantages.

- Destination nodes are specified by a relative path, without fixed routing tables.
- The CIP uses the producer/consumer model. Nodes in the network are arranged on the same level and it is possible to communicate with required devices whenever it is necessary.
  The consumer node will receive data sent from a producer node when the connection ID in the packet indicates that the node requires the data. Since the producer can send the same data with the same characteristics in a multicast (either multicast or unicast can be selected), the time required for the transfer is fixed and not dependent on the number of consumer nodes.

1-2 Devices Required for Constructing a Network

The basic configuration for an EtherNet/IP System consists of one switching hub to which nodes are attached in star configuration using twisted-pair cable.



The devices shown in the following table are required to configure a network with EtherNet/IP Units or the built-in EtherNet/IP port.

Network device	Contents
(1) CS1W-EIP21S/EIP21 CJ1W-EIP21S/EIP21 CJ3M-CPU3□ CJ2H-CPU6□-EIP CJ2M-CPU3□	These are Communications Units or built-in ports that connect a CS-series or CJ-series PLC to an EtherNet/IP network.
(2) Twisted-pair cable	The twisted-pair cable connects EtherNet/IP Units or built-in EtherNet/IP ports to the switching hub, with an RJ45 Modular Connector at each end. Use an STP (shielded twisted-pair) cable of category 5, 5c, or higher.
(3) Switching Hub	This is a relay device that connects multiple nodes in a star-shaped LAN.

Recommended Switching Hubs

For details on recommended devices for constructing a network, refer to *2-3-1 Recommended Network Devices*.

Note If a repeater hub is used for EtherNet/IP tag data links (cyclic communications), the network's communications load will increase, data collisions will occur frequently, and stable communications will be impossible. Always use a switching hub when using tag data links in the network.

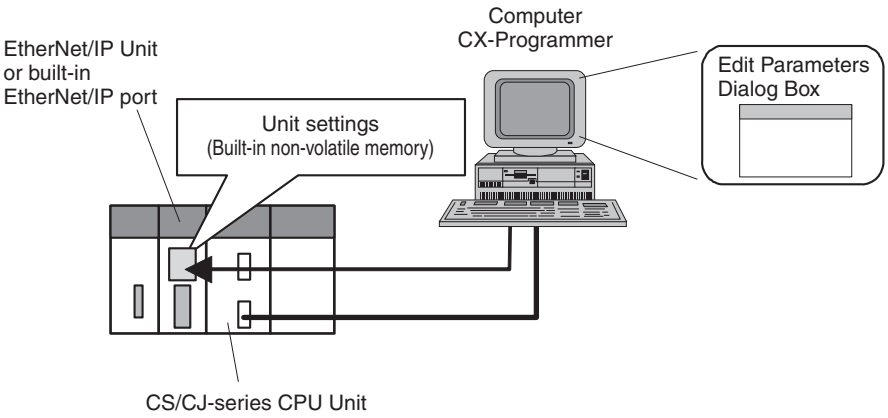
1-3 Support Software Required to Construct a Network

This section describes the Support Software that is required to construct an EtherNet/IP network. Make the tag data link settings and Unit setup settings for the EtherNet/IP Unit or built-in EtherNet/IP port. Both of these settings are stored in the EtherNet/IP Unit's non-volatile memory (See note.). Support Software is provided for each, as described below.

Note Unlike the Ethernet Units, the EtherNet/IP Unit's TCP/IP settings are not stored in the CPU Unit's CPU Bus Unit System Setup Area.

Unit Setup: CX-Programmer

The CX-Programmer is used to set basic parameters, such as the local IP address of the EtherNet/IP Unit or built-in EtherNet/IP port and the subnet mask. (The CX-Programmer is included in the CX-One.)
The CX-Programmer can also be used to check if data I/O is being performed correctly for tag data links.



Refer to the *CX-Programmer Operation Manual* (Cat. No. W446) for information on the CX-Programmer.

User Authentication Setting: EIP21S User Management Tool

The EIP21S User Management Tool (included with CX-One version 4.61 or higher) is used to make the setup to use user authentication with the CS1W/CJ1W-EIP21S, CJ2M-CPU3□ and CJ3M-CPU3□ such as user account registration and deletion.

It is also used to acquire and clear the operation log.

Refer to *13-3 User Authentication* for information on the user authentication and operation log functions.

Note If the OS of your PC is earlier than Windows 10, you cannot either install the EIP21S User Management Tool or select Secure Comm in the CX-Programmer and the PLC Backup Tool.
If the Windows 10 version is earlier than 1803, you cannot either go online by Secure Comm or use the function derived from Secure Comm.

Tag Data Link Settings: Network Configurator

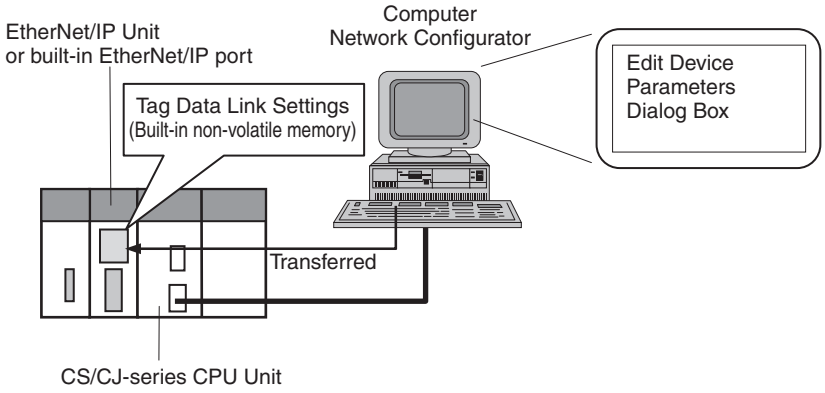
The Network Configurator is used to set the tag data links for the EtherNet/IP Unit or built-in EtherNet/IP port. (The Network Configurator is included in CX-One version 3.0 or higher.) The main functions of the Network Configurator are given below.

1) Setting and Monitoring Tag Data Links (Connections)

The network device configuration and tag data links (connections) can be created and edited. After connecting to the network, the device configuration and tag data link settings can be uploaded and monitored.

2) Multivendor Device Connections

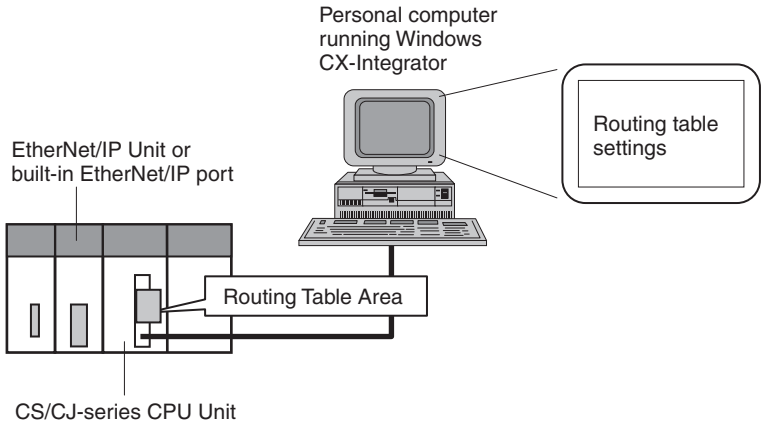
EDS files can be installed and deleted to enable constructing, setting, and managing networks that contain EtherNet/IP devices from other companies. The IP addresses of EtherNet/IP devices can also be changed.



For details on the Network Configurator, refer to *SECTION 6 Tag Data Link Functions*.

Routing Table Settings: CX-Integrator

Propriety OMRON FINS network system can be constructed from OMRON Communications Units. When FINS services are used, the CX-Integrator allows you to set routing tables to define transmission paths. (The CX-Integrator is included in the CX-One.) If FINS services are not used, then routing tables are not required.



Refer to the *CX-Integrator Operation Manual* (Cat. No. W464) for information on the CX-Integrator.

1-4 Communications Services Overview

The following communications services are supported.

CIP (Common Industrial Protocol) Communications Services

1) Tag Data Links (Cyclic Communications)

A program is not required to perform cyclic data exchanges with other devices in the EtherNet/IP network.

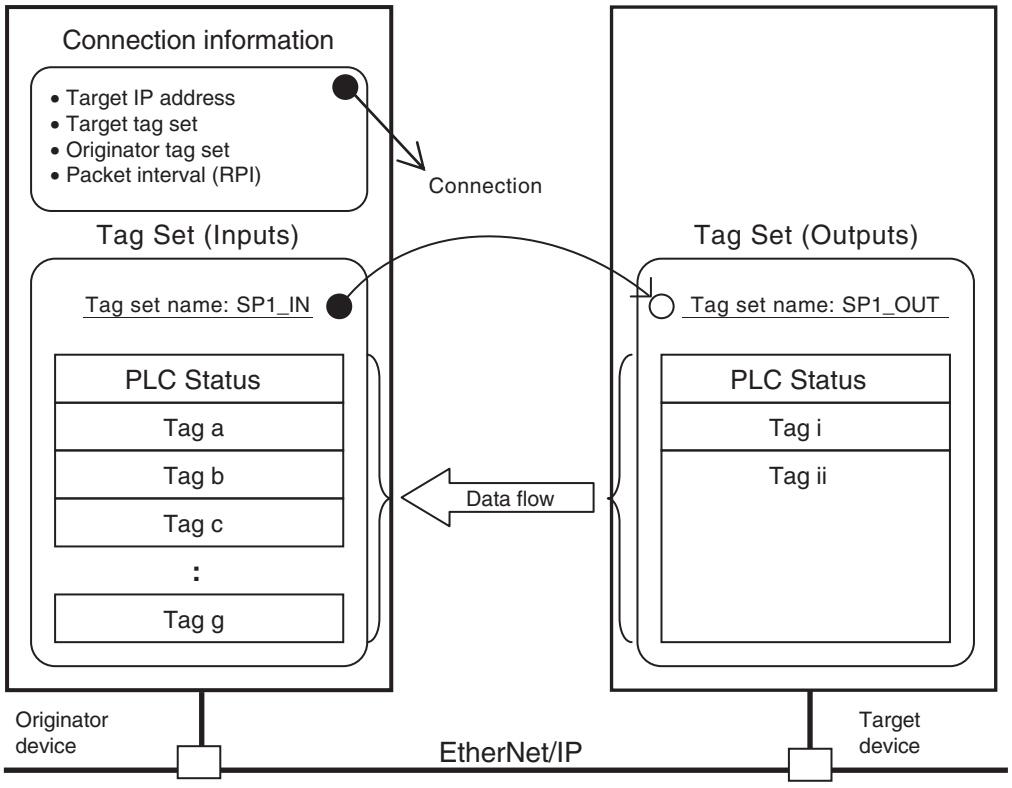
Normally, the tag data links in an EtherNet/IP Unit or built-in EtherNet/IP port are started by grouping the tags created with the Network Configurator into a tag set, and establishing a connection with the target device using that group of tags. One connection is used per group (tag set). Up to 32 connections for the CJ2M-EIP21 and up to 256 connections for other CPU Units) can be registered.

The following table gives the tag and tag set specifications.

Tags		Tag sets	
CS1W-EIP21/EIP21S CJ1W-EIP21/EIP21S CJ2H-CPU□□-EIP CJ3M-CPU3□	CJ2M-CPU3□	CS1W-EIP21 CJ1W-EIP21 CJ2H-CPU□□-EIP CJ3M-CPU3□	CJ2M-CPU3□
Total size of all tags ≤ 184,832 words	Total size of all tags ≤ 640 words	Maximum size of 1 tag set ≤ 722 words (The maximum size is 721 words when the tag set includes the PLC status.)	Maximum size of 1 tag set ≤ 640 words*1 (The maximum size is 639 words when the tag set includes the PLC status.)*2
Maximum size of 1 tag ≤ 722 words (The maximum size is 721 words when the tag set includes the PLC status.)	Maximum size of 1 tag ≤ 640 words*1 (The maximum size is 639 words when the tag set includes the PLC status.)*2	Number of tags per tag set ≤ 8 (7 tags/tag set when the tag set includes the PLC status) **Note** Input and output variables cannot be combined.	
Number of registrable tags ≤ 256	Number of registrable tags ≤ 32	Number of registrable tag sets ≤ 256	Number of registrable tag sets ≤ 32

*1 Unit version 2.0: 20 words maximum.

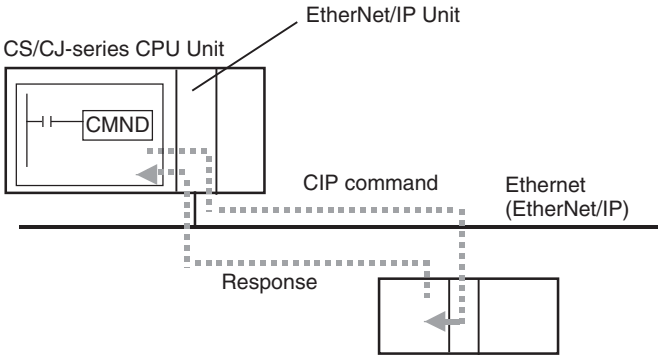
*2 Unit version 2.0: 19 words maximum.



Note In this example, a connection is established with the originator's tag list containing tags a to g (inputs), which are grouped in a tag set called SP1_IN, and the target's tag list containing tags i and ii (outputs), which are grouped in a tag set called SP1_OUT.

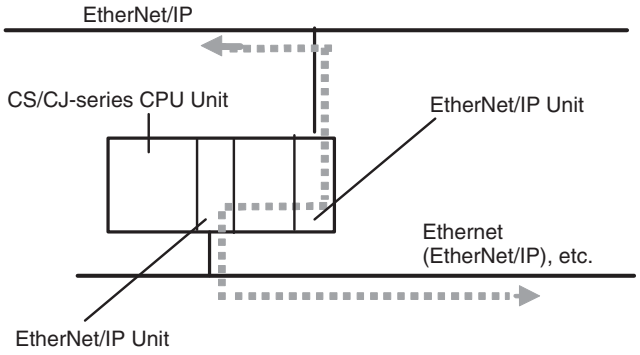
2) Message Communications (Unconnected Message Service)

User-specified CIP commands can be sent to devices on the EtherNet/IP network. CIP commands, such as those for reading and writing data, can be sent and their responses received by executing the CMND instruction from the CS/CJ-series CPU Unit's user program (without using a connection).



CIP messages (CIP commands and responses) can also be transferred to another CIP-based network via the EtherNet/IP Unit or built-in EtherNet/IP port using the CIP routing function for message communications.

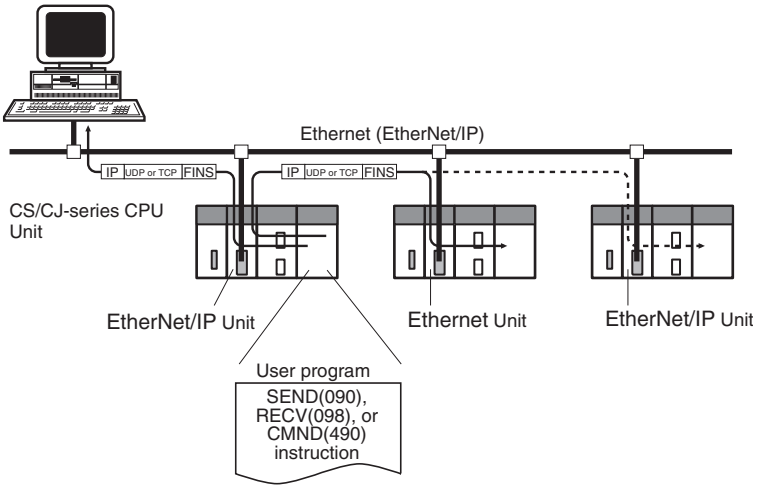
In the CS/CJ Series, CIP routing is possible only through two EtherNet/IP Units or built-in EtherNet/IP port.



FINS Communications Service

FINS commands can be sent to or received from other PLCs or computers on the same Ethernet network by executing SEND(090), RECV(098), or CMND(490) instructions in the ladder diagram program. This enables various control operations such as the reading and writing of I/O memory between PLCs, mode changes, and file memory operations.

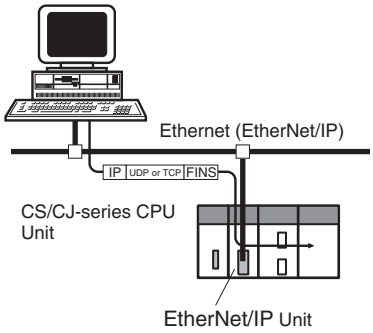
Note There are no particular restrictions when sending FINS messages to OMRON EtherNet/IP Unit and Built-in EtherNet/IP Port in an Ethernet network.



Various control operations (such as the reading and writing of I/O memory between PLCs, mode changes, and file memory operations) can be executed from the host computer by sending the corresponding FINS command with a UDP/IP or TCP/IP header attached.

For example, it is possible to connect online via Ethernet from FINS communications applications such as the CX-Programmer, and to perform remote programming and monitoring. (See note.)

Note Use CX-Programmer version 4.0 or higher to use TCP/IP. For lower versions of CX-Programmer, FinsGateway Version 2003 or higher is required to use TCP/IP.



The FINS gateway function enables access to PLCs on not only the same Ethernet network but on various other networks, including SYSMAC LINK and Controller Link.

Socket Services

The socket services allow devices on the Ethernet to send and receive various data using either the UDP or TCP protocol.

Note The Socket Service function is supported by the CS1W/CJ1W-EIP21S and CJ3M-CPU3□.

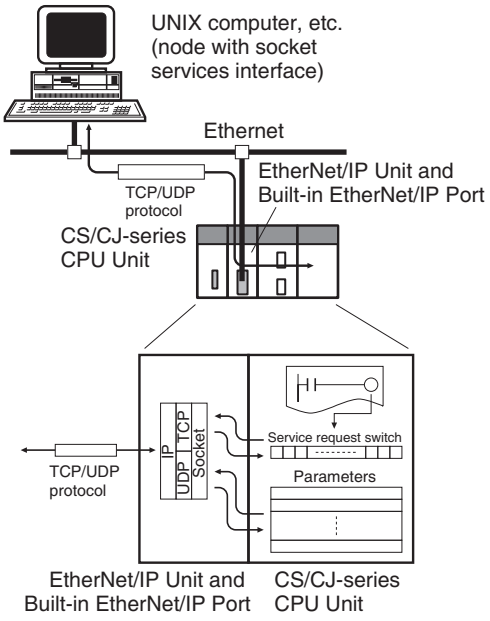
1) Manipulating Dedicated Control Bits

One way to use socket services is to set the required parameters in the parameter area allocated in the DM Area, and then to request particular UDP or TCP socket services by turning ON dedicated control bits in memory. When the EtherNet/IP Unit and Built-in EtherNet/IP Port has completed the requested process, the same bit is turned OFF to provide notification. Data that is sent or received is automatically handled according to the I/O memory locations specified in the parameter area.

There is no need to execute the CMND(490) or CMND2(493) instruction or to monitor the completion timing and processing timing of the instruction, so this helps to simplify ladder programming.

A total of eight ports (UDP and TCP combined) can be used for socket services.

The performance of sending and receiving has been improved by using the option settings.



2) Executing CMND(490) or CMND2(493)

Another way to use socket services is to request a UDP or TCP socket service by sending a FINS command to the EtherNet/IP Unit by executing CMND(490) or CMND2(493) from the CPU Unit.

When the EtherNet/IP Unit receives the socket service request, the EtherNet/IP Unit and Built-in EtherNet/IP Port returns a response to the CPU Unit to confirm that it received the request, and then begins the requested processing.

When the processing is completed, the results are stored in the Results Storage Area in the CPU Unit.

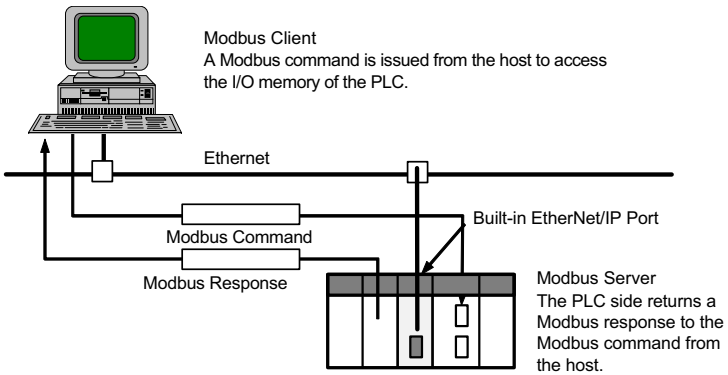
Eight TCP ports and eight UDP ports can be used.

Modbus Server/Client Functions

1) Modbus Server Functions

Allocating Modbus addresses in the I/O memory of the CPU Unit enables reading and writing in the I/O memory of the CPU Unit from a host PC, host PLC, HMI, or other Modbus client device. A Modbus TCP server and Modbus UDP server are supported, and a Modbus TCP server can be connected with up to eight clients.

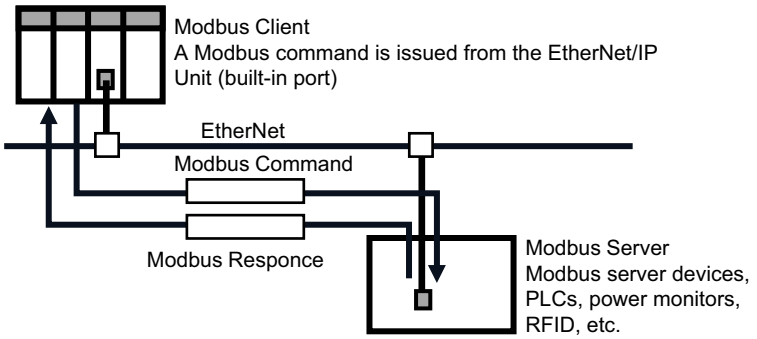
Note The Socket Service function is supported by the CJ3M-CPU3□.



2) Modbus Client Functions

The reading and writing of Modbus coils and registers can be performed by accessing devices (PLCs, etc.) that have the Modbus server function with function blocks using the socket service. Function blocks support Modbus TCP clients and Modbus UDP clients, which can each be connected with up to eight Modbus server devices.

Note The Socket Service function is supported by the CS1W/CJ1W-EIP21S and CJ3M-CPU3□.



1-5 Network Configurator Overview

1-5-1 Overview

Network Configurator for EtherNet/IP is a dedicated tool for building the network configuration and configuring various settings of EtherNet/IP compatible devices of multiple vendors including OMRON.

Network Configurator is included in CX-One.

The versions of Network Configurator that support EtherNet/IP Units (built-in ports) are as follows.

EtherNet/IP Units (built-in ports)	Network Configurator Version
CJ1W/CS1W-EIP21 CJ2H-CPU6□-EIP	Ver. 3.0 or later
CJ2M-CPU3□	Ver. 3.2 or later
CS1W/CJ1W-EIP21S	Ver. 3.74a or later
CJ3M-CPU3□	Ver. 3.78 or later

The Network Configurator provides the following functions for building, setting, and controlling EtherNet/IP.

Network Control

The Network configuration can be created and edited regardless of whether the Network Configurator is online or offline. The Network configuration can be read from a file or the network.

Hardware (EDS File) Control

EDS files used by the Network Configurator can be installed and deleted.

1-5-2 Network Configurator Requirements

Item		Specification	
Operating environment		Refer to the *CX-One Setup Manual* (W463). CXONE-AL□□C-V4/CXONE-AL□□D-V4	
Network connection method		**CS1/CJ1**	**CJ2/CJ3**
	Serial interface	CPU Unit's Peripheral or RS-232C port	CPU Unit's USB or RS-232C port
	Ethernet interface	EtherNet/IP Unit's Ethernet port	CPU Unit's Ethernet port EtherNet/IP Unit's Ethernet port
Location on Network		A single node address is used (only when directly connected to EtherNet/IP).	
Number of Units that can be connected to Network		A single Network Configurator per network (More than one Configurator cannot be used in the same system.)	
Main functions	Network control functions	• The network configuration can be created and edited regardless of whether the Network Configurator is online or offline. • The network configuration can be read from a file or the network.	
	Hardware control functions	The EDS files used by the Network Configurator can be installed and deleted.	
Supported file formats		Configurator network configuration files (*.nvf) Configuration files (*.ncf) created using the Network Configurator for EtherNet/IP (version 2) can be imported by selecting ***External Data - Import*** from the File Menu.	

1-5-3 Precautions When Using the Network Configurator

Only an OMRON EtherNet/IP Unit can be set as the originator for a connection using the Network Configurator.

- The Network Configurator can be connected to the EtherNet/IP network through the following ports:
  - CS1/CJ1-series CPU Unit's serial port (peripheral or RS-232C) or Ethernet port on EtherNet/IP Unit
  - CJ2/CJ3-series CPU Unit's serial port (USB or RS-232C), Ethernet port on EtherNet/IP Unit or built-in EtherNet/IP port
- The Network Configurator can be connected directly to the EtherNet/IP network from the computer's Ethernet port. When connecting directly to the EtherNet/IP network, an Ethernet port must be set up in the computer in advance. In this case, the Network Configurator will be connected to the EtherNet/IP network as a single node. If there isn't an unused node address available, the Network Configurator can't be connected directly to the EtherNet/IP network.

SECTION 2
Unit Specifications

This section provides the specifications of EtherNet/IP Unit and built-in EtherNet/IP port and introduces recommended network configuration devices.

2-1 EtherNet/IP Unit and Built-in EtherNet/IP Port Specifications 16
2-1-1 General Specifications 16
2-1-2 Unit Specifications. 16
2-1-3 Communications Specifications 24
2-1-4 Dimensions 28
2-1-5 Software Configuration 30
2-2 Nomenclature and Functions 31
2-2-1 Nomenclature and Functions 31
2-2-2 Switch Settings 37
2-3 Selecting the Network Devices 39
2-3-1 Recommended Network Devices 39
2-3-2 Network Devices Manufactured by OMRON. 39
2-3-3 Switching Hub Types. 39
2-3-4 Switching Hub Functions. 40
2-3-5 Precautions When Selecting a Switching Hub 40

2-1 EtherNet/IP Unit and Built-in EtherNet/IP Port Specifications

2-1-1 General Specifications

The general specifications conform to those of the CS-series and CJ-series PLCs.

2-1-2 Unit Specifications

CS-series EtherNet/IP Units

Item		Specifications
Model number		CS1W-EIP21/EIP21S
Type		100Base-TX (See note 1.)
Applicable PLCs		CS-series PLCs (See note 2.)
Unit classification		CS-series CPU Bus Unit
Mounting location (See note 3.)		CPU Rack or Expansion Rack
Number of Units that can be mounted		8 max. (including Expansion Racks)
CPU Unit words used	Allocated CIO Area words (CPU Bus Unit words)	25 words/Unit (one unit number's words)
		These words contain control bits and flags, the target node PLC's operating and error information, Unit status, communications status, registered/normal target node information, and FINS/TCP connection status.
	Allocated DM Area words (CPU Bus Unit words)	100 words/Unit (one unit number's words)
		These words contain the IP address display/setting area
	User-set area	Any usable data area words
		Target node PLC's operating and error information, and registered/normal target node information
	CPU Bus Unit System Setup	Not used.
Non-volatile memory within EtherNet/IP Unit (See note.)		The following settings are stored in the EtherNet/IP Unit's non-volatile memory. **Note** Unlike the regular Ethernet Units, the CPU Bus Unit Setup Area in the CPU Unit is not used for these settings. 1. Unit setup (communications settings for the EtherNet/IP Unit, such as the IP address, DNS server settings, host name, baud rate, FINS/UDP settings, and FINS/TCP settings) 2. Tag data link settings (device parameters) 3. User authentication settings (CS1W-EIP21S only) 4. Operation log (CS1W-EIP21S only)
Transfer specifications	Media access method	CSMA/CD
	Modulation method	Baseband
	Transmission paths	Star form
	Baud rate	100 Mbit/s (100Base-TX)
	Transmission media	Shielded twisted-pair (STP) cable Categories: 100 Ω at 5, 5e
	Transmission distance	100 m (distance between hub and node)
	Number of cascade connections	There is no limitation when a switching hub is used.
Current consumption (Unit)		CS1W-EIP21: 410 mA max. at 5 V DC CS1W-EIP21S: 620 mA max. at 5 V DC
Weight		CS1W-EIP21: 171 g max. CS1W-EIP21S: 180 g max.

Item	Specifications
Dimensions	35 × 130 × 101 mm (W × H × D)
Other general specifications	Other specifications conform to the general specifications of the CS-series

Note

(1) If tag data links are being used, use 100Base-TX. Otherwise, 10Base-T can be used, but this is not recommended.

(2) For the CS1W-EIP21S, the following CPU Units are supported. CS1G-CPU□□H, CS1H-CPU□□H, CS1D-CPU□□HA/H, CS1D-CPU□□SA/S, and CS1D-CPU□□P

(3) In a mixed configuration of the CS1W-EIP21 and the CS1W-EIP21S, the total number of CS1W-EIP21 and CS1W-EIP21S EtherNet/IP Units must not exceed the number of Units that can be mounted.

CJ-series EtherNet/IP Unit

Item		Specifications
Model number		CJ1W-EIP21/EIP21S
Type		100Base-TX (See note 1.)
Applicable PLCs		CJ-series PLCs (See note 2, 3, and 4.)
Unit classification		CJ-series CPU Bus Unit
Mounting location		CPU Rack or Expansion Rack
Number of Units that can be mounted (See note 5.)		8 max. (including Expansion Racks) **Note** Up to seven EtherNet/IP Units can be connected to a CJ2H-CPU□□-EIP or CJ3M-CPU3□ CPU Unit. A maximum of two EtherNet/IP Units can be connected to a CJ2M-CPU1□/3□ CPU Unit (regardless of whether the CPU Unit has a built-in port).
CPU Unit words used	Allocated CIO Area words (CPU Bus Unit words)	25 words/Unit (one unit number's words)
		These words contain control bits and flags, the target node PLC's operating and error information, Unit status, communications status, registered/normal target node information, and FINS/TCP connection status.
	Allocated DM Area words (CPU Bus Unit words)	100 words/Unit (one unit number's words)
		These words contain the IP address display/setting area.
	User-set area	Any usable data area words
		Target node PLC's operating and error information, and registered/normal target node information
	CPU Bus Unit System Setup	Not used.
Non-volatile memory within EtherNet/IP Unit (See note.)		The following settings are stored in the EtherNet/IP Unit's non-volatile memory. **Note** Unlike the regular Ethernet Units, the CPU Bus Unit Setup Area in the CPU Unit is not used for these settings. 1. Unit Setup (communications settings for the EtherNet/IP Unit, such as the IP address, DNS server settings, host name, baud rate, FINS/UDP settings, and FINS/TCP settings) 2. Tag data link settings (device parameters) 3. User authentication settings (CJ1W-EIP21S only) 4. Operation log (CJ1W-EIP21S only)
Transfer specifications	Media access method	CSMA/CD
	Modulation method	Baseband
	Transmission paths	Star form
	Baud rate	100 Mbit/s (100Base-TX)
	Transmission media	Shielded twisted-pair (STP) cable Categories: 100 Ω at 5, 5e
	Transmission distance	100 m (distance between hub and node)
	Number of cascade connections	There is no limitation when a switching hub is used.
Current consumption (Unit)		CJ1W-EIP21: 410 mA max. at 5 V DC CJ1W-EIP21S: 650 mA max. at 5 V DC
Weight		CJ1W-EIP21: 94 g max. CJ1W-EIP21S: 91 g max.
Dimensions		31 × 90 × 65 mm (W × H × D)
Other general specifications		Other specifications conform to the general specifications of the CJ-series.

Note (1) If tag data links are being used, use 100Base-TX. Otherwise, 10Base-T can be used, but this is not recommended.

(2) When mounted in a CJ2/CJ3-series CPU Unit, the following expanded area can be accessed.
IOM Area (Words A960 to A1471 and bits A10000 to A11535 in Auxiliary Area, banks D to 18 in EM Area)

(3) For the CJ1W-EIP21S, the following CPU Units are supported.
CJ3M-CPU□□, CJ2H-CPU□□, CJ2H-CPU□□-EIP, CJ2M-CPU□□, CJ1G-CPU4□P, CP1H-X40D□-□, CP1H-XA40D□-□, and CP1H-Y20DT-D
When connected to the CP1H CPU Units, the following of the security features of the CJ1W-EIP21S cannot be used with the CX-Programmer and PLC backup tools.
- Secure communications
- User authentication
- Operation log

(4) For information on support for NJ-series CPU Units, refer to the *CJ-series EtherNet/IP Units Operation Manual for NJ-series CPU Unit* (Cat. No. W495).

(5) In a mixed configuration of the CJ1W-EIP21 and the CJ1W-EIP21S, the total number of CJ1W-EIP21 and CJ1W-EIP21S EtherNet/IP Units must not exceed the number of Units that can be mounted.

CJ2/CJ3 CPU Built-in EtherNet/IP Port

Item		Specifications
Model number		CJ2H-CPU□□-EIP, CJ2M-CPU3□, CJ3M-CPU3□
Type		100Base-TX (See note.)
Unit classification		CJ2/CJ3 CPU Unit built-in port
CPU Unit words used	Allocated CIO Area words (CPU Bus Unit words)	25 words/Unit (one unit number's words)
		These words contain control bits and flags, the target node PLC's operating and error information, Unit status, communications status, registered/normal target node information, and FINS/TCP connection status.
	Allocated DM Area words (CPU Bus Unit words)	100 words/Unit (one unit number's words)
		These words contain the IP address display/setting area.
	User-set area	Any usable data area words
		Target node PLC's operating and error information, and registered/normal target node information
	CPU Bus Unit System Setup	Not used.
Non-volatile memory for the CJ2/CJ3 built-in EtherNet/IP port		The following settings are stored in the non-volatile memory for the CJ2/CJ3 CPU Unit. **Note** Unlike the regular Ethernet Units, the CPU Bus Unit Setup Area in the CPU Unit is not used for these settings. 1. Unit Setup (communications settings for the built-in EtherNet/IP port, such as the IP address, DNS server settings, host name, baud rate, FINS/UDP settings, and FINS/TCP settings) 2. Tag data link settings (device parameters)
Transfer specifications	Media access method	CSMA/CD
	Modulation method	Baseband
	Transmission paths	Star form
	Baud rate	100 Mbit/s (100Base-TX)
	Transmission media	Shielded twisted-pair (STP) cable Categories: 100 Ω at 5, 5e
	Transmission distance	100 m (distance between hub and node)
	Number of cascade connections	There is no limitation when a switching hub is used.
Current consumption (Unit)		Refer to CJ-series CJ2 CPU Unit Hardware User's Manual (W472), CJ3 CPU Unit Hardware User's Manual (W664).
Weight		
Dimensions		
Other general specifications		Other specifications conform to the CJ2/CJ3 CPU Unit.

Note If tag data links are being used, use 100Base-TX. Otherwise, 10Base-T can be used, but this is not recommended.

Restrictions for Installation (CS1W/CJ1W-EIP21S Only)

Coping with Long Unit Startup Time

The startup time of CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ EtherNet/IP Units is several seconds longer than that of other EtherNet/IP Units.

After power ON, the CPU Unit can start operation when all the Special I/O Units and CPU Bus Units have been recognized. For this reason, the CPU Unit startup time is several seconds longer in a system that includes the CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ than in a system that does not include it.

Check the effect on the system's initial setup operation.

Coping with the Need to Continue Power Supply When the System Power Is Turned OFF

The startup time of CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ Units with a hardware revision of None is several seconds longer than that of other EtherNet/IP Units. For this reason, there are restrictions on the selection of the Power Supply Unit when using the power OFF detection time. Use that does not comply with the restrictions may cause the Unit to fail.

■ Restrictions on the Power Supply Unit Usage

CJ1W-EIP21S with lot number 250331 or earlier (indication of mounting compatibility is no printing or "+NJ") cannot use the Power Supply Unit CJ1W-PD022. Use another CJ-series Power Supply Unit or use CJ1W-EIP21S with lot number 250401 or later (indication of mounting compatibility "+CJ/CP/NJ").

The relationship between the lot number, hardware revision, and indication of mounting compatibility (printing at the lower right of the Unit's front panel) is as follows.

Lot number	Hardware revision	Indication of mounting compatibility (printing at the lower right of the Unit's front panel)
250401 or later	"A"	"+CJ/CP/NJ"
241001 to 250331	None	"+NJ"
240930 or earlier	None	No printing

The printing at the lower right of the Unit's front panel means as follows.

Printing	Mean
CJ	No restrictions for the CJ-series Power Supply Units. (see *Restrictions for Installation (CS1W/CJ1W-EIP21S Only)* in *2-1-2 Unit Specifications*.
CP	Can be connected to the CP1H-series CPU Units.
NJ	Can be connected to the NJ-series CPU Units. (See CJ-series EtherNet/IP Units Operation Manual for NJ-series CPU Unit.)

When setting the power OFF detection time, there are the following usage restrictions depending on the input power voltage conditions of the Power Supply Unit.

Power Supply Unit		Condition of supply voltage and applicability of Power Supply Unit *1			Remarks
Supported PLC	**Model**	**200 VAC or higher**	**Lower than 200 VAC**	**DC input**	
CJ Series (CJ1, CJ2 and CJ3)	CJ1W-PA202	Yes	Yes	---	CJ1W-EIP21S with lot number 250331 or earlier (indication of mounting compatibility is no printing or “+NJ”) cannot use the power OFF detection time below 200 VAC.
	CJ1W-PA205C	Yes	Yes	---	
	CJ1W-PA205R	Yes	Yes	---	
	CJ1W-PD025	---	---	Yes	CJ1W-EIP21S with lot number 250331 or earlier (indication of mounting compatibility is no printing or “+NJ”) cannot use the power OFF detection time.
	CJ1W-PD022	---	---	No	The setting of the power OFF detection time cannot be used. CJ1W-EIP21S with lot number 250331 or earlier (indication of mounting compatibility is no printing or “+NJ”) cannot use CJ1W-PD022 with or without the setting of the power OFF detection time.

Power Supply Unit		Condition of supply voltage and applicability of Power Supply Unit *1			Remarks
Supported PLC	**Model**	**200 VAC or higher**	**Lower than 200 VAC**	**DC input**	
CS Series	C200HW-PA204	Yes	No	---	Depending on the date of manufacture, the supply voltage is not wide range, but is switchable. For details, refer to the CS-series Programmable Controllers Operation Manual (Cat. No. W339).
	C200HW-PA204R	Yes	No	---	
	C200HW-PA204C	Yes	No	---	---
	C200HW-PA204S	No	No	---	---
	C200HW-PA209R	No	No	---	---
	C200HW-PD024	---	---	No	---
	C200HW-PD025	---	---	No	---
CS Series	CS1D-PA207R	No	No	---	---
	CS1D-PA207R	---	---	No	---
	CS1D-PD025	---	---	No	---

*1 Use the supply voltage within the allowable power supply voltage fluctuation range.

2-1-3 Communications Specifications

Item			CS1W/CJ1W-EIP21S CS1W/CJ1W-EIP21 when connected to CS1/CJ1/CP1H CPU Unit	CS1W/CJ1W-EIP21S CS1W/CJ1W-EIP21 when connected to CJ2/CJ3 CPU Unit, or CJ2H-CPU6□-EIP, CJ3M-CPU3□ built-in EtherNet/IP port	CJ2M-CPU3□ CPU built-in EtherNet/IP port
CIP service	Tag data links (Cyclic communications)	Number of connections	256		32
		Packet interval (refresh cycle)	0.5 to 10,000 ms (in 0.5-ms units) Can be set independently for each connection. (Data is refreshed over the network at the preset interval and does not depend on the number of nodes.)		1 to 10,000 ms (in 0.5-ms units) Can be set independently for each connection. (Data is refreshed over the network at the preset interval and does not depend on the number of nodes.)
		Allowed communications bandwidth per Unit	6,000 to 12,000 pps (See note 1.) (Units with unit version 2.1 or earlier excluding EIP21S: 6,000 pps) **Note** Including the heartbeat.		3000 pps (See note 1.) **Note** Including the heartbeat.
		Number of tags that can be registered	256		32
		Tag types	CIO Area, DM Area, EM Area, Holding Area, Work Area, and network symbols (See note 8.)		
		Number of tags per connection (= 1 tag set)	8 (7 tags when the tag set contains the PLC status)		
		Maximum link data size per node (total size of all tags)	184,832 words		640 words (See note 9.)
		Maximum data size per connection	252 words or 722 words (See note 2.) **Note** Data synchronicity is maintained within each connection.		640 words (See note 9.) **Note** Data synchronicity is maintained within each connection.
		Number of registrable tag sets	256 (1 connection = 1 tag set)		32 (1 connection = 1 tag set)
		Maximum size of 1 tag set	722 words (The PLC status uses 1 word when the tag set contains the PLC status.)		640 words (The PLC status uses 1 word when the tag set contains the PLC status.)
		Maximum number of tags that can be refreshed per CPU Unit cycle (See note 3.)	Output/Transmission (CPU → EtherNet/IP): 19 Input/Reception (EtherNet/IP → CPU): 20 (See note 4.)	Output/Transmission (CPU → EtherNet/IP): 256 Input/Reception (EtherNet/IP → CPU): 256	Output/Transmission (CPU → EtherNet/IP): 32 Input/Reception (EtherNet/IP → CPU): 32

Item			CS1W/CJ1W-EIP21S CS1W/CJ1W-EIP21 when connected to CS1/CJ1/CP1H CPU Unit	CS1W/CJ1W-EIP21S CS1W/CJ1W-EIP21 when connected to CJ2/CJ3 CPU Unit, or CJ2H-CPU6□-EIP, CJ3M-CPU3□ built-in EtherNet/IP port	CJ2M-CPU3□ CPU built-in EtherNet/IP port
CIP service	Tag data links (Cyclic communi-cations)	Data that can be refreshed per CPU Unit cycle (See note 3.) (The layout of the allo-cated CIO Area words is the default.) (See note 10.)	Output/Transmission (CPU → EtherNet/IP): 7,469 words Input/Reception (EtherNet/IP → CPU): 7,469 words	Output/Transmission (CPU → EtherNet/IP): 6,432 words Input/Reception (EtherNet/IP → CPU): 6,432 words	Output/Transmission (CPU → EtherNet/IP): 640 words Input/Reception (EtherNet/IP → CPU): 640 words
		Changing tag data link parameters during operation	Supported (See note 5.)		
		Multicast packet filter function (See note 6.)	Supported		
		QuickConnect	Originator only is supported (See note 13.)		Not supported
CIP service	Explicit messaging	Class 3 (connected)	Number of connections: 128		
		UCMM (unconnected)	Number of clients that can communicate at one time: 32 max. Number of servers that can communicate at one time: 32 max.		Number of clients that can communicate at one time: 16 max. Number of servers that can communicate at one time: 16 max.
		CIP routing	CS1W-EIP21/EIP21S CJ1W-EIP21/EIP21S CJ2H-CPU□□-EIP CJ2M-CPU3□ CJ3M-CPU3□		
FINS service (See note 7.)		FINS/UDP	Supported		
		FINS/TCP	16 connections max.		
Modbus		Modbus UDP Server	Not supported	Supported (See note 11.)	Not supported
		Modbus TCP Server	Not supported	8 connections max. (See note 11.)	Not supported
		Modbus UDP Client (See note 12.)	Not supported	8 connections max. Possible with a function block using the socket service by CMND2 instruction.	Not supported
		Modbus TCP Client (See note 12.)	Not supported	8 connections max. Possible with a function block using the socket service by CMND2 instruction.	Not supported
SNMP		Agent	SNMPv1, SNMPv2C, and SNMP trap		
		MIB	MIB-II		
SNTP			Supported		
FTP Server			Supported		
DNS			Supported SNMP, SNTP only.		
Procol			TCP/IP, UDP, ARP, ICMP (ping only), IGMP, BOOTP, and LLDP (See note 11.)		

Item	CS1W/CJ1W-EIP21S CS1W/CJ1W-EIP21 when connected to CS1/CJ1/CP1H CPU Unit	CS1W/CJ1W-EIP21S CS1W/CJ1W-EIP21 when connected to CJ2/CJ3 CPU Unit, or CJ2H-CPU6□-EIP, CJ3M-CPU3□ built-in EtherNet/IP port	CJ2M-CPU3□ CPU built-in EtherNet/IP port
EtherNet/IP conformance test	CJ3M-CPU3□: CT21 CJ1W-EIP21S/CS1W-EIP21S: CT17 Other than CJ3M-CPU3□ or CJ1W-EIP21S/CS1W-EIP21S: CT11		
Ethernet interface	10BASE-T or 100BASE-TX Auto Negotiation or fixed settings Auto MDI or MDI-X		10BASE-T or 100BASE-TX Auto Negotiation or fixed settings

Note

(1) In this case, pps means “packets per second” and indicates the number of packets that can be processed in one second.

(2) To use 505 to 1,444 bytes as the data size, the system must support the Large Forward Open standard (an optional CIP specification). The CS/CJ-series Units support this standard, but before connecting to nodes of other companies, confirm that those devices also support it.

(3) If the maximum data size is exceeded, the data refreshing with the CPU Unit will extend over two or more cycles.

(4) If status layout is set to user settings, the maximum number of tags is as follows.

Condition	Output/Transmission	Input/Reception
CS1W/CJ1W-EIP21S	18	18
CS1W/CJ1W-EIP21	19	19

(5) If parameters are changed in the EtherNet/IP Unit, however, the EtherNet/IP Unit will be restarted. When other nodes are communicating with the affected node, the communications will temporarily time out and automatically recover later.

(6) Because the EtherNet/IP Unit is equipped with an IGMP client (version 2), unnecessary multicast packets can be filtered by using a switching hub that supports IGMP snooping.

(7) The EtherNet/IP Unit uses the TCP/UDP port numbers shown in the following table.
Other services than those shown in the table blow are not supported.

Service	Protocol	Port number	Default value of port		Remarks
			Product A group*3	Product B group*3	
Tag data links	UDP	2222	Open	Open	The port number is fixed.
CIP message communications (Class 3, UCMM)	TCP/UDP	44818	Open	Open	
DNS	UDP	53	Closed	Closed	
Secure Comm	TCP	443	Open*1	Unsupported	The port number is fixed.
SSH/SFTP	TCP	22	Closed	Unsupported	The port number is fixed. It is for maintenance.

Service	Protocol	Port number	Default value of port		Remarks
			Product A group*3	Product B group*3	
FINS/UDP service	UDP	9600	Closed	Open	The port number can be changed by Unit Setup of the CX-Programmer.
FINS/TCP service	TCP	9600	Closed	Open	
Modbus Server *2	TCP	502	Closed	Unsupported	
	UDP	502	Closed	Unsupported	
FTP	TCP	20, 21	Closed	Open	
SNTP	UDP	123	Closed	Closed	
SNMP	UDP	161	Closed	Closed	
SNMP trap	UDP	162	Closed	Closed	

*1 The value is Closed when the CJ1W-EIP21S is mounted on NJ-series CPU Units.

*2This is enabled for CJ3M-CPU3☐ only.

*3The product A group is CS1W/CJ1W-EIP21S and CJ3M-CPU3☐. The product B group is CS1W/CJ1W-EIP21, CJ2H-CPU6☐-EIP and CJ2M-CPU3☐.

(8) Network symbols can be used for the following CPU Units.
The CJ2 CPU Units of CJ2H-CPU6☐(-EIP) with unit version 1.6 or later, CJ2M-CPU☐☐ with unit version 2.2 or later, and CJ3M CPU☐☐.

(9) Unit version 2.0: 20 words maximum.

(10) The table below shows values when the layout type is *User defined*. The values differ between the CS1W/CJ1W-EIP21 and CS1W/CJ1W-EIP21S.

		When connected to CS1/CJ1/CP1H CPU Unit		When connected to CJ2/CJ3 CPU Unit	
		EIP21	EIP21S	EIP21	EIP21S
Data (words) that can be refreshed per CPU Unit cycle	Output/ Transmission	7,405	7,321	6,368	6,172
	Input/ Reception	7,405	7,385	6,368	6,236

(11) This is enabled for CJ3M-CPU3☐ only.

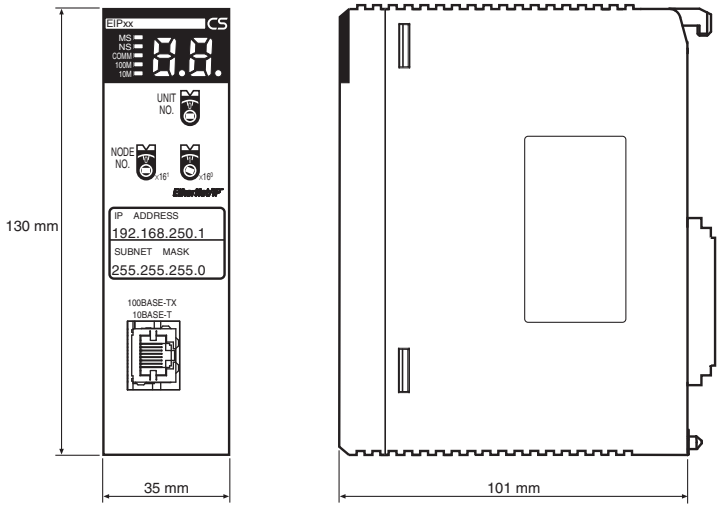
(12) This is enabled for CS1W/CJ1W-EIP21S connected to the CJ3M-CPU3☐ and CJ2/CJ3 CPU Unit only.

(13) This is enabled for CJ3M-CPU3☐ or CS1W/CJ1W-EIP21S only.

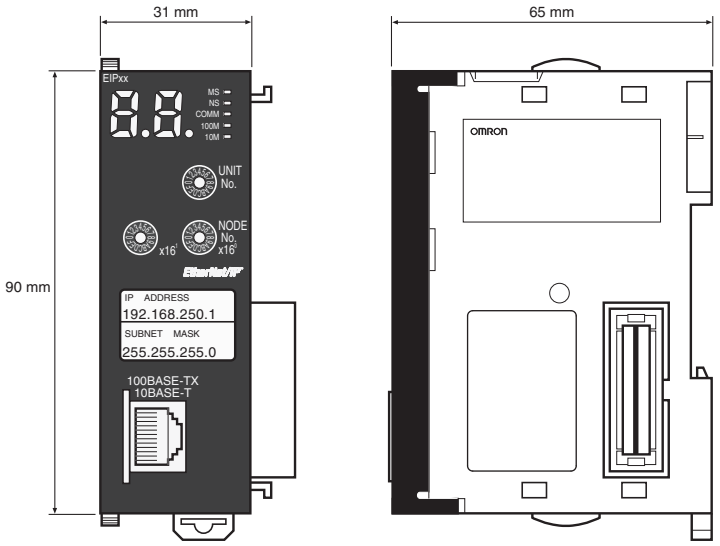
Note The communications specifications of EtherNet/IP ports on CJ2M-CPU3☐ Units depend on the unit version. Check the differences in specifications between unit versions carefully before using a port.

2-1-4 Dimensions

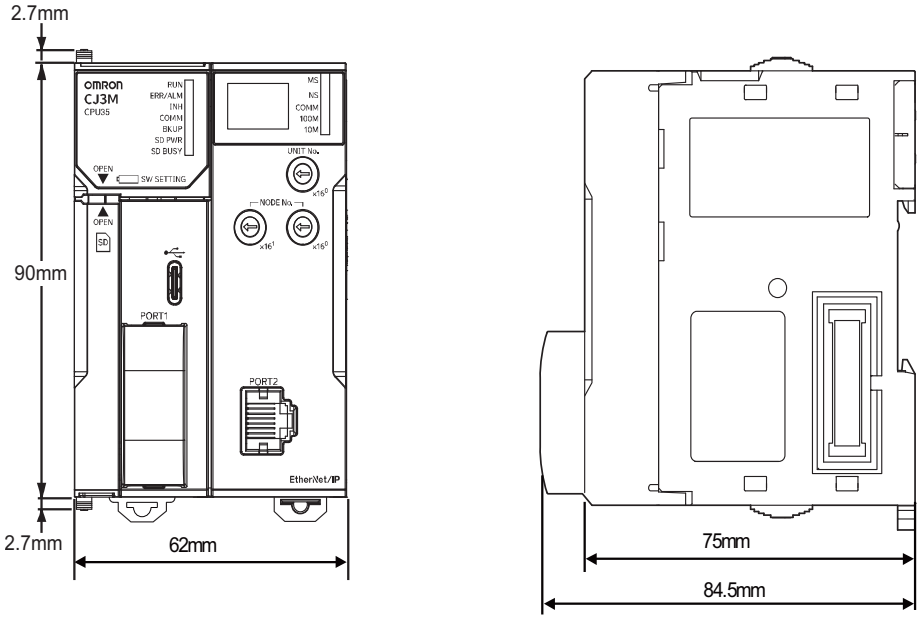
CS1W-EIP21/EIP21S



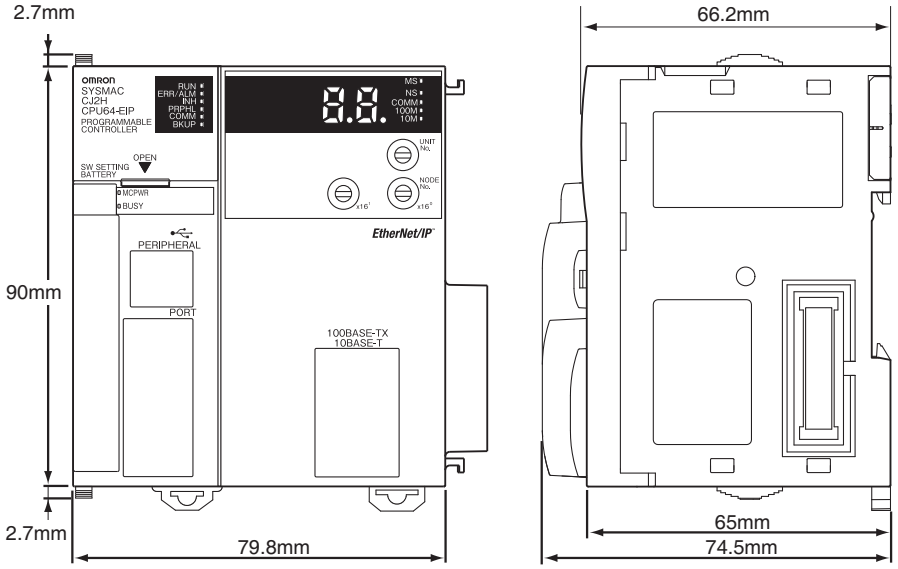
CJ1W-EIP21/EIP21S



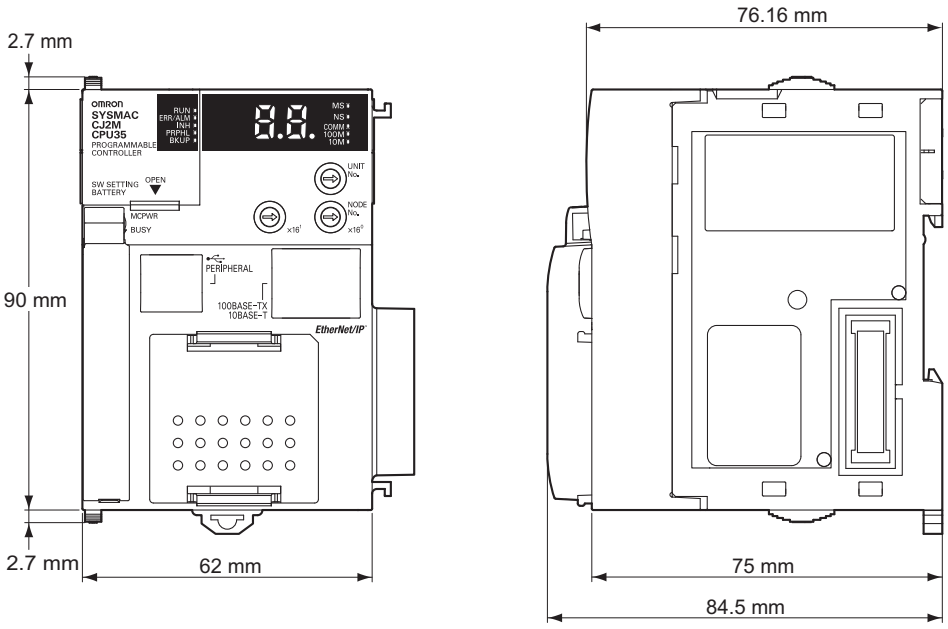
CJ3M-CPU3□



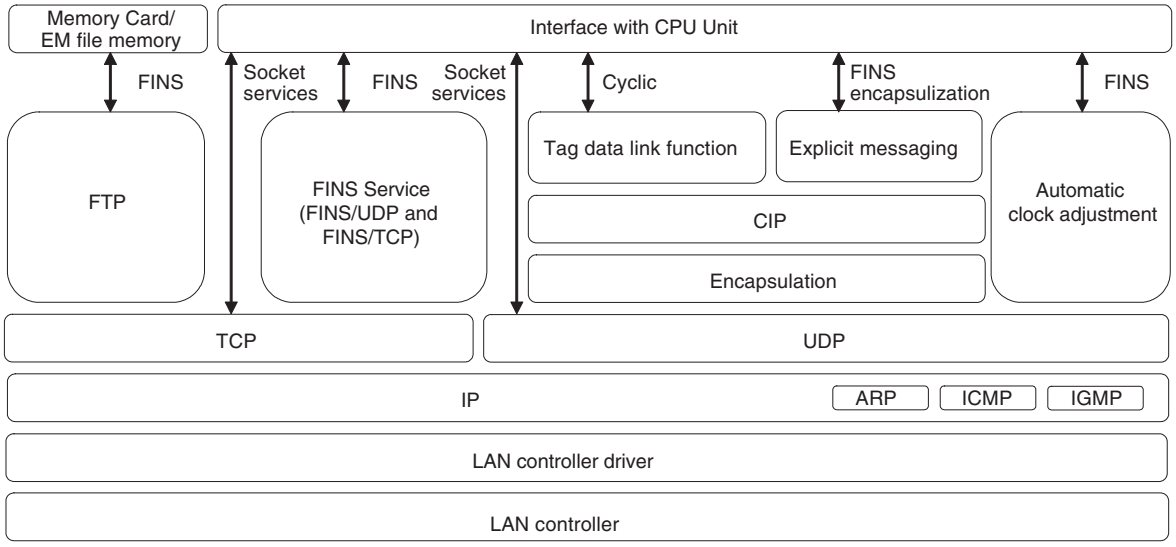
CJ2H-CPU□□-EIP



CJ2M-CPU3□



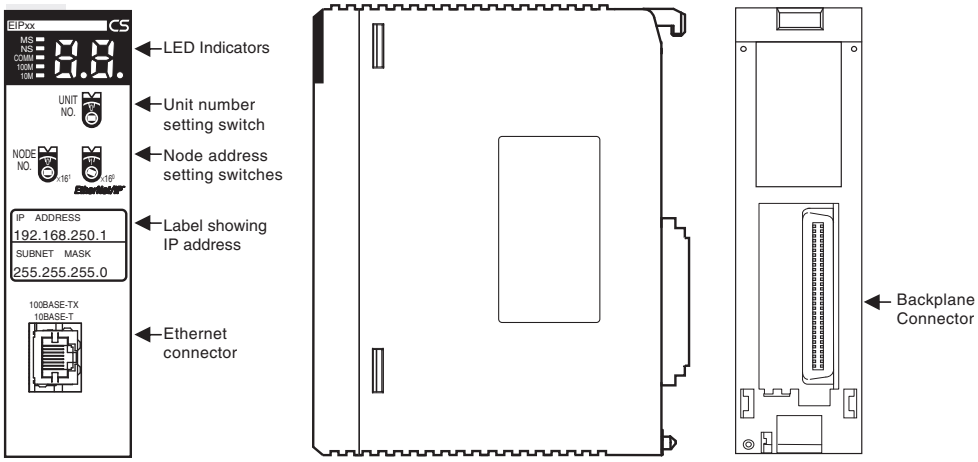
2-1-5 Software Configuration



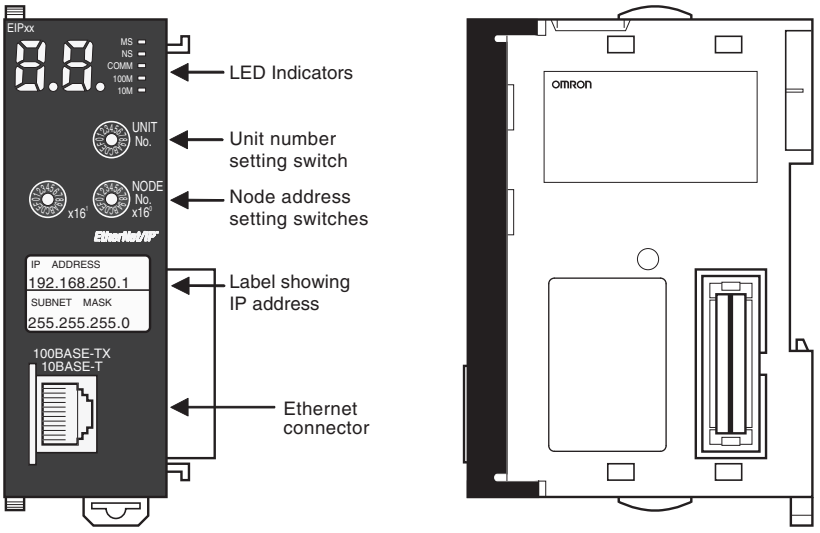
2-2 Nomenclature and Functions

2-2-1 Nomenclature and Functions

CS1W-EIP21/EIP21S

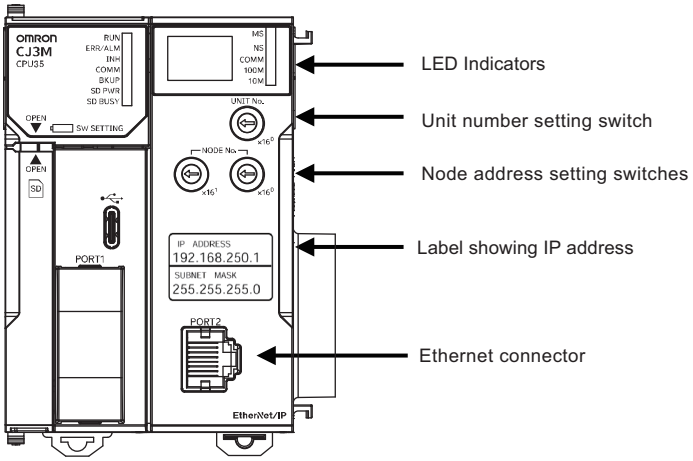


CJ1W-EIP21/EIP21S

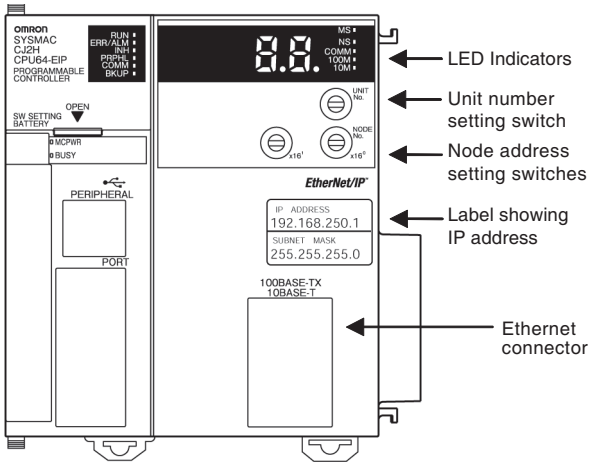


Note For the CJ1W-EIP21S, which can be mounted on NJ-series CPU Units, “+NJ” or “+CJ/CP/NJ” is printed at the lower right of the Unit’s front panel.
For the CJ1W-EIP21S, which can be mounted on CP1H series CPU Units, “+CJ/CP/NJ” is printed at the lower right of the Unit’s front panel.

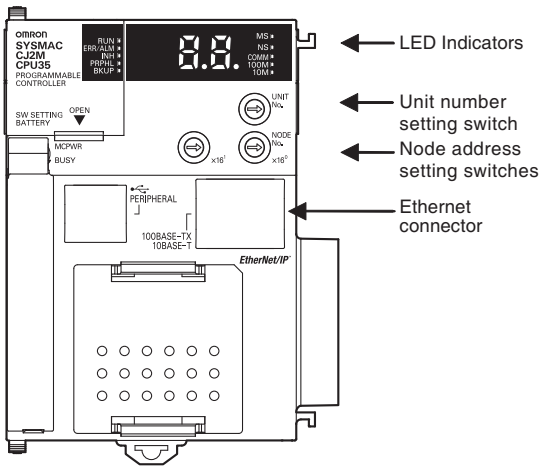
Built-in EtherNet/IP Port in CJ3M-CPU3□



Built-in EtherNet/IP Port in CJ2H-CPU□□-EIP

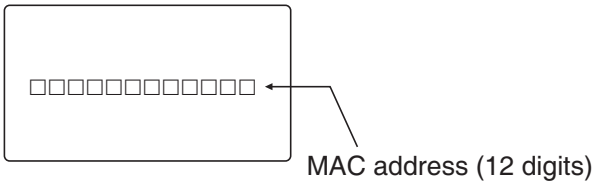


Built-in EtherNet/IP Port in CJ2M-CPU3□



MAC Address Notation

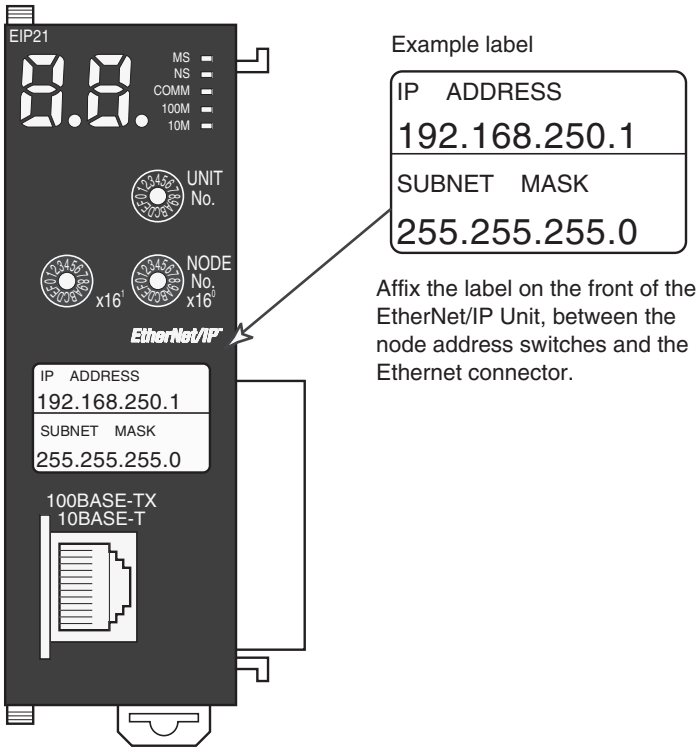
A specific MAC address is allocated to all devices connected to the Ethernet network. The EtherNet/IP Unit's address is listed in 12-digit hexadecimal on the right side of the Unit.



Note

(1) For details, refer to *Appendix E FINS Commands Addressed to EtherNet/IP Units or Built-in EtherNet/IP Ports*.

(2) An IP address label is included with the EtherNet/IP Unit, so the user can record the user-set IP address and subnet mask on the label, and affix the label to the front of the Unit. When this label is affixed to the front of the Unit, it is easy to confirm the Unit's IP address and subnet mask.



Indicators

An EtherNet/IP Unit or built-in EtherNet/IP port is equipped with the following indicators that indicate the operating status of the node itself and the overall network.

CS1W-EIP21/EIP21S



CJ1W-EIP21/EIP21S, CJ2H-CPU□□-EIP, CJ2M-CPU3□, and CJ3M-CPU3□



Status Indicators: MS, NS, COMM, 100M, and 10M

The MS (Module Status) indicator indicates the status of the node itself and the NS (Network Status) indicator indicates the status of the network.

The COMM, 100M, and 10M indicators indicate the status of Ethernet communications.

The MS and NS indicators can be green or red. The COMM, 100M, and 10M indicators are yellow. These indicators can be lit, flashing, or not lit. The following table shows the meaning of these indicator conditions.

Refer to *SECTION 16 Modbus Client Function* for details on using these indicators for troubleshooting.

Indicator	Name	Color	LED status	Indicated operating status
MS	Module Status	Red	Lit	Fatal error
			Flashing	Recoverable error
		Green	Lit	Normal
			Flashing*1	IP address not set
		---	Not lit	Power supply OFF
NS	Network Status	Red	Lit	Fatal error
			Flashing	Recoverable error
		Green	Lit	Tag data link and message connections established
			Flashing	Tag data link and message connections not established
		---	Not lit	Offline or power supply OFF
COMM	Communication	Yellow	Lit	Transferring data
			Not lit	Not transferring data
100M	100 Mbps	Yellow	Lit	100BASE-TX link established
			Not lit	100BASE-TX link not established
10M	10 Mbps	Yellow	Lit	10BASE-TX link established
			Not lit	10BASE-TX link not established

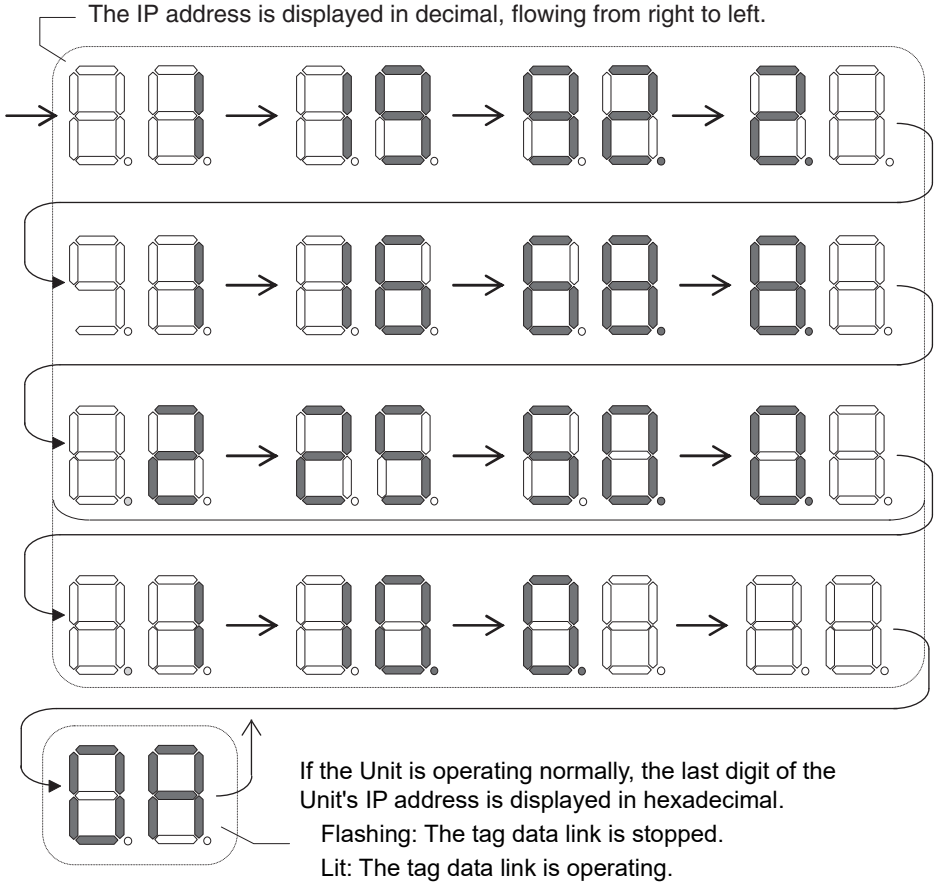
*1 This is enabled for CS1W/CJ1W-EIP21S, CJ3M-CPU3□ only.

Seven-segment Display

When the power is turned ON (or the Unit is restarted), all of the segments will flash twice, the IP address set in the EtherNet/IP Unit or built-in EtherNet/IP port will be displayed on the 7-segment display just once, from right to left. Afterwards, the rightmost 8 bits of the IP address is displayed in hexadecimal during normal operation.

If the d5 error (verification error, target nonexistent) mask is enabled, the right dot on the hexadecimal display of the lower 8 bits of the IP address will light.

Example 1: Displaying IP Address 192.168.250.10

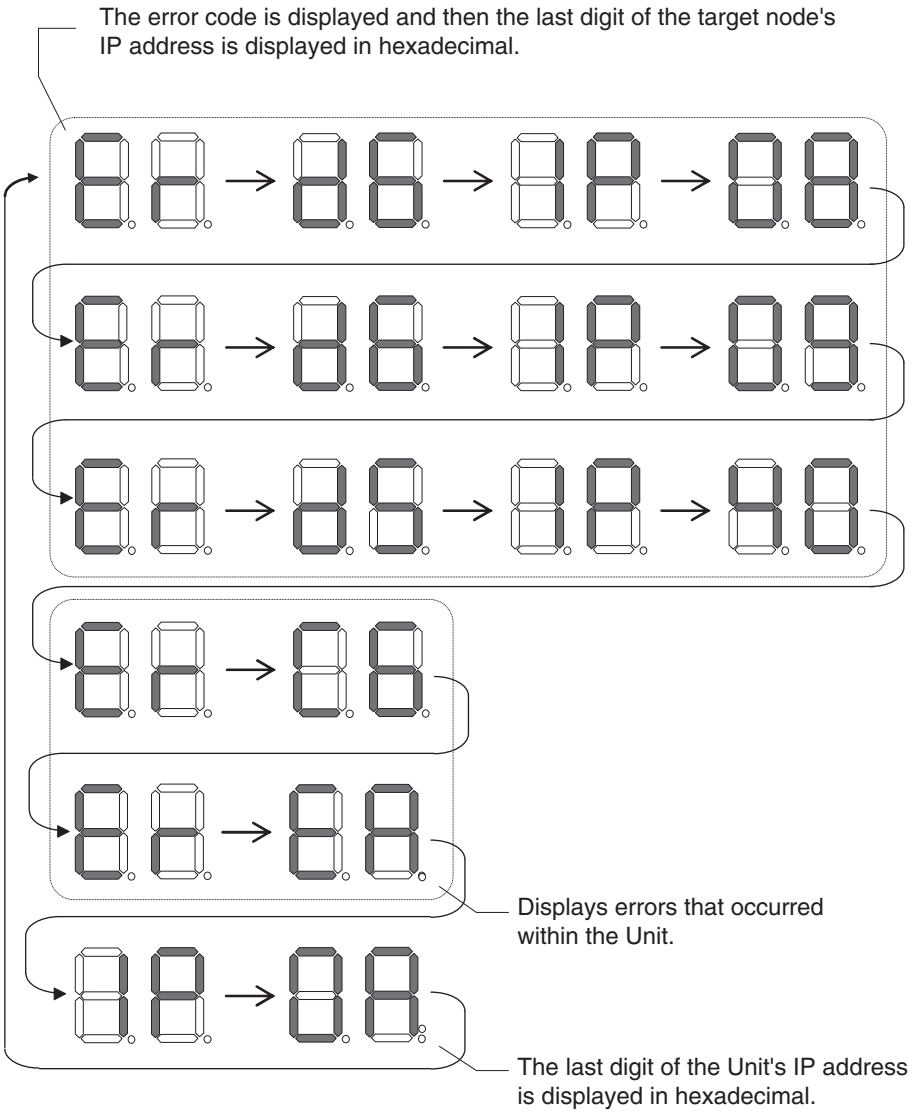


If an error occurs, the error code will be displayed alternately with the rightmost byte of the affected device's IP address. For details on error codes, refer to *SECTION 16 Modbus Client Function*.

Note For EtherNet/IP Units or built-in EtherNet/IP ports that are manufactured in January 2014 or later, you can use a d5 error (verification error, target nonexistent) mask.

Displaying Multiple Error Sources

- A d6 error (failed to establish connection) occurred with IP address 192.168.250.8.
- A d6 error (failed to establish connection) occurred with IP address 192.168.250.9.
- A d5 error (verification error, target nonexistent) occurred with IP address 192.168.250.64.
- A C6 error (multiple switches ON) and EA error (EtherNet/IP expansion setting error) occurred at the local EtherNet/IP Unit or built-in EtherNet/IP port, IP address 192.168.250.10.



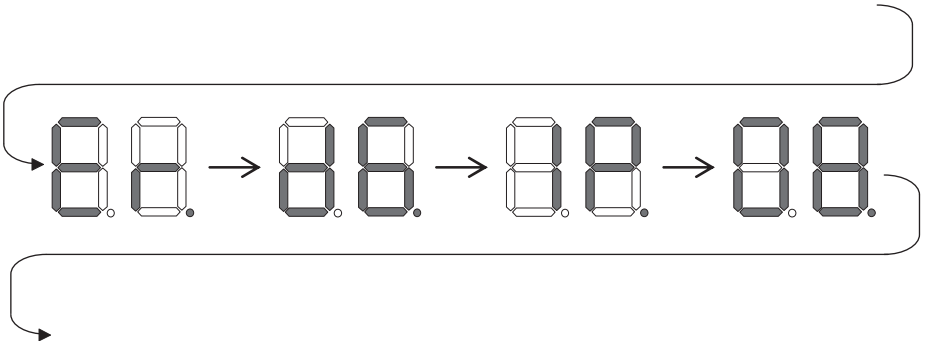
- There is no particular priority to the order in which the errors are displayed. All of the errors are displayed repeatedly in order.

Right and Left Dot LEDs

If an error occurred in two or more devices with the same rightmost byte in their IP addresses, the Right Dot LED will be lit while the devices' error is being displayed.

Example: Displaying the Following Errors

- A d6 error (failed to establish connection) occurred with IP address 10.0.1.8.
- A d6 error (failed to establish connection) occurred with IP address 10.0.2.8.



2-2-2 Switch Settings

Unit Number Setting Switch

The Unit Number Setting Switch sets the unit number of the EtherNet/IP Unit or built-in EtherNet/IP port as a CPU Bus Unit. The unit number determines which data area words are allocated to the Unit to contain data such as control bits, flags, status information, and connection information.



Setting method	Setting range
One-digit hexadecimal	0 to F

Note The unit number is factory-set to 0.

The unit number can be set to any number in the setting range (0 to F), as long as the same number is not set on another CPU Bus Unit in the same PLC.

Note

(1) Use a small screwdriver to make the setting, and be sure not to damage the rotary switch.

(2) Always turn OFF the PLC's power supply before setting the unit number.

(3) The unit number is factory-set to 0.

(4) If the same unit number is set on more than one CPU Bus Unit mounted in a PLC, a unit number duplication error will occur in the PLC and the EtherNet/IP Unit or built-in EtherNet/IP port will not be able to start operating.

Node Address Setting Switch

The Node Address Setting Switch sets the node address of the EtherNet/IP Unit or built-in EtherNet/IP port.



Setting method	Setting range
Two-digit hexadecimal	01 to FE

Note The node address is factory-set to 01. With the default settings, the values set on these switches become the last two digits of the local IP address of the EtherNet/IP Unit or built-in EtherNet/IP port.

Default IP address = 192.168.250.node address
With the factory-default node address setting of 01, the default IP address is 192.168.250.1.

The node address can be set to any number in the setting range (01 to FE), as long as the same address is not set on another node in the network.

Note If the node address setting is changed during operation, the MS Indicator will flash red.

2-3 Selecting the Network Devices

2-3-1 Recommended Network Devices

The following table shows the devices recommended for use with the EtherNet/IP.

Part	Maker	Model number	Inquires
Switching Hub	OMRON Corporation	W4S1-05D	Number of ports: 5
	Cisco Systems, Inc.	Consult the manufacturer.	---
	Contec USA, Inc.	Consult the manufacturer.	---
	Phoenix Contact	Consult the manufacturer.	---
Twisted-pair cable (100BASE-TX)	KURAMO ELECTRIC Co., Ltd.	KETH-SB	AWG24 × 4P, Cat5e
		KETH-PSB-OMR	AWG22 × 2P, Cat5e
	JMACS Japan Co., Ltd.	IETP-SB	AWG24 × 4P, Cat5e
		PNET/B	AWG22 × 2P, Cat5e
Connectors (STP plug)	Panduit Corporation	MPS588-C	For AWG24
	OMRON Corporation	XS6G-T421-1	For AWG22

Note (1) Always use a switching hub when using tag data links in the network.

(2) If a repeater hub is used for EtherNet/IP tag data links (cyclic communications), the network's communications load will increase, data collisions will occur frequently, and stable communications will be impossible.

2-3-2 Network Devices Manufactured by OMRON

The following network devices are manufactured by OMRON for EtherNet/IP networks.

Name	Model	Function	Number of ports	Error detection output
Switching Hub	W4S1-05D	Packet priority control (QoS): EtherNet/IP control data priority Failure detection: Broadcast storm, LSI error detection, 10/100Base-TX, Auto-Negotiation	5	None

2-3-3 Switching Hub Types

Unmanaged Layer 2 (L2) Switching Hubs

These switching hubs use the Ethernet MAC address to switch ports. Ordinary switching hubs have this function. Switching hub functions and settings cannot be changed.

Managed Layer 2 (L2) Switching Hubs

These switching hubs use the Ethernet address to switch ports. Switching hub functions and settings can be changed using special software tools for switching hubs running on a network node. Analytical data can also be collected. These switching hubs provide more-advanced functions than unmanaged layer 2 switching hubs.

2-3-4 Switching Hub Functions

This section describes the switching hub functions that are important when using an EtherNet/IP network. When using an EtherNet/IP Unit, set the following two functions.

- Multicast filtering
- QoS (Quality of Service) for TCP/UDP port numbers (L4)

Multicast Filtering

Multicast filtering transfers multicast packets to the specific nodes only. This function is implemented in the switching hub as IGMP Snooping or GMRP. “Specific nodes” are nodes equipped with an IGMP client that have made transfer requests to the switching hub. (OMRON EtherNet/IP Units are equipped with an IGMP client.)

When the hub does not use multicast filtering, multicast packets are sent to all nodes, just like broadcast packets, which increases the traffic in the network. Settings must be made in the switching hub to enable this function.

There must be enough multicast filters for the network being used.

QoS (Quality of Service) Function for TCP/UDP Port Numbers (L4)

This function controls the priority of packet transmissions so that packets can be sent with higher priority to a particular IP address or TCP (UDP) port. The TCP and UDP protocols are called transport layer protocols, leading to the name L4 (layer 4) QoS function.

When tag data links and message communications are executed on the same network, tag data links can be sent at higher priority to prevent problems such as transmission delays due to message communications traffic and packet losses due to buffer overflow. Settings must be made in the switching hub to enable this function and give higher priority to tag data link packets.

Support for the above two functions is as follows for the different types of switching hubs.

Hub	Multicast filtering	L4 QoS	Remarks
Unmanaged L2 switching hub	None	None	---
Managed L2 switching hub	Provided.	Provided.	Both functions must be set with a special software tool.
OMRON W4S1-series Switching Hubs	None	Provided.	L4 QoS is set using a switch. No software tool is necessary.

Note If the Network Configurator is used to set the connection type in the connection settings to a multicast connection, multicast packets will be used. If the connection type is set to a point-to-point connection, multicast packets will not be used.

2-3-5 Precautions When Selecting a Switching Hub

The functions supported by the switching hub may affect tag data link transmission delays and the configuration. In addition, if the switching hub supports advanced functions, special settings are required for those functions.

When selecting a switching hub, it is necessary to consider whether the switching hub will be selected based on the kind and amount of communications that will be performed in the network or the kind of switching hub that you want to use. Refer to the following precautions when selecting a switching hub.
Refer to *10-2 Adjusting the Communications Load* to estimate the communications load for tag data links.

Selecting the Switching Hub Based on the Types of Network Communications

Executing Tag Data Links Only

We recommend using an L2 switching hub without multicast filtering or an L2 switching hub with multicast filtering.

Using an L2 switching hub with multicast filtering prevents increased traffic due to unnecessary multicast packets, so the tag data links can operate at higher speed. If either of the following conditions exists, the amount traffic will be the same for both kinds of L2 switching hubs (with or without multicast filtering).

- The tag data links are set to share the same data with all nodes in the network. (The multicast packets are transferred to all nodes in the network, just like a broadcast.)
- The tag data link settings are all one-to-one (unicast) and multicast packets cannot be used.

If multicast filters are being used, settings must be made in the switching hub. There must be enough multicast filters for all of the networks being used.

Executing Tag Data Links and Message Communications

We recommend using an L2 switching hub with multicast filtering and L4 QoS.

By setting tag data links for higher-priority transmission, it is possible to prevent problems such as transmission delays due to message communications traffic and packet losses due to buffer overflow. Settings must be made in the switching hub to enable this function and give higher priority to tag data link packets.

Special settings must be made in the switching hub when using the multicast filtering function and L4 QoS function.

Selecting the Switching Hub Based on the Hub's Supported Functions

L2 Switching Hub without Multicast Filtering

We recommend this kind of switching hub when only tag data links are executed and any of the following conditions is met.

- The tag data links are set to share the same data with all nodes in the network. (The multicast packets are transferred to all nodes in the network, just like a broadcast.)
- The tag data link settings are all one-to-one (unicast) and multicast packets cannot be used.
- There is little traffic in the tag data links.

No special settings are required for an L2 switching hub without multicast filtering.

L2 Switching Hub with Multicast Filtering

We recommend this kind of switching hub when only tag data links are executed and the following condition is met.

- There are many 1:N links (where N represents some number of nodes in the network) in the tag data link settings, i.e., there are many multicast packets used, or there is heavy traffic in the tag data links.

Special settings are required for an L2 switching hub with multicast filtering. There must be enough multicast filters for the network being used.

L3 Switching Hub with Multicast Filtering and L4 QoS Functions

We recommend this kind of switching hub when both tag data links and message communications are executed.

By setting tag data links for higher-priority transmission, it is possible to prevent problems such as transmission delays due to message communications traffic and packet losses due to buffer overflow. Settings must be made in the switching hub to enable this function and give higher priority to tag data link packets.

Special settings must be made in the switching hub when using the multicast filtering function and L4 QoS function. There must be enough multicast filters for the network being used.

Note

(1) Ask the switching hub manufacturer for setting procedures for the switching hub.

(2) Install the switching hub so that its environmental resistance capabilities are not exceeded. Ask the switching hub manufacturer for information on the environmental resistance of the switch hub.

SECTION 3
Installation and Initial Setup

This section explains how to install and make the initial settings required for operation of the EtherNet/IP Unit or built-in EtherNet/IP port.

3-1 Overview Initial Setup Procedures 44
3-1-1 Procedures 44
3-2 Switch Settings. 47
3-2-1 Setting the Unit Number 47
3-3 Mounting to a PLC 49
3-3-1 Mounting to a CS-series PLC 49
3-3-2 Mounting to a CJ-series PLC 49
3-3-3 Mounting 50
3-3-4 Handling Precautions 51
3-4 Network Installation 52
3-4-1 Basic Installation Precautions 52
3-4-2 Recommended Products. 52
3-4-3 Precautions 52
3-4-4 Using Contact Outputs (Common to All Units) 54
3-5 Connecting to the Network. 56
3-5-1 Ethernet Connectors 56
3-5-2 Connecting the Cable 56
3-6 Creating I/O Tables 58
3-6-1 I/O Table Overview 58
3-6-2 Connecting Programming Devices to the PLC 58
3-6-3 Procedure for Creating I/O Tables. 58
3-7 Setting the Local IP Address 63
3-8 TCP/IP and Link Settings 66
3-8-1 Setting Procedure with the CX-Programmer. 66
3-8-2 Making TCP/IP Settings with the Network Configurator 72
3-9 Tag Data Link Parameters 74
3-9-1 Network Configurator Setting Procedure 74
3-10 User Authentication Settings 78
3-11 Other Parameters. 79
3-12 Communications Test. 90
3-12-1 PING Command 90
3-12-2 EtherNet/IP Unit or Built-in EtherNet/IP Port Operation 90
3-12-3 Host Computer Operation 90

3-1 Overview Initial Setup Procedures

3-1-1 Procedures

Initial Settings

1,2,3...

1. Set the unit number and node address with the switches on the front of the EtherNet/IP Unit or, for the built-in EtherNet/IP port, on the front of the CPU Unit.

   Refer to *3-2 Switch Settings*.
2. Mount the Unit in the CPU Rack.

   Refer to *3-3 Mounting to a PLC*.
3. Wire the Ethernet network with twisted-pair cable.

   Refer to *3-4 Network Installation* and *3-5 Connecting to the Network*.
4. Prepare a computer with Support Software installed on it and a serial cable or an Ethernet cable (twisted-pair cable) to connect to the PLC. These are required to perform network settings using the Support Software (e.g., Network Configurator, CX-Programmer, and CX-Integrator).
5. Connect the PLC to the computer and create the I/O tables using the CX-Programmer. I/O tables do not need to be created for the built-in EtherNet/IP port on the CJ2H-CPU□□-EIP, CJ2M-CPU3□ or CJ3M-CPU3□.

   Refer to *3-6 Creating I/O Tables*.
6. Set the IP address of the EtherNet/IP Unit or built-in EtherNet/IP port using one of the following methods.

   a) Using the Unit without setting the IP address:
   - The default IP address is *192.168.250.Node_address*.

   b) Setting a particular IP address:
   - If you want to store the setting in the CPU Unit, set it in the EtherNet/IP Unit's allocated DM area within the CPU Unit.
   - If you want to store the setting in the Unit, set the IP address in the Edit Parameters Dialog Box of the I/O Table Dialog Box from the CX-Programmer, and transfer the setting to the Unit.

   Refer to *3-7 Setting the Local IP Address* and *3-8 TCP/IP and Link Settings*.
7. When necessary, set the following items in the Edit Parameters Dialog Box and transfer them: TCP/IP, Ethernet, FINS/UDP, FINS/TCP, FTP, Auto Adjust Time, Status Area, SNMP, and SNMP Trap

   Refer to *3-11 Other Parameters*.
8. When necessary, set the routing tables.

   If the FINS communications service is being used and multiple network Communications Units are mounted in the PLC, set the routing tables from the CX-Integrator, and transfer the table.

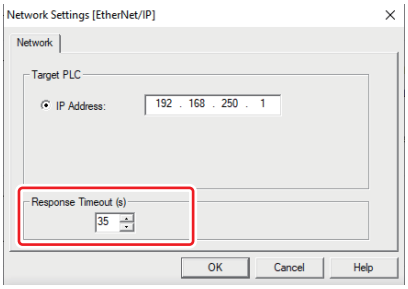
   Refer to the *CX-Integrator Operation Manual* (Cat. No. W464) for the setting procedure.

   Note that you cannot go beyond the network when connecting the Support Software to CS1W/CJ1W-EIP21S or CJ3M-CPU3□ using *Secure Comm*.
9. Test communications.
   Send a PING command to the EtherNet/IP Unit or built-in EtherNet/IP port.

   Refer to *3-12 Communications Test*.

Note If you connect the CX-Programmer with the Network Type set to *EtherNet/IP*, you may not be able to perform the following operation.

- On the CS1W/CJ1W-EIP21S or CJ3M-CPU3☐, transfer the parameters in the Edit Parameters Dialog Box and then restart the Unit.
- On the CS1W/CJ1W-EIP21S or CJ3M-CPU3☐, restart the Unit in the Edit Parameters Dialog Box.
  If this problem occurs, once close and then open the Edit Parameters Dialog Box again. If the problem persists, click the **Settings** Button in the *Network Type* group and, in the Network Settings [EtherNet/IP] Dialog Box displayed, set the value of *Response Timeout (s)* to 35 or higher.



Settings Required for Tag Data Link Service (Cyclic Communications)

1. Using the EtherNet/IP Datalink Tool in the Network Configurator to Set the Parameters

With this method, there is no flexibility in the settings, but you can easily set the data link parameters using only memory addresses, and the settings will conform to Controller Link data link parameters. Refer to *3-9 Tag Data Link Parameters* or *SECTION 6 Tag Data Link Functions*.

2. Using the Tag Data Link Setting Function in the Network Configurator to Set the Parameters

With this method, you can set the connections that define the tag data links for each EtherNet/IP node. Tag data links can be set with a high degree of flexibility using both memory addresses and network variables. Refer to *SECTION 6 Tag Data Link Functions* for information on how to make these settings.

Settings Required for the Message Communications Service

Execute a CMND(490) instruction in the CS/CJ-series CPU Unit's user program.

Refer to *SECTION 9 Message Communications*.

Settings Required for Security Functions

To use security functions, use CS1W/CJ1W-EIP21S or CJ3M-CPU3□. The security functions cannot be used other units.

1,2,3...

1. Perform the initial settings described above.
2. Make the user authentication settings using the EIP21S User Management Tool and register the user account.
   Refer to *13-3 User Authentication*.
3. Close any unused ports and set the IP packets to pass through the packet filter.
   Refer to *13-4 Opening and Closing the Port* and *13-5 IP Packet Filtering*.
4. Check the operation of the Unit to be sure that the security function settings are as intended.

3-2 Switch Settings

3-2-1 Setting the Unit Number

The unit number is used to identify individual CPU Bus Units when more than one CPU Bus Unit is mounted to the same PLC. Use a small screwdriver to make the setting, taking care not to damage the rotary switch. The unit number is factory-set to 0.

CS series



Setting range:
0 to F

CJ series



Setting range:
0 to F

Note

(1) Turn OFF the power supply before setting the unit number.

(2) If the unit number is being set for the first time or changed, then I/O tables must be created for the PLC.

(3) With CS-series and CJ-series PLCs, words are automatically allocated in the CIO Area and DM Area according to the unit numbers that are set. For details, refer to *SECTION 4 Memory Allocations*.

Setting the Node Address

When there are multiple EtherNet/IP Units or Ethernet Units connected to the Ethernet network for the FINS communications service, the EtherNet/IP Units are identified by node addresses. Use the node address switches (NODE NO.) to set the node address between 01 and FE hexadecimal (1 to 254 decimal). Do not set a number that has already been set for another node on the same network.

CS series



Setting range:
01 to FE (1 to 254 decimal)

CJ series



Setting range:
01 to FE (1 to 254 decimal)

The left switch sets the sixteens digit (most significant digit) and the right switch sets the ones digit (least significant digit). The node address is factory-set to 01.

Note Turn OFF the power supply before setting the node address.

Relationship to IP Addresses

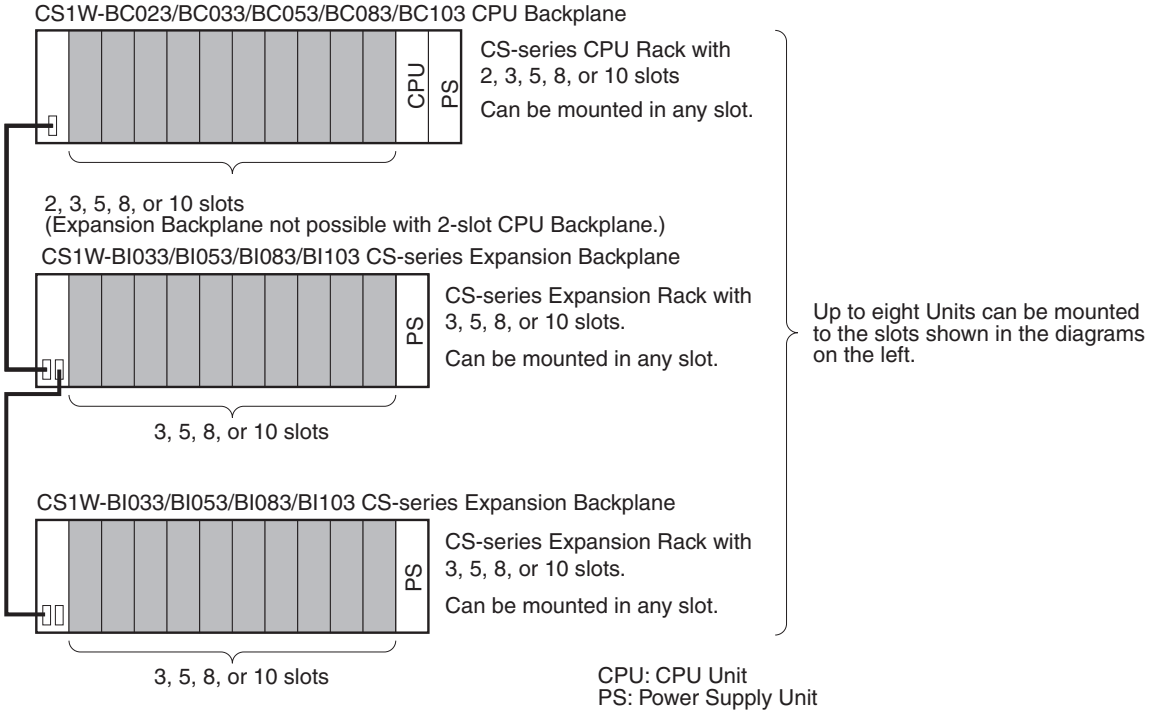
When IP addresses are generated automatically (either dynamic or passive), the rightmost byte of the host ID of the IP address is set to the same value as the node address. (Refer to *Section 5 Determining IP Addresses*.) If the same node address value cannot be used, the IP address table method or the combined method must be used for address conversion. (For details, refer to *SECTION 5 Determining IP Addresses*.)

If the FINS communications service is not being used on the Ethernet network, then it is all right for the same node address to be set on two or more EtherNet/IP Units. The setting, however, must be made within a range of 01 to FE. If a value outside of this range is set, the MS indicator will light red, the 7-segment display will indicate code H4 (node address setting error), and the EtherNet/IP Unit will stop operating.

3-3 Mounting to a PLC

3-3-1 Mounting to a CS-series PLC

EtherNet/IP Units can be mounted to any slot in a CS-series CPU Rack or a CS-series Expansion CPU Rack, but the number of slots to which they can be mounted depends on the Backplane. A maximum of eight EtherNet/IP Units can be mounted in a single PLC.

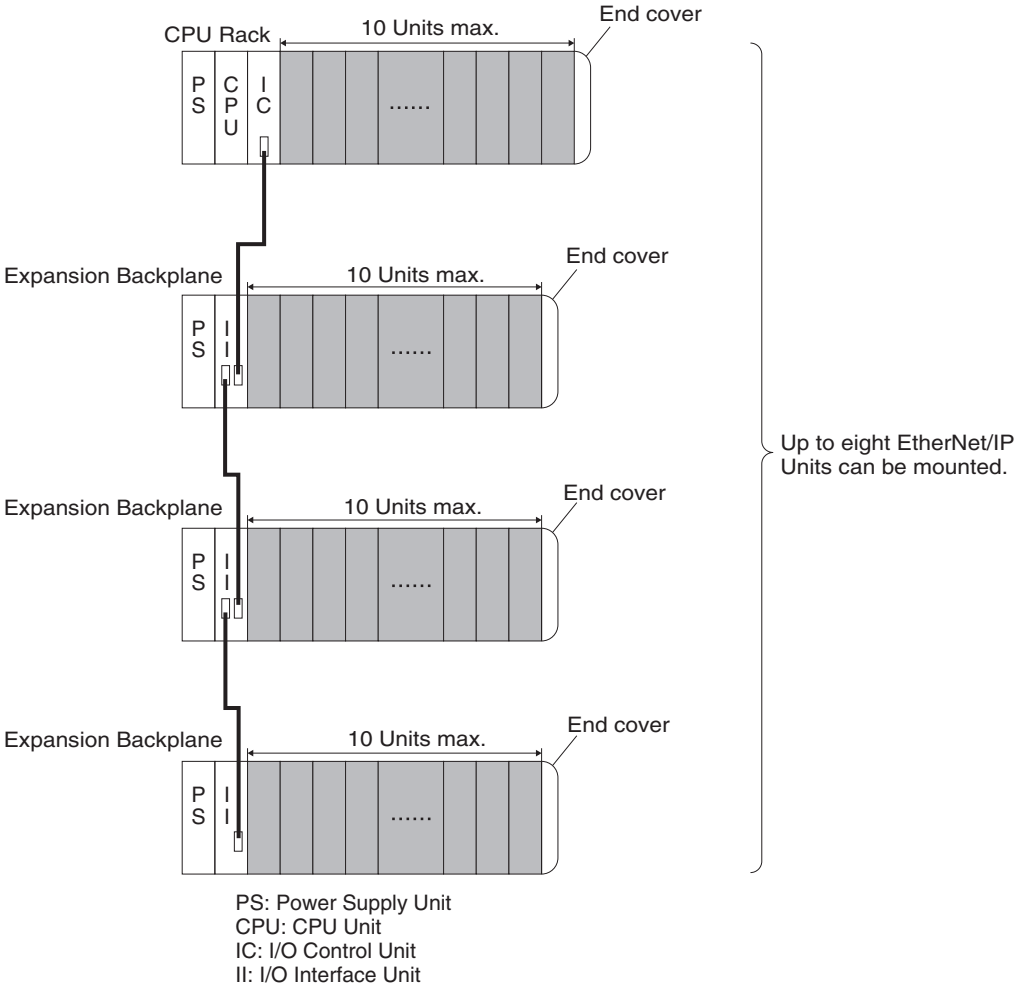


3-3-2 Mounting to a CJ-series PLC

EtherNet/IP Units can be mounted in a CJ-series CPU Rack or a CJ-series Expansion CPU Rack. Connect the EtherNet/IP Unit in any of the positions shown below using the sliders on the top and bottom of the Unit.

Number of Units that can be mounted in the CPU unit

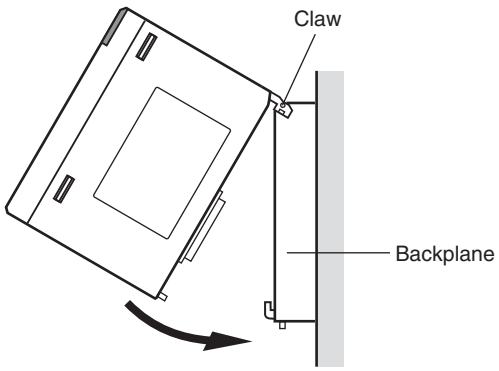
CPU unit	Number of mounted EtherNet/IP Units
CJ2H-CPU6□-EIP, CJ3M-CPU3□	7
CJ2M-CPU1□/3□, CP1H	2
CJ3M-CPU1□, CJ2H-CPU6□, CJ1□-CPU□□	8



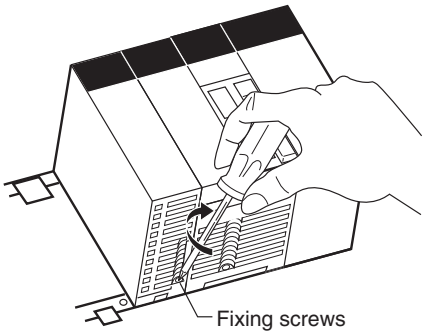
3-3-3 Mounting

Mount the EtherNet/IP Unit to the Backplane using the following procedure.

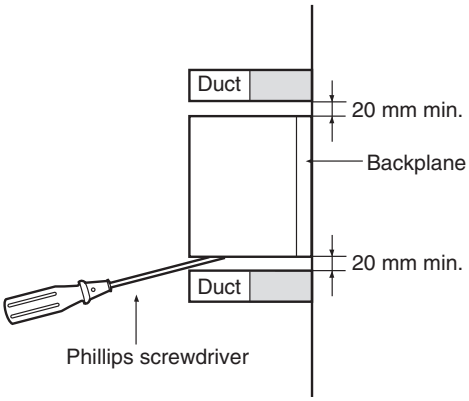
1,2,3... 1. Hook the claw on the top of the Unit onto the Backplane.



2. Insert the Unit into Backplane connectors and securely tighten the screw at the bottom of the Unit. Tighten the screws to a torque of 0.4 N·m.
3. When removing the Unit, first loosen the screw at the bottom of the Unit.



Note When mounting the Unit, provide the clearance shown below to facilitate easy mounting or dismounting.



3-3-4 Handling Precautions

- Always turn OFF the power supply to the PLC before mounting or dismounting a Unit or connecting or disconnecting cables.
- Provide separate conduits or ducts for the I/O lines to prevent noise from high-tension lines or power lines.
- Do not allow scraps and chips of wire to enter the Unit. Doing so may result in burning, failure, or malfunction. Take measures such as covering the Unit, in particular, during installation.
- Do not insert foreign matter from any opening of the Unit. Doing so may result in burning, electric shock, or failure.

3-4 Network Installation

3-4-1 Basic Installation Precautions

- Take the greatest care when installing the Ethernet System, being sure to follow ISO 8802-3 specifications. You must obtain a copy of these specifications and be sure you understand them before attempting to install an Ethernet System. Unless you are already experienced in installing communications systems, we strongly recommend that you employ a professional to install your system.
- Do not install Ethernet equipment near sources of noise. If a noisy environment is unavoidable, take adequate measures against noise interference, such as installing network components in grounded metal cases or using optical cable in the system.
- When installing an EtherNet/IP network that combines an information system with the control system, and the communications load may be heavy due to tag data links, we recommend configuring the network so that the load does not affect communications. For example, install the tag data links in a segment that is separate from the information network.

3-4-2 Recommended Products

The following table shows the devices recommended for use with the EtherNet/IP Unit in *2-3 Selecting the Network Devices*.

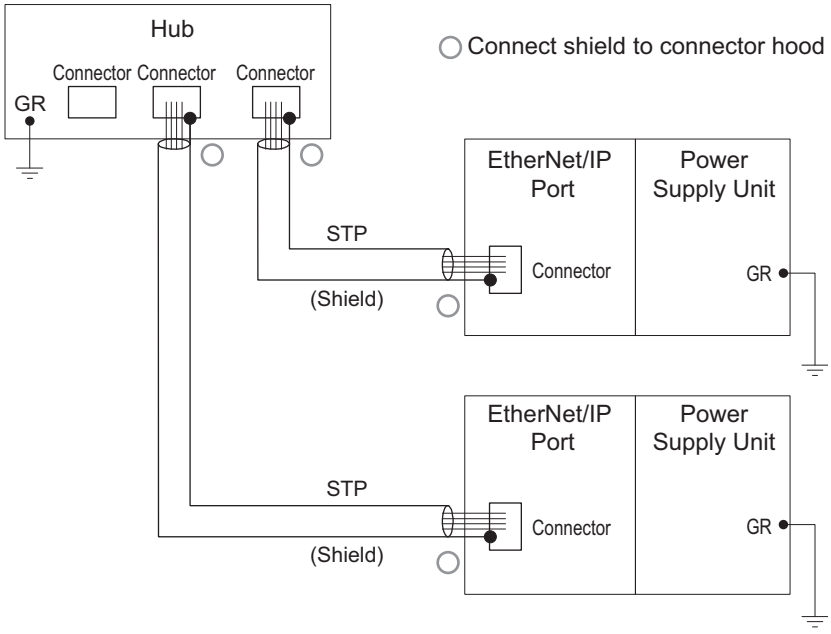
3-4-3 Precautions

Precautions on Laying Twisted-pair Cable

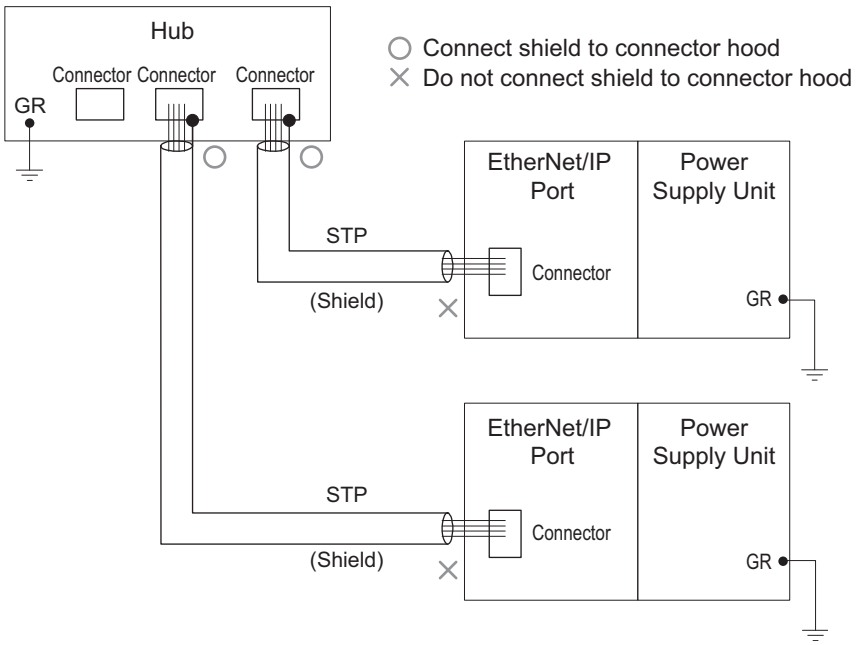
■ **Between a Built-in EtherNet/IP Port and an Switching Hub**

Connect the cable shields to the connector hoods as described in either (1) or (2) below.

1. Connecting the shields at both ends of the cable
   Connect the shields to the connector hoods at both ends of the cables.



2. Connecting the shields only at the Ethernet switch side
   Connect the shields to the connector hoods only at the Ethernet switch side.



Note Noise immunity may be reduced and device damage may occur due to ground loops, which may be caused by improper shield connections and grounding methods.

■ **Between Two Ethernet Switches**

Regardless of which baud rate is used, check with the Ethernet switch manufacturers for information about installing the network between Ethernet switches, and in particular whether or not it is necessary to connect the cable shields to the connector hoods.

- Press the cable connector in firmly until it locks into place at both the switching hub and the EtherNet/IP Unit.
- Do not lay the twisted-pair cable together with high-voltage lines.
- Do not lay the twisted-pair cable near devices that generate noise.
- Do not lay the twisted-pair cable in locations subject to high temperatures or high humidity.
- Do not lay the twisted-pair cable in locations subject to excessive dirt and dust or to oil mist or other contaminants.

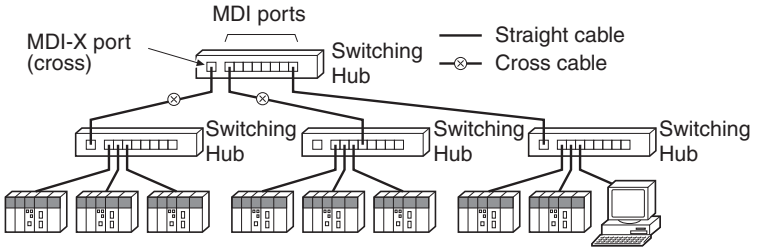
Switching Hub Installation Environment Precautions

- Do not ground the switching hub in the same location as a drive-system component such as an inverter.
- Always use a dedicated power supply for the switching hub's power supply. Do not use the same power supply used for other equipment, such as an I/O power supply, motor power supply, or control power supply.
- Before installation, check the switching hub's environment-resistance specifications, and use a switching hub appropriate for the ambient conditions. Contact the switching hub manufacturer for details on switching hub's environment-resistance specifications.

Switching Hub Connection Methods

Connect two hubs to each other as follows: Connect an MDI port to an MDI-X port with a straight cable; connect two MDI ports with a cross cable; and connect two MDI-X ports with a cross cable.

Note It is very difficult to distinguish cross cables and straight cables by appearance. Incorrect cables will cause communications to fail. We recommend using cascade connections with straight cables whenever possible.



Some switching hubs can automatically distinguish between MDI and MDI-X. When this kind of switching hub is being used, straight cable can be used between switching hubs.

Note Adjust the link settings of the EtherNet/IP Unit or built-in EtherNet/IP port to match the communications settings of the connected switching hub. If the settings do not match, the link will become unstable and prevent normal communications. The following table shows the allowed settings for each switching hub communications mode.

Switching hub setting		EtherNet/IP Unit setting				
		Auto-negotiation	10 Mbps (fixed)		100 Mbps (fixed)	
			Full duplex	Half duplex	Full duplex	Half duplex
Auto-negotiation		Best	---	OK	---	OK
10 Mbps (fixed)	Full duplex	---	OK	---	---	---
	Half duplex	OK	---	OK	---	---
100 Mbps (fixed)	Full duplex	---	---	---	Best	---
	Half duplex	OK	---	---	---	OK

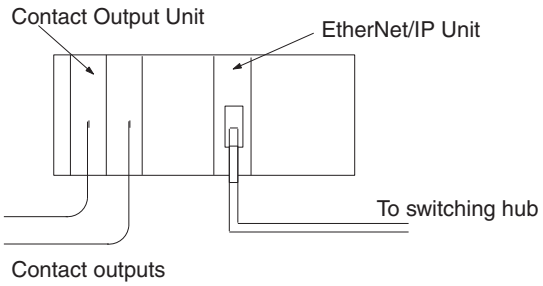
Note Best = Recommended; OK = Allowed; --- = Not allowed.

3-4-4 Using Contact Outputs (Common to All Units)

When an EtherNet/IP Unit or built-in EtherNet/IP port and Contact Output Unit are mounted in the same Rack or connected to the same PLC, communications errors may occur due to noise generated by the contact outputs. Use one or more of the following measures when installing Contact Output Units and EtherNet/IP Units on the same Rack.

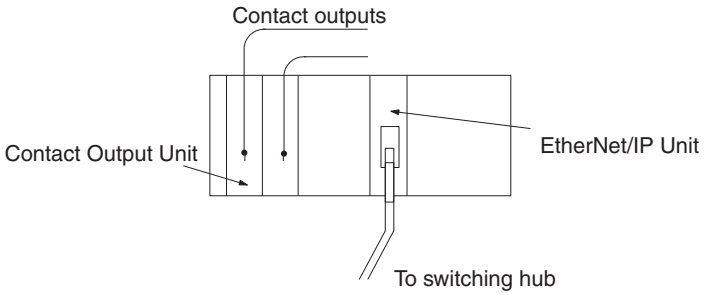
Mounting Location

Mount (or connect) any Contact Output Units as far away from the EtherNet/IP Unit or built-in EtherNet/IP port as possible.



Cable Location

Separate the transceiver cable or twisted-pair cable connecting the EtherNet/IP Unit as far from the wiring to the Contact Output Units as possible. The coaxial cable must also be placed as far away from the Contact Output Units and their wiring as possible.



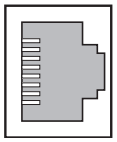
3-5 Connecting to the Network

3-5-1 Ethernet Connectors

The following standards and specifications apply to the connectors for the Ethernet twisted-pair cable.

- Electrical specifications: Conforming to IEEE802.3 standards.
- Connector structure: RJ45 8-pin Modular Connector (conforming to ISO 8877)

8pin
•
•
1pin

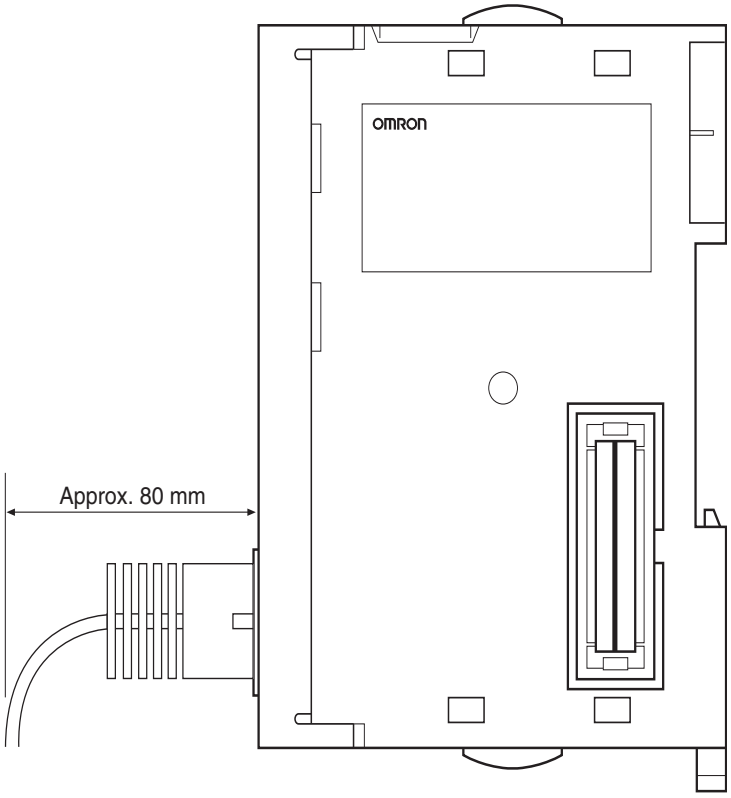


Connector pin	Signal name	Abbr.	Signal direction
1	Transmission data +	TD+	Output
2	Transmission data –	TD–	Output
3	Reception data +	RD+	Input
4	Not used.	---	---
5	Not used.	---	---
6	Reception data –	RD–	Input
7	Not used.	---	---
8	Not used.	---	---
Hood	Frame ground	FG	---

3-5-2 Connecting the Cable

⚠ **Caution** Turn OFF the PLC's power supply before connecting or disconnecting twisted-pair cable.

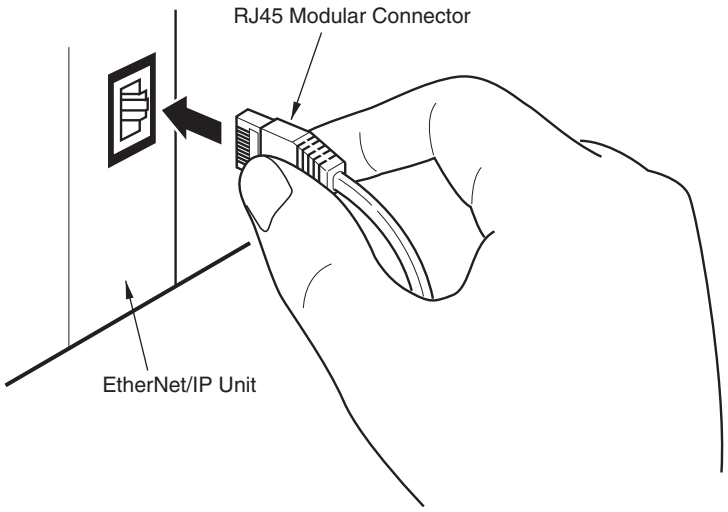
⚠ **Caution** Allow sufficient space for the bending radius of the twisted-pair cable. The required space depends on the communications cable and connector that are used. Consult with the manufacturer or sales agent.



1,2,3... 1. Lay the twisted-pair cable.

2. Connect the cable to the switching hub. Be sure to press in the cable until it locks into place.
3. Connect the twisted-pair cable to the connector on the EtherNet/IP Unit. Be sure to press the connectors (both the switching hub side and Ethernet side) until they lock into place.

Example: CS1W-EIP21



3-6 Creating I/O Tables

3-6-1 I/O Table Overview

I/O tables are used to identify Units mounted to the PLC, and to allocate I/O to them. With CS-series and CJ-series PLCs, whenever there is a change to the Unit configuration it is necessary to create I/O tables and register the mounted Units in the CPU Unit.

The I/O tables can be created in the following ways.

- Using the CX-Programmer offline.
- Using the CX-Programmer online to create the I/O table based on the Units mounted to the PLC.
- Using the Programming Console to create the I/O table based on the Units mounted to the PLC.
- Using the CPU Unit's automatic I/O allocation at startup. (This method is available for the CJ Series only.)

3-6-2 Connecting Programming Devices to the PLC

To create the I/O tables, connect a Programming Device (such as a CX-Programmer or Programming Console) to the PLC.

Applicable Programming Devices

The following Programming Devices can be used with CS/CJ-series PLCs.

Programming Console

Model number	Key Sheet (required)	Recommended cable (required)
C200H-PRO27-E	CS1W-KS001-E	CS1W-CN224 (cable length: 2.0 m) CS1W-CN624 (cable length: 6.0 m)
CQM1-PRO01-E		CS1W-CN114 (cable length: 0.1 m)

Note A Programming Console cannot be used with the CJ2/CJ3 CPU Units. Use the CX-Programmer.

CX-Programmer

For information on how to connect and operate the CX-Programmer, refer to the *CX-Programmer Operation Manual* (Cat. No. W446).

3-6-3 Procedure for Creating I/O Tables

Programming Console

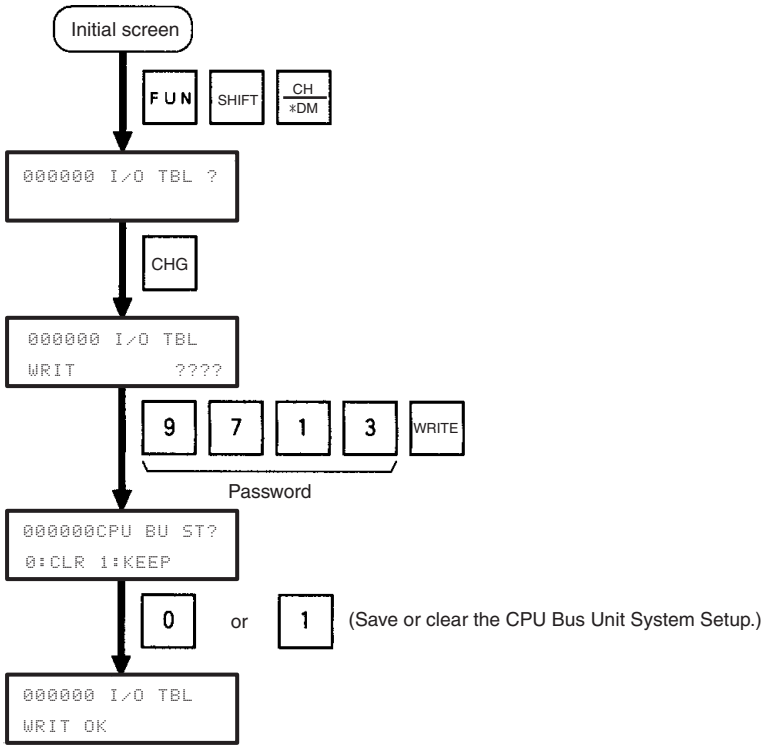
This section provides the procedure for creating the I/O tables using a Programming Console. For details on using the Programming Console, refer to the Programming Console's operation manual.

Note

(1) With the CJ Series, it is necessary to create I/O tables only when the user is allocating I/O manually. With the CS Series, it is always necessary to create I/O tables.

(2) With the CJ2/CJ3 CPU Units, the built-in EtherNet/IP port is set in the I/O tables by default and cannot be changed. It is not necessary to register it in the I/O tables.

Use the following procedure to create the I/O tables.

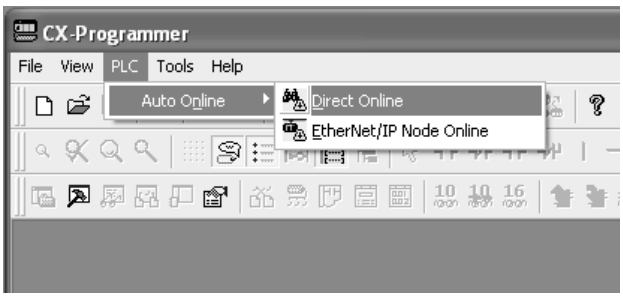


CX-Programmer

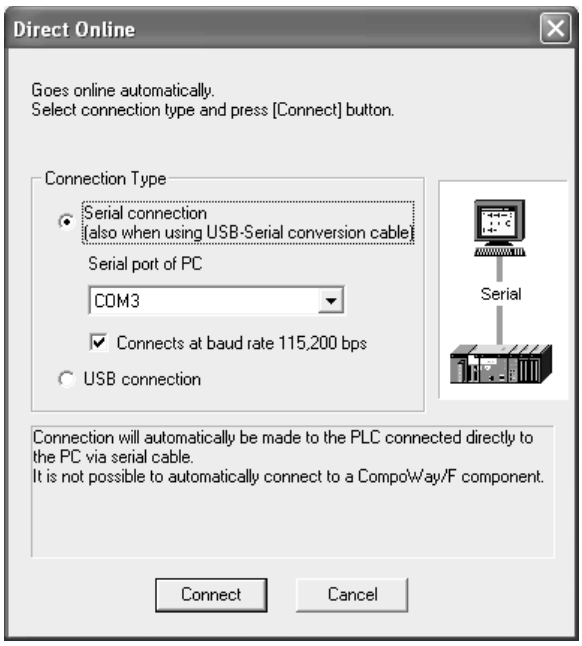
This section describes how to register an EtherNet/IP Unit in the I/O tables using the CX-Programmer. Refer to the *CX-Programmer Operation Manual* (Cat. No. W446) for details on the operating procedures.

This section describes how to register the CJ1W-EIP21 in the I/O tables by creating the I/O tables on a computer with the CX-Programmer. In this example, the computer is connected to the PLC using a serial cable. The CJ1W-EIP21 is connected to a CJ1H-CPU67 CPU Unit.

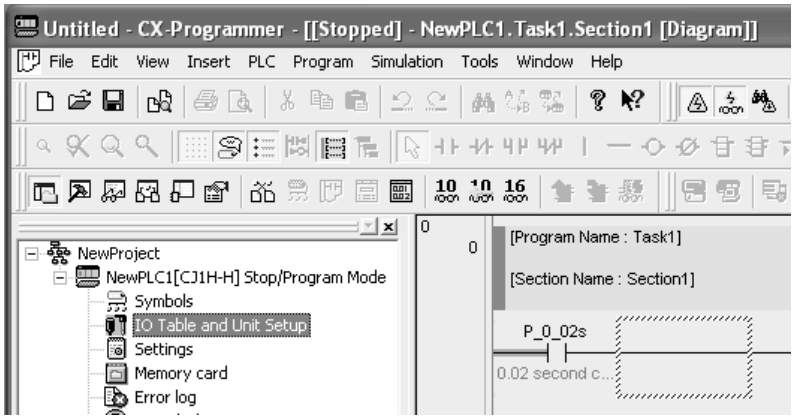
1,2,3... 1. Start the CX-Programmer, and then select ***PLC*** – ***Auto Online*** – ***Direct Connection*** from the menus.



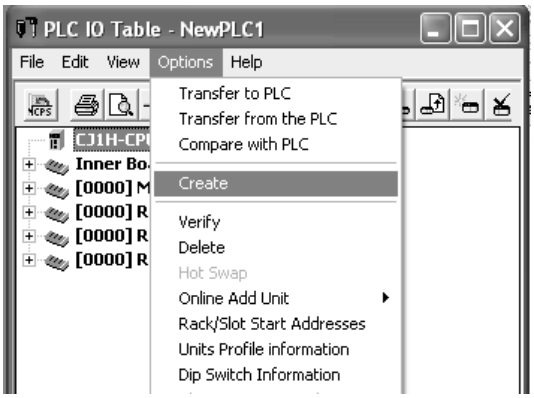
2. The Direct Online Dialog Box will be displayed. Select a serial connection, select the name of the applicable computer serial port, and then press the Connect Button.



3. If the connection process is successful, the system will be connected on-line. Here, check the operating mode of the PLC. If the operating mode is not PROGRAM mode, change the mode by selecting ***PLC*** – ***Operating Mode*** – ***Program*** from the menus.
4. Double-click **IO Table and Unit Setup** Icon in the project workspace in the CX-Programmer. The PLC IO Table Dialog Box will be displayed. Select ***Options*** – ***Create*** from the menus.



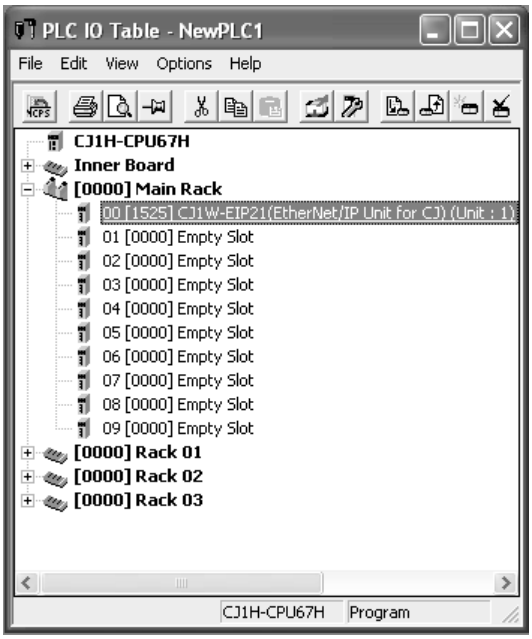
CPU Unit model	I/O table display format
CJ2H-CPU□-EIP	CJ2B-EIP21
CJ2M-CPU3□	CJ2M-EIP21
CJ3M-CPU3□	CJ3M-EIP21S



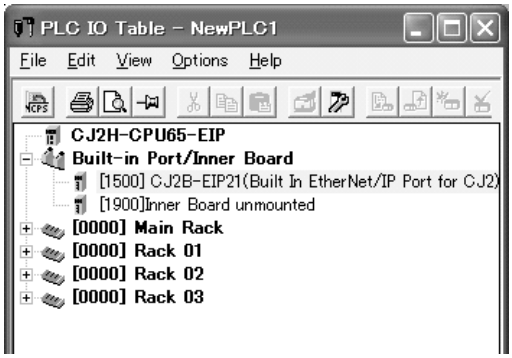
Executing the I/O table creation command causes the EtherNet/IP Unit to be restarted. After the EtherNet/IP Unit is restarted, perform transfer operation in the dialog box that is displayed.

5. The EtherNet/IP Unit will be displayed at the position it is mounted in the PLC.

Note If it is not displayed correctly, select *Options* – *Transfer from PLC* from the menus.



Note Creating I/O tables is not required if the built-in EtherNet/IP port of a CJ2/CJ3 CPU Unit is used. The EtherNet/IP built-in ports are displayed as follows in “Built-in Port / Inner Board” in the I/O table. You cannot delete a built-in port from the I/O tables.



CPU Unit Model	I/O table display format
CJ2H-CPU6□-EIP	CJ2B-EIP21
CJ2M-CPU3□	CJ2M-EIP21
CJ3M-CPU3□	CJ3M-EIP21S

3-7 Setting the Local IP Address

This section describes the 3 ways to set the local I/O address of an EtherNet/IP Unit or built-in EtherNet/IP port.

Number	Setting method	Example of use	Setting of each method for enabling
Method 1	Using the default IP address (192.168.250.Node_address)	• When you want to establish connection with the CX-Programmer etc. via Ethernet immediately after purchasing the EtherNet/IP Units	When both of the following are satisfied • The IP address setting by Method 2 is 0000. • The IP address setting by Method 3 is 0.0.0.0.
Method 2	Setting an IP address in the CPU Unit's allocated DM area The local IP address is set (stored) in the CPU Units.	• When you want to set a specific IP address for data link • When you want to set an IP address from HMI etc.	The IP address setting by Method 3 is 0.0.0.0.
Method 3*1	Setting the TCP/IP Configuration from the CX-Programmer The local IP address is set (stored) in the EtherNet/IP Units.	• When you want to set a subnet mask etc. in addition to a particular IP address • When you want to make advanced settings, such as getting an IP address from the BOOTP server	---

*1When an IP address is set by Method 3, the value will be reflected in *IP Address Display/Setting Area* (words m+98 and m+99) of the allocated DM Area words of Method 2.

When FINS communications are being used, it is necessary to show the correspondence between the IP addresses and FINS node addresses. Refer to *SECTION 5 Determining IP Addresses* for an explanation of IP addresses as well as the correspondence between FINS node addresses and IP addresses.

The three setting methods are described in the following paragraphs.

Method 1: Using the Default IP Address (192.168.250.Node_address)

When the EtherNet/IP Unit or built-in EtherNet/IP port is just mounted in the PLC and the I/O table is created, the EtherNet/IP Unit or built-in EtherNet/IP port will operate with its default IP address. This default address is enabled when the local IP address in the allocated DM area and the TCP/IP Configuration are both set to their defaults (0.0.0.0).

The default IP address is *192.168.250.Node_address*, where *Node_address* is the node address set with the rotary switches on the front of the EtherNet/IP Unit. This address is also used as the FINS node address.

The following table shows the various settings in the Unit Setup when the IP address and TCP/IP Configuration are all set to their default values.

Setting	Operating status
IP address	192.168.250.Node_address
Subnet mask	255.255.255.0 (class C mask)
Default gateway	None (IP routing disabled)
Preferred DNS server	None
Alternate DNS server	None
Host name	None
Domain name	None
Baud rate	Auto-detect

Method 2: Setting the Address in the CPU Bus Unit's Allocated DM Area

With this method, an IP address is not set in the TCP/IP Configuration (left at its default setting), and an IP address is set in the allocated DM Area words (the IP Address Display/Setting Area in words m+98 and m+99).

The IP address can be written in the two IP Address Display/Setting Area words using the CX-Programmer or the Programming Console. To enable the new IP Address setting, the EtherNet/IP Unit or built-in EtherNet/IP port must be restarted or the PLC's power must be turned OFF and then ON again.

The beginning word m of the allocated DM Area words of the applicable Unit is calculated by the following equation:

m = D30000 + (100 x unit number)

Words m+98 and m+99 are the IP Address Display/Setting Area.

	15 14 13 12	11 10 9 8	7 6 5 4	3 2 1 0
m+98	(1)	(2)	(3)	(4)
m+99	(5)	(6)	(7)	(8)

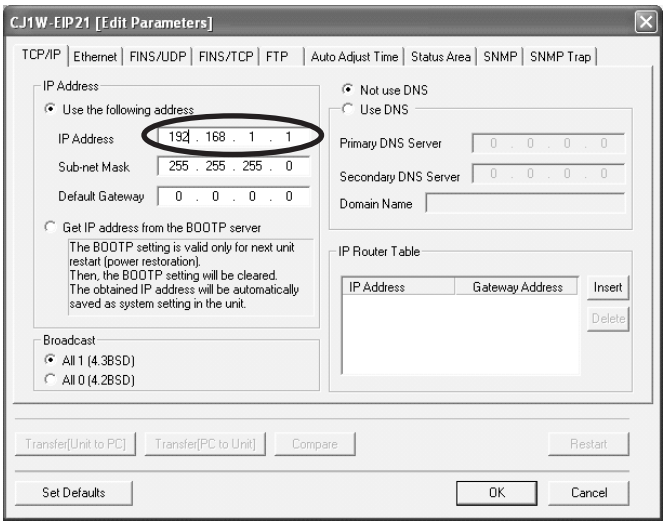
IP Address: (1)(2).(3)(4).(5)(6).(7)(8) (Hex)

The following table shows the various Unit Setup when only the IP Address Display/Setting Area is set, and the other TCP/IP Configuration settings are left at their default values.

Setting	Operating status
IP address	IP address set in words m+98 and m+99 (IP Address Display/Setting Area) of the DM Area words allocated to the EtherNet/IP Unit as a CPU Bus Unit
Subnet mask	Determined by class of the IP address
Default gateway	None (IP routing disabled)
Preferred DNS server	None
Alternate DNS server	None
Host name	None
Domain name	None
Baud rate	Auto-detect

Method 3: Setting the TCP/IP Configuration from the Network Configurator

This method can be used to set IP addresses from the CX-Programmer. For details, refer to *3-8 TCP/IP and Link Settings*.



If the IP address is set in the TCP/IP Tab Page, that IP address setting will be displayed in the IP Address Display/Setting Area (words m+98 and m+99) in the DM Area words allocated to the Unit/port.

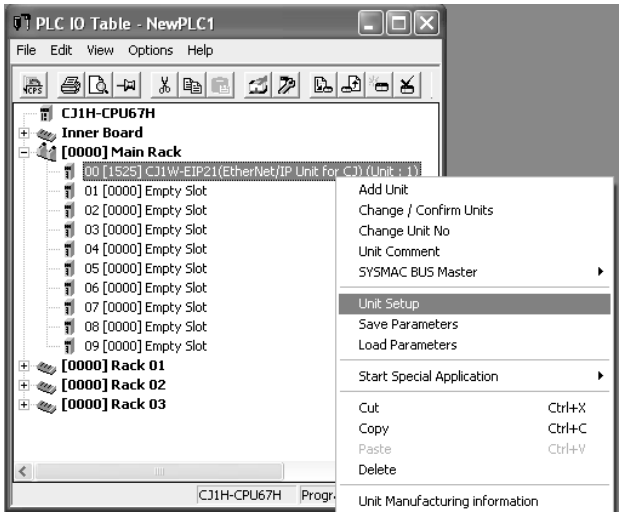
3-8 TCP/IP and Link Settings

This section describes the TCP/IP-related settings, such as the local IP address and subnet mask for the EtherNet/IP Unit or built-in EtherNet/IP port. Use the CX-Programmer to make these settings. The settings are stored in non-volatile memory in the Unit.

Note Unlike the Ethernet Units, the TCP/IP settings of the EtherNet/IP Unit and built-in EtherNet/IP port are not stored in the CPU Unit's CPU Bus Unit System Setup Area.

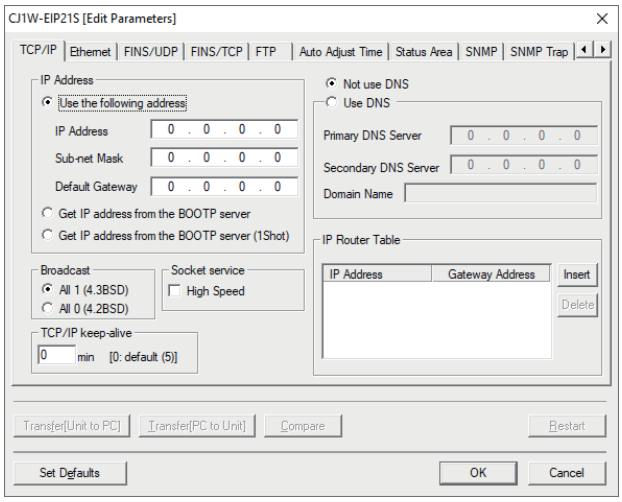
3-8-1 Setting Procedure with the CX-Programmer

1,2,3... 1. When the EtherNet/IP Unit is registered in the I/O tables of the CX-Programmer, the EtherNet/IP Unit and built-in EtherNet/IP port will be displayed in the I/O tables. Refer to *3-6 Creating I/O Tables* for details.

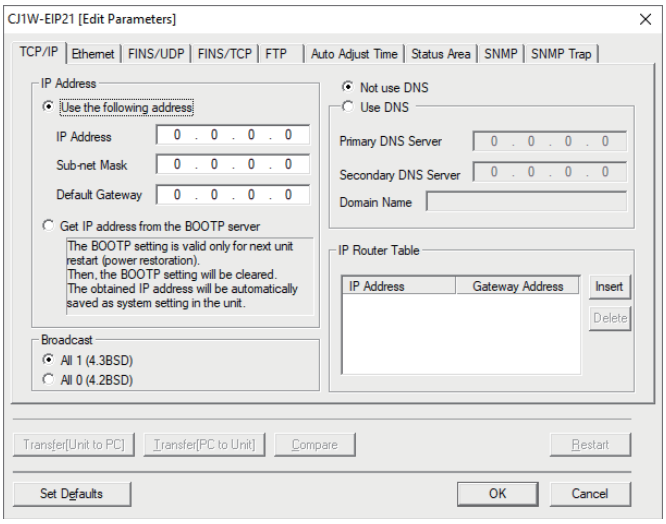


2. Right-click the EtherNet/IP Unit or built-in EtherNet/IP port in the I/O table and select ***Edit - Unit Setup*** from the menus. The Edit Parameters Dialog Box will be displayed.

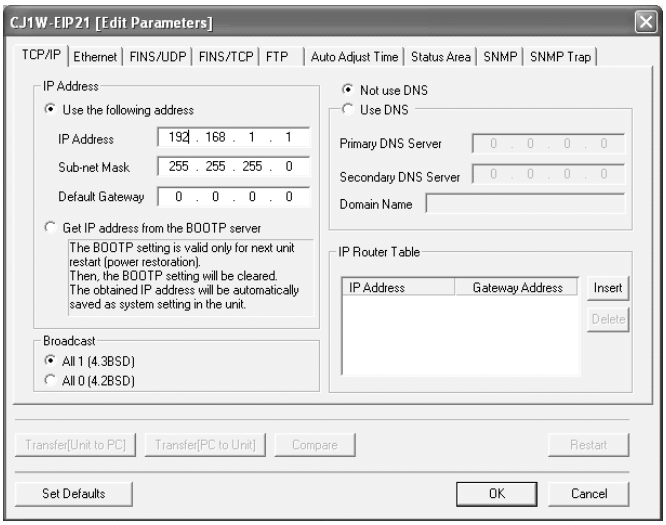
Dialog box for CS1W/CJ1W-EIP21S CJ3M-CPU3□



Dialog box for CS1W/CJ1W-EIP21, CJ2H-CPU□-EIP, and CJ2M-CPU3□



3. Make the necessary settings on the TCP/IP Tab Page of the Edit Parameters Dialog Box. (The IP address is set here.)



4. Place the CX-Programmer online with the PLC and transfer the settings to the EtherNet/IP Unit or built-in EtherNet/IP port.
5. After transferring the settings, a message will ask if you want to restart the EtherNet/IP Unit or built-in EtherNet/IP port. The Unit/port must be restarted to enable the settings.
6. Check the 7-segment display for the EtherNet/IP Unit or built-in EtherNet/IP port.
7. If the 7-segment display is tested again after it goes OFF, and finally displays the IP address, it indicates that the EtherNet/IP Unit has recognized the new TCP/IP Configuration settings (the IP address in this case).

Note (1) The EtherNet/IP Unit or built-in EtherNet/IP port must restart in order to enable the parameter settings that are transferred to it. Verify that restarting the Unit/port will not cause any problems in the system before restarting it.

(2) If the target node address (IP address) is not set correctly, invalid device parameters may be set in the wrong PLC, so check the connected PLC before downloading parameters.

Settings on the TCP/IP Tab Page

Settings for the following items are provided on the TCP/IP Tab Page of the Edit Parameters Dialog Box in the CX-Programmer.

- IP Address
  - IP address
  - Subnet mask
  - Default gateway
- Broadcasting
- High-speed Socket Services
- TCP/IP keep-alive
- Preferred DNS server
- Alternate DNS server
- Domain name
- IP router table

IP Address

Set how to set the local IP address of the EtherNet/IP Unit or built-in EtherNet/IP port.

Item	Contents	Default
IP Address	Select how to set the local IP address of the EtherNet/IP Unit or built-in EtherNet/IP port from the following. Use the following address (See note 1.) Get IP address from the BOOTP server (See note 2.) Get IP address from the BOOTP server (1-Shot)	Use the following address

Note (1) This includes the following settings that are described later.
- IP address
- Subnet mask
- Default gateway

(2) This setting is provided for CS1W/CJ1W-EIP21S, CJ3M-CPU3□ only.

■ IP Address

Sets the local IP address of the EtherNet/IP Unit or built-in EtherNet/IP port.
Set the local IP address on the TCP/IP Tab Page when not setting the IP address in the CPU Unit's allocated DM Area or using the default IP address (default IP address = 192.168.250.Node_address).
When the IP address is set on the TCP/IP Tab Page, it will be stored as the IP address in the DM Area words allocated to the Unit/port as a CPU Bus Unit.

■ Subnet Mask

For the subnet mask, all bits corresponding to the bits in the IP address used as the network ID are set to 1, and the bits corresponding to the host number are set to 0. The EtherNet/IP Unit or built-in EtherNet/IP port supports CIDR (Classless Inter-Domain Routing). The subnet mask can be set to 192.0.0.0 to 255.255.255.252.

Note The CIDR is not supported by the CS1W-EIP21 and CJ2H-CPU6□-EIP (Unit version 1.0).
If no subnet mask is set, or if an illegal value is set, the following values will be used depending on the IP address class.

In normal applications, we recommend setting the subnet mask defined for the class.

Class	Subnet mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

With the default setting (0.0.0.0), a subnet mask corresponding to the IP address class is used.

The following table shows the various parameters in the Unit Setup when only the IP address and subnet mask are set and other settings are left at their default values.

Setting	Operating status
Default gateway	None (IP routing disabled)
Preferred DNS server	None
Alternate DNS server	None
Host name	None
Domain name	None
Broadcasting	4.3 BSD specifications
IP router table	None

■ **Default Gateway**

Sets the default gateway's IP address.

This setting is not required when the IP routing is not being used.

Broadcasting

Sets the IP address specification method for broadcasting with FINS/UDP.

- All 1's (4.3BSD): Broadcasting is performed with the host ID set to all 1's.
- All 0's (4.2BSD): Broadcasting is performed with the host ID set to all 0's.

Normally, use the default setting of all 1's (4.3BSD).

TCP/IP keep-alive

Set the liveness-checking interval. When socket services using either FINS/TCP or TCP/IP, the connection will be terminated if there is no response from the remote node (either a server or client) within the time set here. (Enabled for socket services using FINS/TCP or TCP/IP only.)

Setting range: 0 to 65,535 minutes (The default is 0, meaning that the checking time is 5 minutes.)

This setting applies to the keep-alive setting for each connection set with the FINS/TCP tab.

Note This is enabled for CS1W/CJ1W-EIP21S or CJ3M-CPU3□ only.

High-speed Socket Services

Selecting this option improves the performance of processing for sending and receiving by using bits for socket services. For information on communications performance, refer to *14-8-5 Times Required for Sending and Receiving for Socket Services*. When the High Speed Option is selected, socket services that are implemented using a CMND(490) or CMND2(493) instruction will cause an error.

Note This is enabled for CS1W/CJ1W-EIP21S or CJ3M-CPU3□ only.

Preferred DNS Server and Alternate DNS Server

When accessing another node from the EtherNet/IP Unit or built-in EtherNet/IP port using the host name, the DNS server searches for the other node's

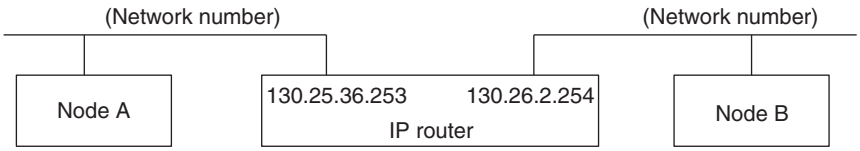
IP address from the other node's host name to the DNS server. These settings register the IP addresses of the preferred and alternate DNS servers that will perform the search. At this time, the EtherNet/IP Unit is not equipped with any functions that require a DNS server, so these settings are not used. (The functionality required to use a DNS server is not provided on CS1W/CJ1W-EIP21 or CJ2H-CPU6□-EIP with unit version 1.0. The DNS server cannot be used with these Units.)

Domain Name

Sets the domain name of the domain to which the EtherNet/IP Unit or built-in EtherNet/IP port belongs. The EtherNet/IP Unit or built-in EtherNet/IP port does not use a domain name in actual communications.

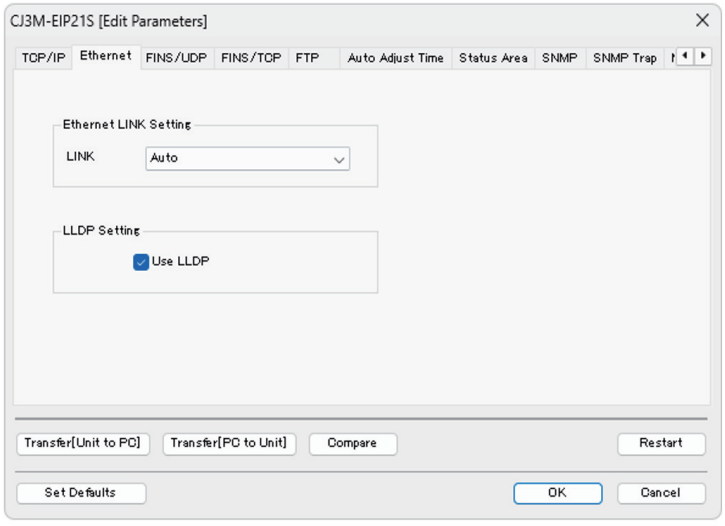
IP Router Table

The IP router table is used to find the IP address of the IP rooter that is connected to the target segment. This is done when performing communications with a node that is on an IP network segment that is connected to the EtherNet/IP Unit through an IP router. The IP router table is set when EtherNet/IP Unit communications are routed to a specific node through any IP router other than the default gateway.



For the IP address in the table, set the network ID of the other IP network segment to communicate with. The length of the network ID in bytes depends on the IP address class. The IP address can be set to four bytes. Set the network ID from the beginning of the text box and enter zeros for any unused digits. You can set up to eight records. No records are set in the default settings.

Settings on the Ethernet Tab Page



The following settings are provided on the Ethernet Tab Page of the Unit Setup for the EtherNet/IP Unit or built-in EtherNet/IP port.

- Link settings (baud rate and half/full duplex)

Link Setting

Sets the communications baud rate.

Setting	Meaning
Auto (default)	The baud rate with the switching hub is detected automatically. If possible, the Unit operates in 100Base-T (full duplex).
10 Mbps, Half Duplex	Operates in 10Base-T, half duplex.
10 Mbps, Full Duplex	Operates in 10Base-T, full duplex.
100 Mbps, Half Duplex	Operates in 100Base-TX, half duplex.
100 Mbps, Full Duplex	Operates in 100Base-TX, full duplex.

Note Adjust the EtherNet/IP Unit's link settings to match the communications settings of the connected switching hub. If the settings do not match, the link will become unstable and prevent normal communications. The following table shows the allowed settings for each switching hub communications mode.

Switching hub setting		EtherNet/IP Unit setting				
		Auto-negotiation	10 Mbps (fixed)		100 Mbps (fixed)	
			Full duplex	Half duplex	Full duplex	Half duplex
Auto-negotiation		Best	---	OK	---	OK
10 Mbps (fixed)	Full duplex	---	OK	---	---	---
	Half duplex	OK	---	OK	---	---
100 Mbps (fixed)	Full duplex	---	---	---	Best	---
	Half duplex	OK	---	---	---	OK

Note Best = Recommended; OK = Allowed; --- = Not allowed.

LLDP Settings (CJ3M-CPU3□ only)

Set whether or not to use the LLDP (Link Layer Discovery Protocol) function.

- Use: Enabled LLDP.
- Not Use: Disabled LLDP.

No records are set in the default settings.

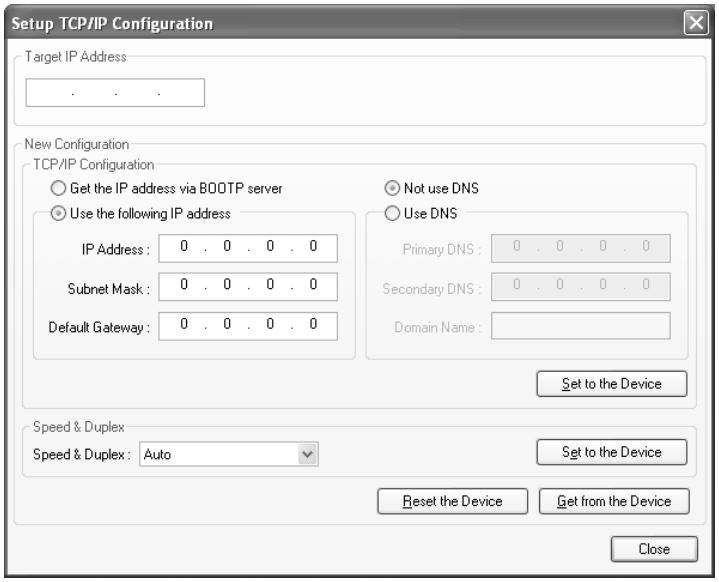
3-8-2 Making TCP/IP Settings with the Network Configurator

Use the Network Configurator to change IP address settings for any device other than a CS/CJ-series EtherNet/IP Unit or built-in port. You can also use the Network Configurator to change IP address settings for a CS/CJ-series EtherNet/IP Unit or built-in port.

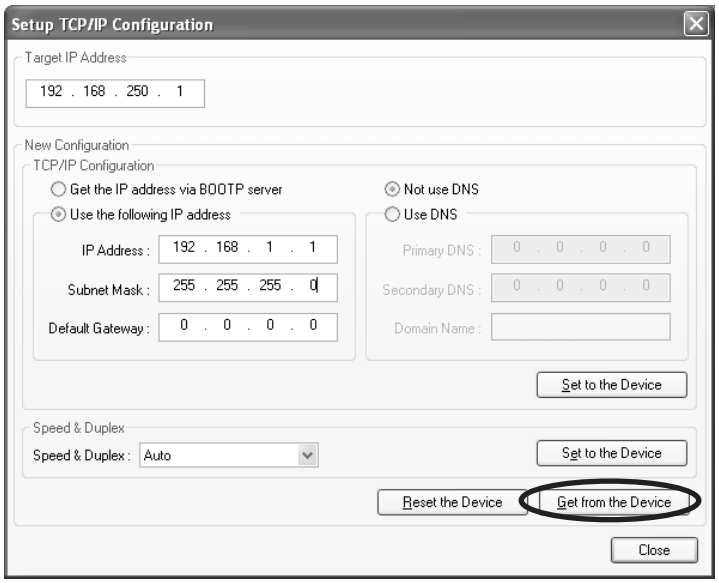
1,2,3... 1. Connect the Network Configurator online.

Refer to *6-2-9 Connecting the Network Configurator to the Network* for details on connecting the Network Configurator to the EtherNet/IP Unit.

2. Select ***Tools - Setup TCP/IP Configuration*** to display the following Setup TCP/IP Configuration Dialog Box, and set the TCP/IP Configuration for the target device. In the following example, the settings are all at their default values.



3. Enter the IP address to set and press the **Get from the Device** Button. The present setting will be obtained. Change the IP address in the *New Configuration* Box if required.



4. Press the **Set to the Device** Button. The IP address will be transferred to the device. The applicable device is the device specified in the *Target IP Address* Box. The device must be reset to enable the transferred setting. If the device is not reset when the new IP address is transferred, click the **Reset the Device** Button.
   When the EtherNet/IP Unit is reset, the IP address will be displayed once in flowing text on the 7-segment display on the front of the Unit.

Note

(1) The transfer function for IP address settings is defined by ODVA specifications. Target devices that do not support these specifications cannot be set. When setting the IP address of the target device with the Network Configurator, connect the devices one at a time, and download the TCP/IP Configuration's IP address parameters. If TCP/IP parameters are set for the EtherNet/IP Unit or built-in EtherNet/IP port from the Network Configurator, the EtherNet/IP Unit may automatically be reset and restarted. Before setting the TCP/IP parameters, make sure that no system problems will occur when the Unit is restarted. If the Unit does not restart automatically, click the **Reset the Device** Button.

(2) If the target node address (IP address) is not set correctly, invalid device parameters may be set in the wrong PLC, so check the connected PLC before downloading parameters.

TCP/IP Parameters

The following TCP/IP parameters can be set from the Network Configurator.

- IP address
- Subnet mask
- Default gateway
- Preferred DNS server
- Alternate DNS server
- Domain name
- Link parameters (baud rate and full/half duplex)

The operation specifications when *Get the IP address via BOOTP server* is selected in the Setup TCP/IP Configuration Dialog Box in the Network Configurator are as follows.

EtherNet/IP Unit or built-in EtherNet/IP port	Operation specification
CS1W/CJ1W-EIP21S CJ3M-CPU3□	Gets the IP address from the BOOTP server each time the power is turned ON or the Unit is restarted.
CS1W/CJ1W-EIP21 CJ2H-CPU6□-EIP CJ2M-CPU3□	Gets the IP address from the BOOTP server when the power is turned ON or the Unit is restarted for the first time. The Unit does not get the IP address from the BOOTP server for the second and subsequent power ON or restart operations.

Except for the above, the meanings of the settings are the same as those described in the setting procedure with the CX-Programmer.

3-9 Tag Data Link Parameters

Set the following parameters when using tag data links with an EtherNet/IP Unit or built-in EtherNet/IP port. The parameter settings are saved in flash memory in the EtherNet/IP Unit or CPU Unit. (See note.)

Note The CPU Bus Unit Setup Area is not used for tag data link settings for an EtherNet/IP Unit or built-in EtherNet/IP port. This point is different from the operation of Ethernet Units.

Refer to *SECTION 6 Tag Data Link Functions* for details.

3-9-1 Network Configurator Setting Procedure

The methods for setting tag data links using the Network Configurator can be roughly divided into the following two.

1. Using the EtherNet/IP Datalink Tool in the Network Configurator to Set the Parameters

With this method, there is no flexibility in the settings, but you can easily set the data link parameters using only memory addresses, and the settings will conform to Controller Link data link parameters.

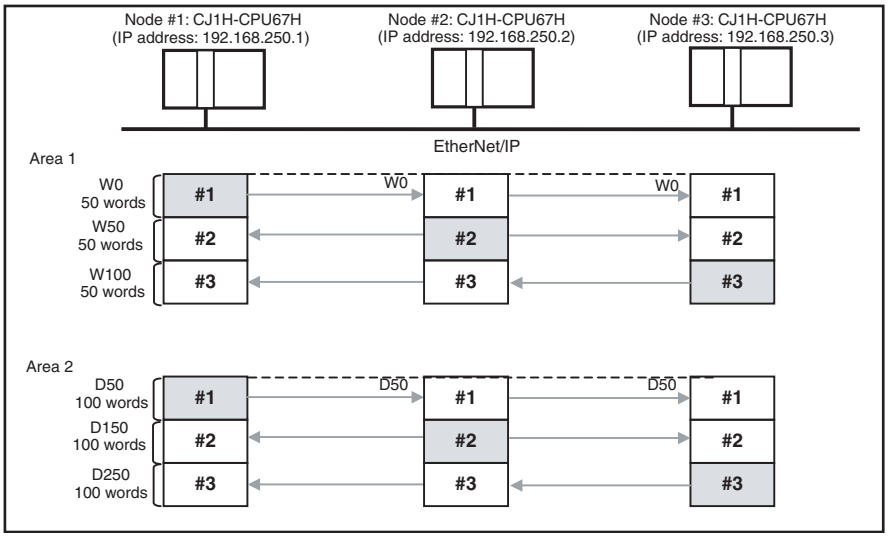
2. Using the Tag Data Link Setting Function in the Network Configurator to Set the Parameters

With this method, you can set the connections that comprise the tag data links for each EtherNet/IP node. Tag data links can be set with a high degree of flexibility using both memory addresses and network variables. Refer to *SECTION 6 Tag Data Link Functions* for details on how to perform these settings. This section presents a setting example using the EtherNet/IP Datalink Tool.

Using the EtherNet/IP Datalink Tool

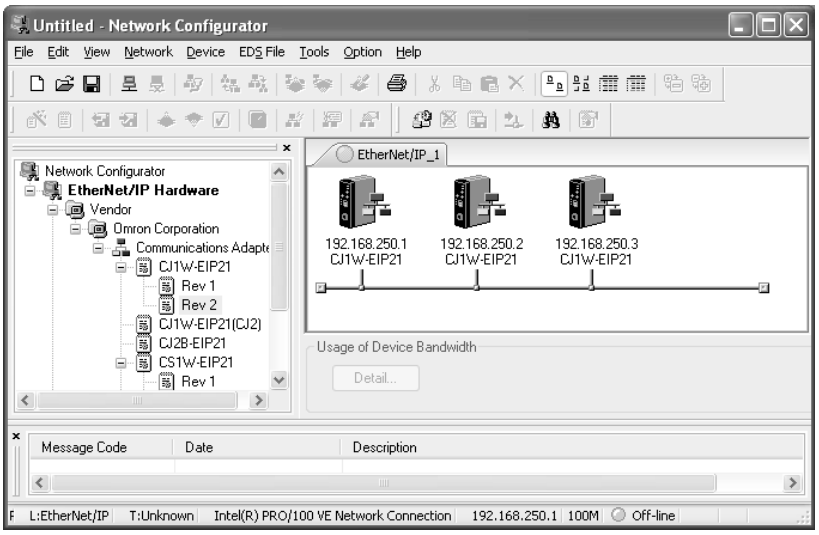
The method that is described here is used to set memory addresses in tables to specify data links between EtherNet/IP Units or built-in EtherNet/IP ports on CS/CJ-series PLCs.

The following method can be used to easily set the data links shown in the following figure using a wizard in the EtherNet/IP Datalink Tool.

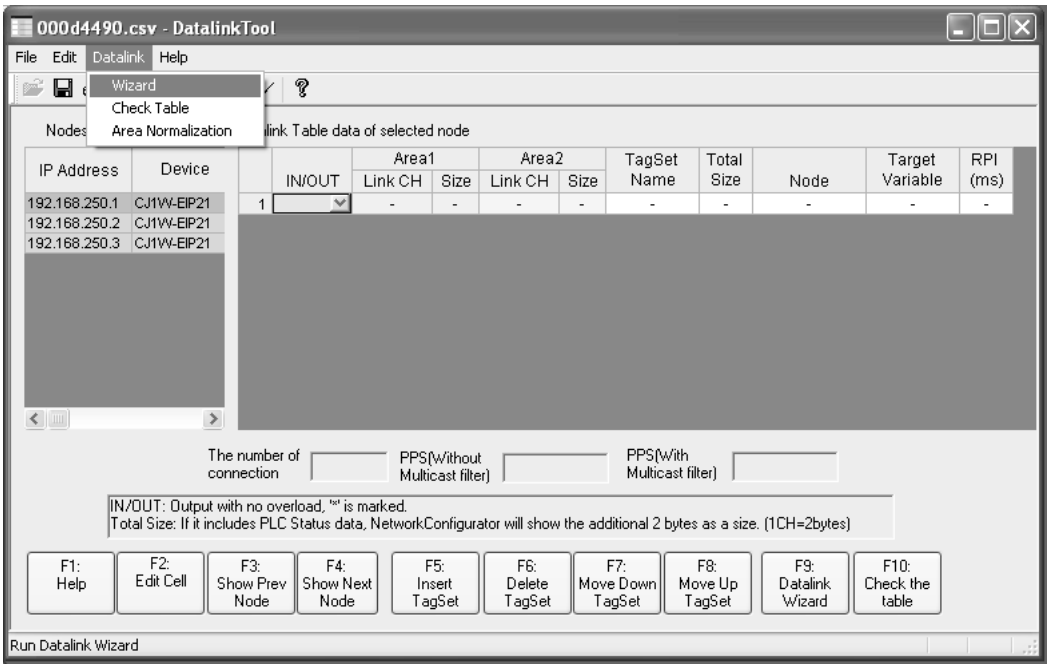


1,2,3... 1. Start the Network Configurator, select the applicable EtherNet/IP Unit in the Tree View on the left, and then paste it into the Device Configuration Pane on the right.

Note If an EtherNet/IP system has already been installed, you can create a similar device configuration by connecting to the EtherNet/IP network and selecting ***Network*** – ***Upload*** from the menus.
Refer to *6-2-9 Connecting the Network Configurator to the Network* for information on connecting.

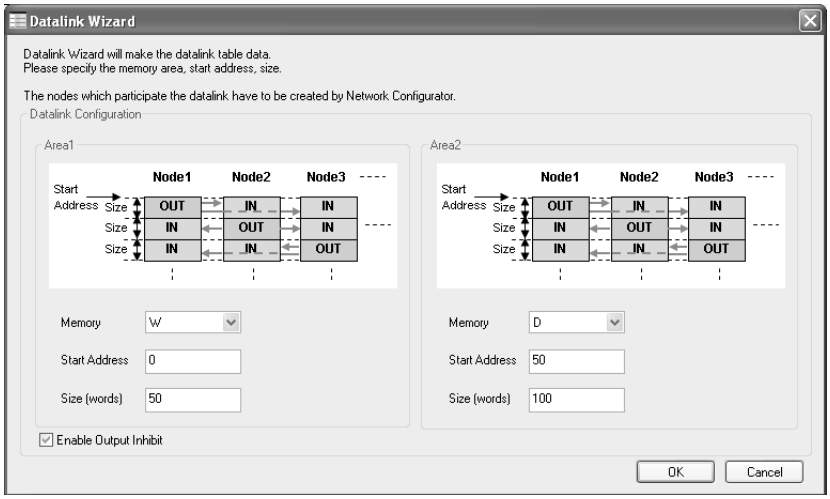


2. Select ***Network*** – ***EtherNet/IP Datalink*** Tool from the menus to start the EtherNet/IP Datalink Tool.
3. Select ***Datalink*** – ***Wizard*** from the menus in the Datalink Tool when it has started.

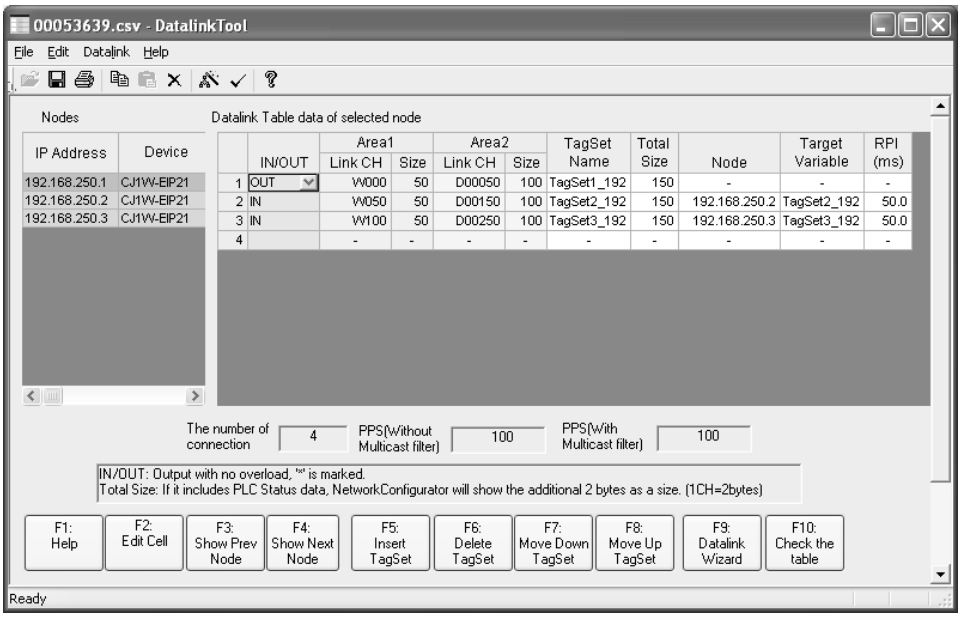


4. In the Datalink Wizard Dialog Box, enter 50 words starting from memory address W000 for area 1 and 100 words starting from D00050 for area 2,

and then press the **OK** Button.

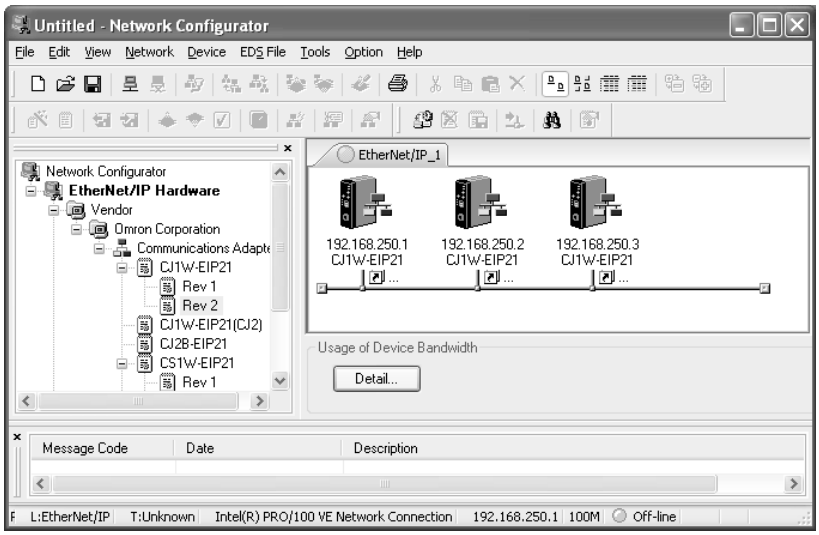


5. The data link settings will be automatically created in the window of the EtherNet/IP Datalink Tool. Select ***File*** – ***Save*** to end. The settings will be saved in the Network Configurator.



6. In the Device Configuration Window of the Network Configurator, a .. mark will be added to each EtherNet/IP Unit to show that data links have

been set.



7. Connect the Network Configurator to the EtherNet/IP network and select ***Network*** – ***Download*** from the menus. The data link settings will be downloaded to the EtherNet/IP Units, and the data links will operate.

3-10 User Authentication Settings

This section describes how to make the security settings of CS1W-EIP21S, CJ1W-EIP21S, and CJ3M-CPU3□.

Use the EIP21S User Management Tool to make the user authentication settings.

The setting data is stored in the non-volatile memory of the CS1W-EIP21S or CJ1W-EIP21S, and CJ3M-CPU3□.

Refer to *13-3 User Authentication* for details on the user authentication setting items and their descriptions.

Note If the OS of your PC is earlier than Windows 10, you cannot either install the EIP21S User Management Tool or select Secure Comm in the CX-Programmer and the PLC Backup Tool.

If the Windows 10 version is earlier than 1803, you cannot either go online by Secure Comm or use the function derived from Secure Comm.

3-11 Other Parameters

In addition to the tag data link parameters, the EtherNet/IP Unit and built-in EtherNet/IP port also have the following communications and operation parameters.

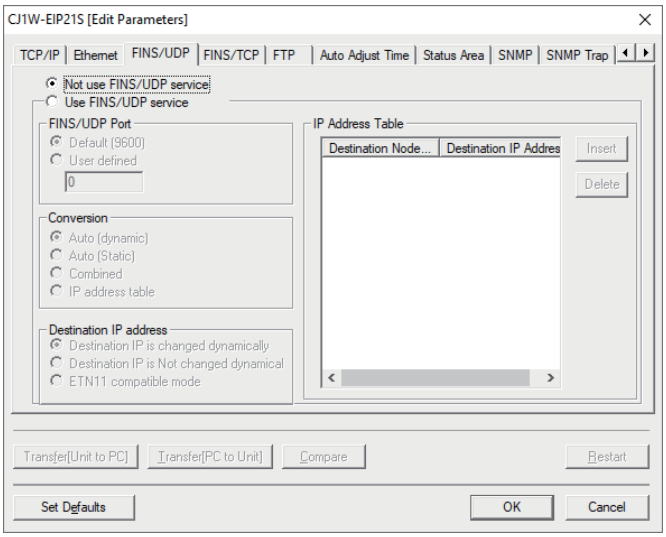
- FINS/UDP
- FINS/TCP
- FTP
- Auto Adjust Time
- Status Area
- SNMP
- SNMP Trap
- IP Packet Filter (CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ Only)
- CIP Settings (CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ Only)
- Modbus Server (CJ3M-CPU3☐ Only)

These parameters are set as Unit Setup from the CX-Programmer. The parameter settings are saved in flash memory in the EtherNet/IP Unit or CPU Unit. (See note.)

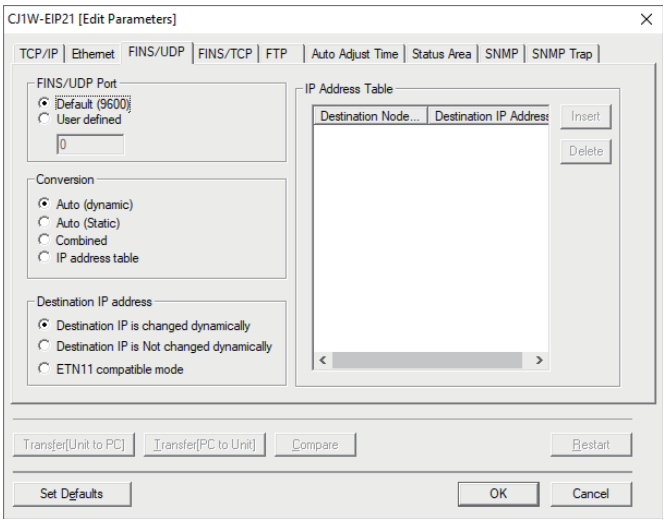
Note The CPU Bus Unit Setup Area is not used for tag data link settings for an EtherNet/IP Unit or built-in EtherNet/IP port. This point is different from the operation of Ethernet Units.

Using FINS/UDP

Dialog box for CS1W/CJ1W-EIP21S or CJ3M-CPU3☐



Dialog box for CS1W/CJ1W-EIP21, CJ2H-CPU6□-EIP or CJ2M-CPU3□

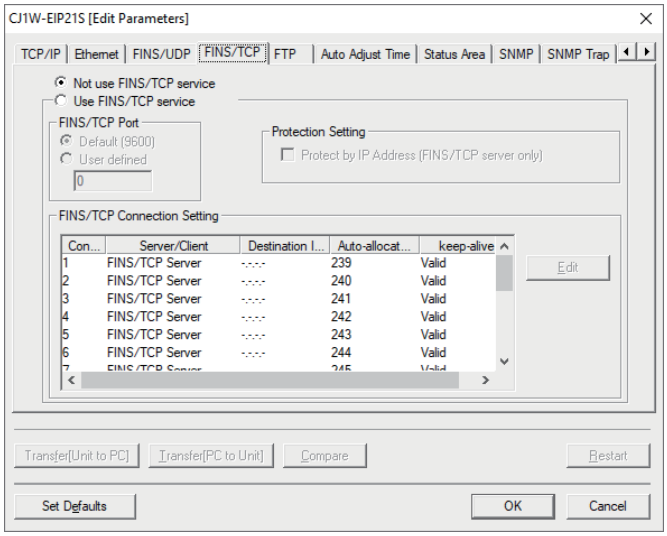


Tab Page in Edit Parameters Dialog Box	Setting	Function
FINS/UDP	Use of FINS/UDP (See note 1.)	Select whether or not to use FINS/UDP services. Selecting to use the services enables the following settings. • Not use FINS/UDP service (default) • Use FINS/UDP service
	FINS/UDP Port	Specifies the local UDP port number to use in the FINS communications service. The UDP uses the UDP port number to distinguish the application layer (FINS communications service in this case). • Default value (9,600) • User-set value (1 to 65,535)
	Conversion	Selects one of the following methods to convert from the FINS node address to an IP address (FINS/UDP only). • Automatic generation (dynamic setting) • Automatic generation (static setting) • IP address table • Combined method
	IP Address Table	Sets the IP address table that defines the relationship between FINS node addresses and IP addresses. This table is effective only when FINS/UDP is being used and the IP address conversion method is set to the IP address table.
	Destination IP is changed dynamically	Selects dynamic change of other FINS/UDP nodes' IP addresses. To disable dynamic changes, deselect this option by removing the check mark.

Note (1) This setting is provided for CS1W/CJ1W-EIP21S or CJ3M-CPU3□ only.

When necessary, set the routing tables using the CX-Integrator.

Using FINS/TCP



Tab Page in Edit Parameters Dialog Box	Setting	Function
FINS/TCP	Use of FINS/TCP (See note 1.)	Select whether or not to use FINS/TCP services. Selecting to use the services enables the following settings. • Not use FINS/TCP service (default) • Use FINS/TCP service
	FINS/TCP Port	Specifies the local TCP port number to use in the FINS communications service. The TCP uses the TCP port number to distinguish the application layer (FINS communications service in this case). • Default value (9,600) • User-set value (1 to 65,535) (See note 2.)
	FINS/TCP Connection Setup	This is the network API used when TCP is used for the FINS communications service. Up to 16 APIs can be used at a time, and they are identified by connection numbers 1 to 16. The EtherNet/IP Unit or built-in EtherNet/IP port can thus simultaneously execute the FINS communications service by TCP with up to 16 remote nodes.
	Protection Setting	Select this check box to refuse connection requests from any IP address not set as the target IP address when the server/client setting is set to a server and the target IP address is set to any value other than 0.0.0.0. This check box can be selected to prevent inappropriate operations on the PLC for FINS commands from specific nodes.

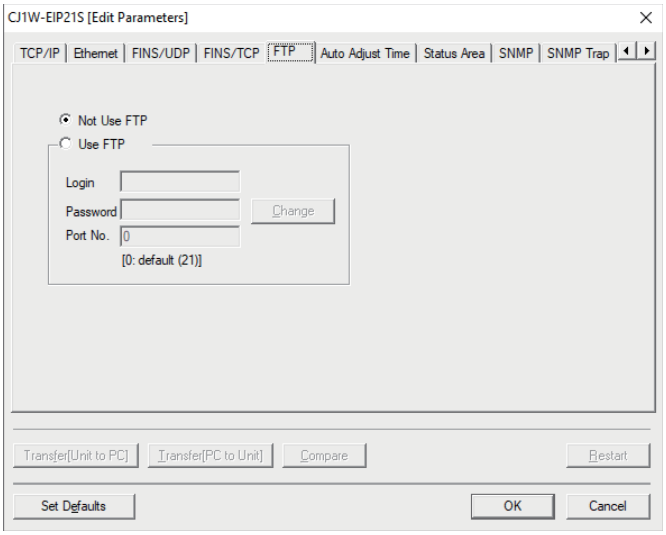
Note (1) This setting is provided for CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ only.

(2) Do not set the following values when you set FINS/TCP client connections in FINS/TCP connection setup.
From 1,024 to (1,024 + n-1), (n is the number of FINS/TCP client connections).

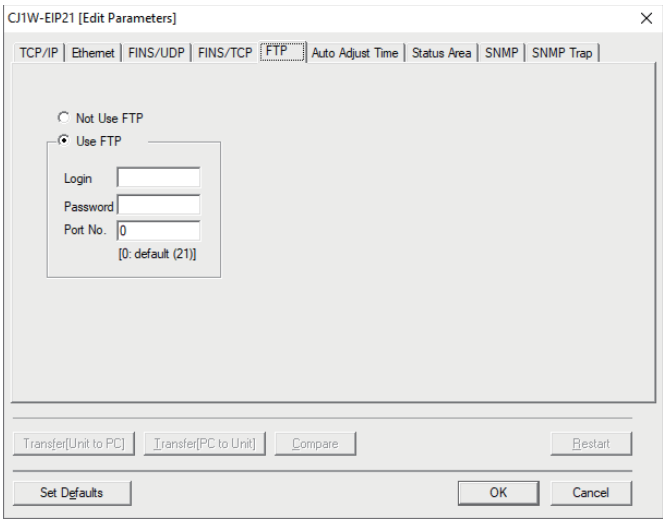
When necessary, set the routing tables using the CX-Integrator.

Using FTP

Dialog box for CS1W/CJ1W-EIP21S or CJ3M-CPU3□



Dialog box for CS1W/CJ1W-EIP21, CJ2H-CPU6□-EIP or CJ2M-CPU3□



Tab Page in Edit Parameters Dialog Box	Setting	Function
FTP	Not Use FTP or Use FTP	Specifies whether to use FTP. FTP connections from external devices will not be possible if *Not Use FTP* is specified.
	Login (See note 1 and 2.)	Sets the login name for FTP connections to the EtherNet/IP Unit or built-in EtherNet/IP port from external devices.
	Password (See note 1 and 3.)	Sets the password for FTP connections to the EtherNet/IP Unit or built-in EtherNet/IP port from external devices.
	Port No.	Sets the FTP port number of the EtherNet/IP Unit or built-in EtherNet/IP port. It is normally not necessary to change this setting. Two ports are used with the FTP: a control port and a data transfer port. Only the control port can be set. The data transfer port number will be one larger than the control port number.

(1) The operation when the login name and password are not set depends on the Unit model number.

Unit model number	Operation
CS1W/CJ1W-EIP21S CJ3M-CPU3☐	Login is not allowed.
CS1W/CJ1W-EIP21 CJ2H-CPU6☐-EIP CJ2M-CPU3☐	Using the login name *CONFIDENTIAL* allows for login without password check.

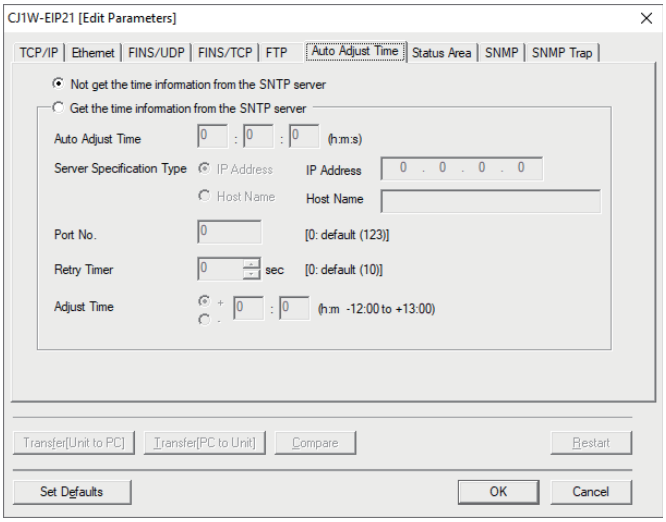
(2) Specifications differ Unit models.

Item	CS1W/CJ1W-EIP21S CJ3M-CPU3☐	CS1W/CJ1W-EIP21 CJ2H-CPU6☐-EIP CJ2M-CPU3☐
Login	User name length: 1 to 16 characters Default user name: None	User name length: 0 to 12 characters Default user name: CONFIDENTIAL

(3) Specifications differ Unit models.

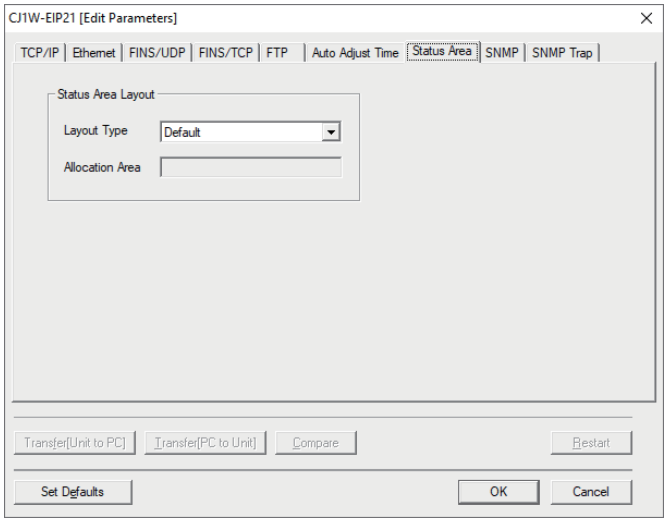
Item	CS1W/CJ1W-EIP21S CJ3M-CPU3☐	CS1W/CJ1W-EIP21 CJ2H-CPU6☐-EIP CJ2M-CPU3☐
Password	Password length: 8 to 16 characters The entered password is replaced by asterisks.	Password length: 0 to 8 characters Default password: None

Using the Automatic Time Adjustment



Tab Page in Edit Parameters Dialog Box	Setting	Function
Auto Adjust Time	Not get the time information from the SNTP server or Get the time information from the SNTP server	Specifies whether to set the clock in the CPU Unit to the time on the SNTP server. The time can be set only in CPU Units with an EtherNet/IP Unit or a built-in EtherNet/IP port.
	Auto Adjust Time	Sets the time to access the SNTP server to automatically adjust the CPU Unit clock. When the specified time arrives, the SNTP server will be accessed and the clock in the CPU Unit will be set to the time on the SNTP server.
	Server Specification Type	Specifies whether to use an IP address or a domain name (i.e., host name) to specify the SNTP server to use for automatic time adjustment.
	IP Address	Sets the IP address of the SNTP server to use for automatic time adjustment. This IP address is valid only when the Server Specification Type is set to an IP address.
	Host Name	Sets the host name of the SNTP server to use for automatic time adjustment. This IP address is valid only when the Server Specification Type is set to a host name.
	Port No.	Sets the port number to use to connect to the SNTP server for automatic time adjustment. It is normally not necessary to change this setting.
	Retry Timer	Sets the time to wait before retrying the connection when connecting to the SNTP server fails. It is normally not necessary to change this setting.
	Adjust Time	Sets the time to offset the clock in the CPU Unit when setting the clock in the CPU Unit to the time obtained from the SNTP server. To use the time from the SNTP server as is, enter 0 for the Adjust Time.

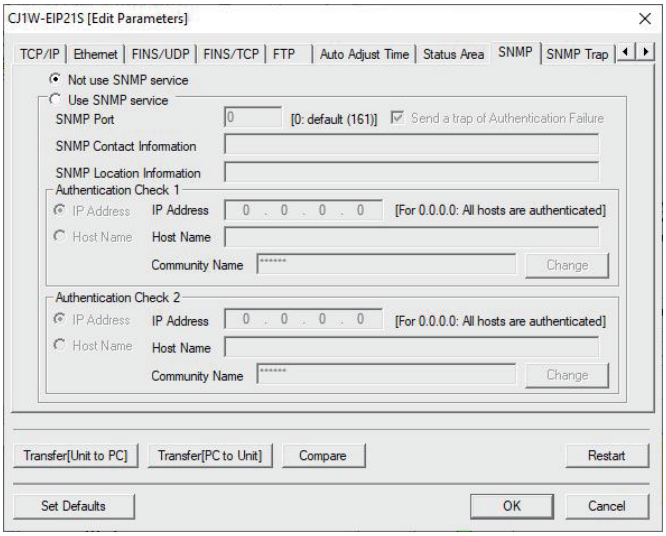
Using the Status Area



Tab Page in Edit Parameters Dialog Box	Setting	Function
Status Area	Layout Type	Specifies whether to use the Default setting or the User defined setting for the words allocated to the status area. (See note 1.)
	Allocation Area	Sets the first word in the status area when the Layout Type is set for the User defined setting. With CS1/CJ1 CPU Units, only an I/O memory address can be set. With CJ2 or NE1S CPU Units, either an I/O memory address or a symbol defined in the CPU Unit can be set.

Note (1) To use socket service functions with the CS1W/CJ1W-EIP21S and CJ3M-CPU3☐, set this to “User settings.”

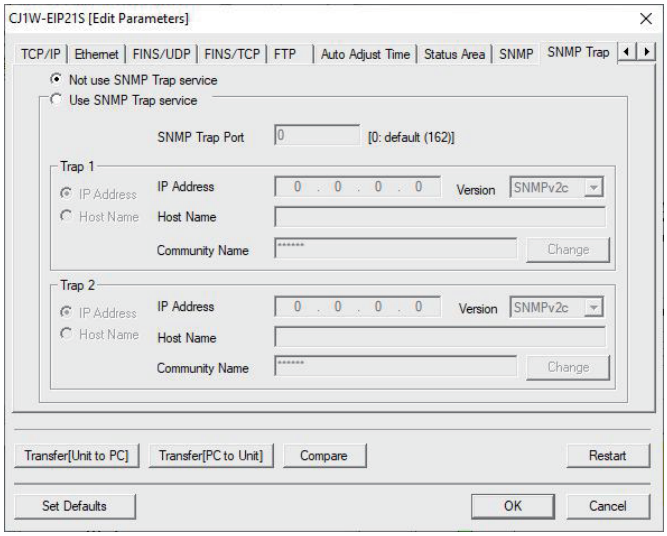
Using SNMP



Tab Page in Edit Parameters Dialog Box	Setting	Function
SNMP	Not use SNMP service or Use SNMP service	Specifies whether to use the SNMP. If not using the SNMP service is specified, an SNMP manager will not be able to connected from an external device.
	SNMP Port	Sets the port number to use when connecting from an SNMP manager. It is normally not necessary to change this setting.
	SNMP Contact Information	Specifies the contact information as text. This information can be read from the SNMP manager.
	SNMP Location Information	Specifies the location information as text. This information can be read from the SNMP manager.
	Authentication Check 1/2	Specifies the SNMP managers that can access the PLC. To restrict access to only specific SNMP managers, specify the SNMP managers using IP addresses or host names. Community names can also be specified (e.g., public). (See note 1.) Ether one or two settings can be made.

Note (1) In the CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ the entered community name is replaced by asterisks.

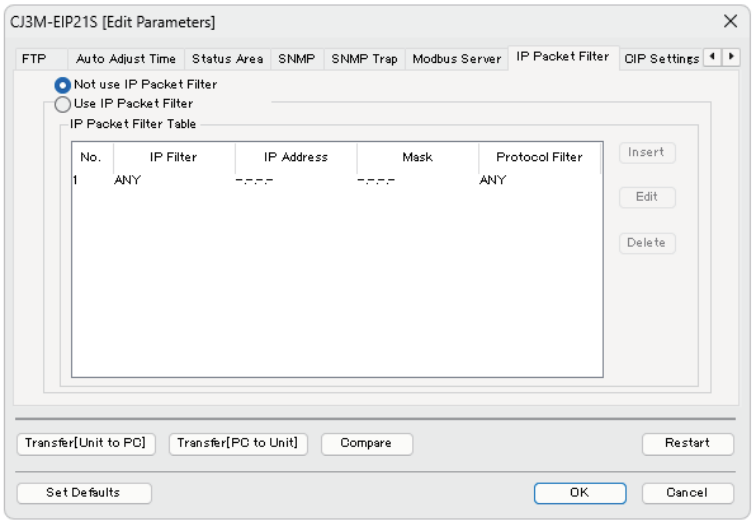
Using SNMP Trap



Tab Page in Edit Parameters Dialog Box	Setting	Function
SNMP Trap	Not use SNMP Trap service or Use SNMP Trap service	Specifies whether to use the SNMP trap. If not using the SNMP trap service is specified, SNMP traps cannot be sent to the SNMP manager.
	SNMP Trap Port	Sets the port number to use to connect to the SNMP manager. It is normally not necessary to change this setting.
	Trap 1/2	Sets the SNMP manager destinations for SNMP traps. The SNMP managers can be specified using IP addresses or host names. Community names can also be specified (e.g., public). (See note 1.) Either one or two trap destinations can be set.

Note (1) In the CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ the entered community name is replaced by asterisks.

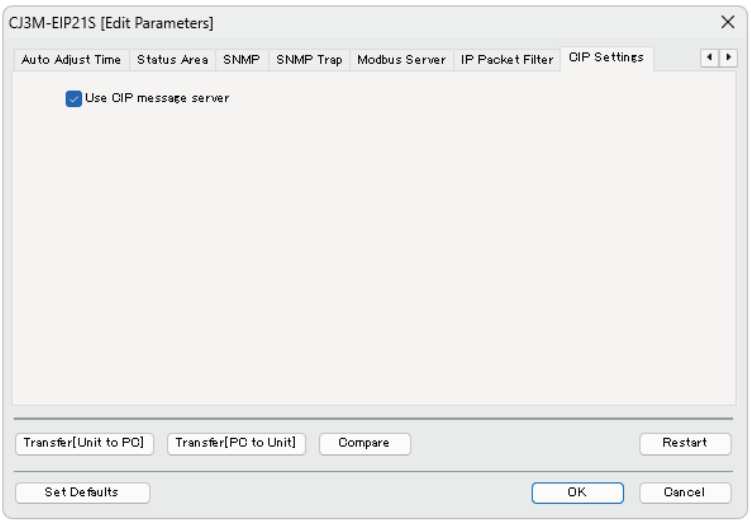
Using the IP Packet Filtering Function



Tab Page in Edit Parameters Dialog Box	Setting	Function
IP Packet Filter	Not use IP Packet Filter or Use IP Packet Filter	Select whether or not to use the IP packet filtering. This function selectively permits packets that EtherNet/IP ports receive to pass through the filter according to set conditions. • Not use IP Packet Filter (default) • Use IP Packet Filter

Note Refer to *13-5 IP Packet Filtering* for details.
This is enabled for CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ only.

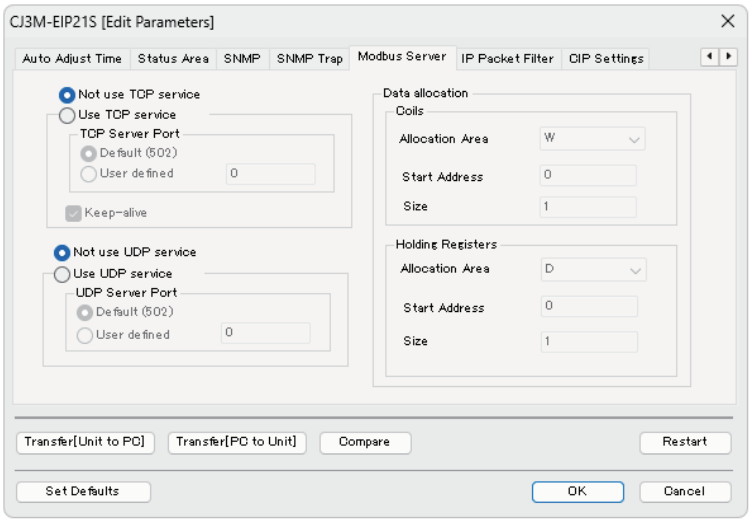
Using the CIP Communication Function



Tab Page in Edit Parameters Dialog Box	Setting	Function
CIP Communication	Use CIP message server	Select whether or not to use the CIP message server (Class 3, UCMM) and tag data links. When the check box is cleared, CIP messages (Class 3, UCMM) and tag data links cannot be used. • Check box selected: Use (default) • Check box cleared: Not use

Note This is enabled for CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ only.

Using the Modbus Server Function



Tab Page in Edit Parameters Dialog Box	Setting	Function
Modbus Server	Not use Modbus Server or Use Modbus Server	Select whether or not to use the Modbus server function. When using this function, you can set the other settings of the Modbus server. • Not use TCP service (default) • Not use UDP service (default)

Note Refer to *15-2 Modbus Server Settings* for details.
This is enabled for CJ3M-CPU3☐ only.

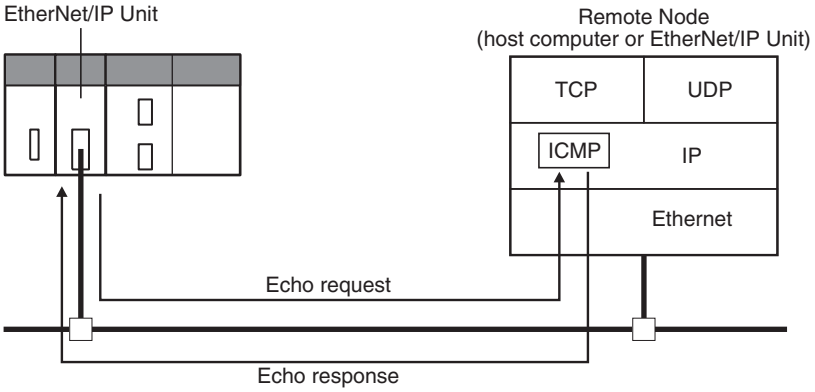
3-12 Communications Test

If the basic settings (in particular the IP address and subnet mask) have been made correctly for the EtherNet/IP Unit or built-in EtherNet/IP port, then it should be possible to communicate with nodes on the EtherNet/IP network. This section describes how to use the PING command to test communications with the EtherNet/IP Unit or built-in EtherNet/IP port.

3-12-1 PING Command

The PING command sends an echo request packet to a remote node and receives an echo response packet to confirm that the remote node is communicating correctly. The PING command uses the ICMP echo request and responses. The echo response packet is automatically returned in the ICMP. The PING command is normally used to check the connections of remote nodes when configuring a network. The EtherNet/IP Unit or built-in EtherNet/IP port supports both the ICMP echo request and reply functions.

If the remote node returns a normal response to the PING command, then the nodes are physically connected correctly and Ethernet node settings are correct.



3-12-2 EtherNet/IP Unit or Built-in EtherNet/IP Port Operation

The EtherNet/IP Unit or built-in EtherNet/IP port automatically returns the echo response packet in response to an echo request packet sent by another node (host computer, or other EtherNet/IP Unit or built-in EtherNet/IP port). An echo request packet can be sent to another node by issuing the FINS command to execute the PING command from the PLC.

3-12-3 Host Computer Operation

The PING command can be executed from the host computer to send an echo request packet to an EtherNet/IP Unit or built-in EtherNet/IP port. The following example shows how to use the PING command in the host computer.

Command Method

Input the following command at the host computer's prompt ($):
$ ping IP_address(host_name)
The destination is specified by its IP address or host name. If the host name is used, the host name must be defined in the /etc/hosts file.

Note The PING command is not supported by some host computers.

Application Example

In this example, a PING command is sent to the node at IP address 130.25.36.8. The “$” in the example represents the host computer prompt.

Normal Execution

```
$ ping   130.25.36.8                          ← Executes the PING command.
PING   130.25.36.8: 56  data  bytes
64   bytes   from   130.25.36.8:   icmp_seq=0.   time=0. ms
64   bytes   from   130.25.36.8:   icmp_seq=0.   time=0. ms
              :              :              :              :              :
64   bytes   from   130.25.36.8:   icmp_seq=0.   time=0. ms
                                              ← Press the Ctrl+C Keys to cancel execution.
---- 130.25.36.8   PING   Statistics ----
9 packets   transmitted,   9 packets  received,   0% packets  loss
round-trip (ms)   min/avg/max   = 0/1/16
$
```

Error Occurred

```
$ png   130.25.36.8                           ← Executes the PING command.
PING   130.25.36.8: 56  data  bytes
                                              ← Press the Ctrl+C Keys to cancel execution.
---- 130.25.36.8   PING   Statistics ----
9 packets   transmitted,   9 packets  received,   0% packets  loss
$
```

Refer to the OS command reference manual for your computer for details on using the PING command.

SECTION 4
Memory Allocations

This section describes the words allocated in the CIO Area and the DM Area for EtherNet/IP Units or built-in EtherNet/IP ports.

4-1 Overview of Memory Allocated to the EtherNet/IP Unit 94
4-2 CIO Area Allocations 96
4-2-1 Overview of the Allocated CIO Area Words 96
4-2-2 Details of the Allocated CIO Area Words 99
4-3 DM Area Allocations 114
4-3-1 Overview of the Allocated DM Area Words 114
4-3-2 Details of the Allocated DM Area Words 114
4-4 User Settings Area 117
4-4-1 Overview of the User Settings Area 117
4-4-2 User Settings Area 117
4-5 Auxiliary Area Data. 120
4-5-1 Read-only Bits/Words 120
4-5-2 Read/Write Bits 121

4-1 Overview of Memory Allocated to the EtherNet/IP Unit

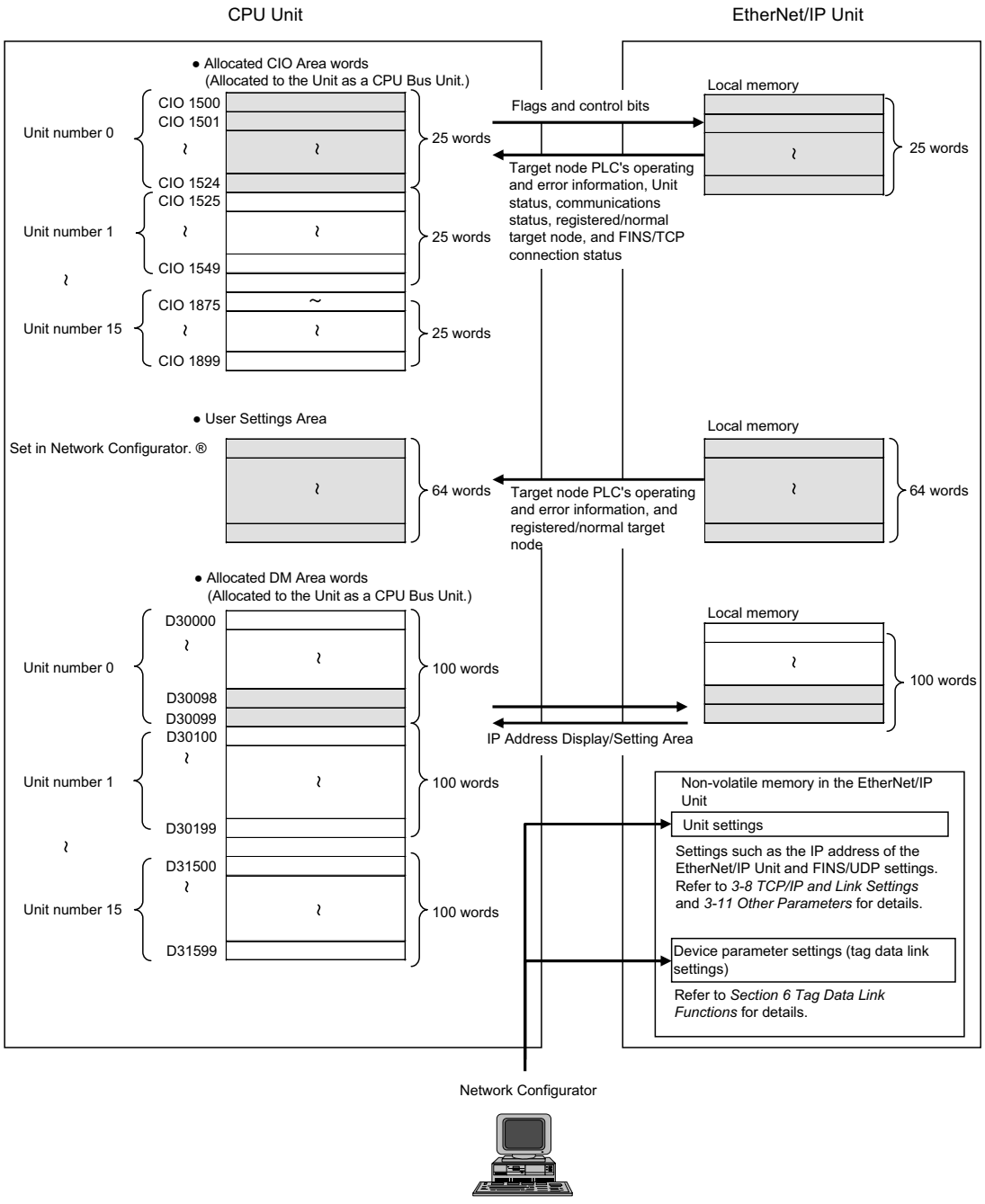
The following CPU Unit words are allocated to the EtherNet/IP Unit or built-in EtherNet/IP port.

- CPU Unit's allocated CIO Area words
  Contains software switch and status information, and software switch and status information related to socket communications.*1
- CPU Unit's allocated DM Area words
  Contains the IP Address Display/Setting Area
- CPU Unit's user settings area
  Contains status information. (This area can be used only when the allocated CIO Area words are set to user settings.)

*1 For use with the CS1W/CJ1W-EIP21S and CJ3M-CPU3□, the status area layout must be set to "User settings."

Note The EtherNet/IP Unit or built-in EtherNet/IP port has the following two data areas in its non-volatile memory. (Unlike the Ethernet Units, settings are not stored in the CPU Unit's CPU Bus Unit System Setup Area.)

- Unit Setup: Settings such as the IP address and FINS/UDP settings. The Unit Setup is set from the CX-Programmer.
- Device parameter settings: Settings such as the tag data link setting parameters. The device parameter settings are made from the Network Configurator.


CPU Unit
EtherNet/IP Unit
● Allocated CIO Area words
(Allocated to the Unit as a CPU Bus Unit.)
CIO 1500
CIO 1501
Unit number 0
CIO 1524
CIO 1525
Unit number 1
CIO 1549
CIO 1875
Unit number 15
CIO 1899
25 words
25 words
25 words
Flags and control bits
Target node PLC's operating and error information, Unit status, communications status, registered/normal target node, and FINS/TCP connection status
Local memory
25 words
● User Settings Area
Set in Network Configurator. ®
64 words
Target node PLC's operating and error information, and registered/normal target node
Local memory
64 words
● Allocated DM Area words
(Allocated to the Unit as a CPU Bus Unit.)
D30000
Unit number 0
D30098
D30099
D30100
Unit number 1
D30199
D31500
Unit number 15
D31599
100 words
100 words
100 words
IP Address Display/Setting Area
Local memory
100 words
Non-volatile memory in the EtherNet/IP Unit
Unit settings
Settings such as the IP address of the EtherNet/IP Unit and FINS/UDP settings. Refer to *3-8 TCP/IP and Link Settings* and *3-11 Other Parameters* for details.
Device parameter settings (tag data link settings)
Refer to *Section 6 Tag Data Link Functions* for details.
Network Configurator

4-2 CIO Area Allocations

4-2-1 Overview of the Allocated CIO Area Words

The various kinds of data are stored in the allocated CIO Area words, which are identified by the offset from the beginning word (n) allocated to each Unit.

There are two patterns for the layout of the allocated CIO Area words: the default settings and user settings. The layout can be selected in the Status Area settings in the Edit Parameters Dialog Box from the CX-Programmer.

To set a customer areas, select *User defined* for the Layout Type on the Status Area Tab Page.

The beginning word n is calculated by the following equation:

Beginning word n = CIO 1500 + (25 × unit number)

Default Settings

Offset		Bit 15 8 7 0	Data direction
0	n	Unit control bits	CPU Unit → EtherNet/IP Unit
1	n+1	(Reserved)	EtherNet/IP Unit → CPU Unit
2	n+2	Target Node PLC Operating Information (4 words only)	EtherNet/IP Unit → CPU Unit
3	n+3		
4	n+4		
5	n+5		
6	n+6	Target Node PLC Error Information (4 words only)	EtherNet/IP Unit → CPU Unit
7	n+7		
8	n+8		
9	n+9		
10	n+10	Unit status 1	EtherNet/IP Unit → CPU Unit
11	n+11	Unit status 2	
12	n+12	Communications status 1	EtherNet/IP Unit → CPU Unit
13	n+13	Communications status 2	
14	n+14	Communications status 3	
15	n+15	(Reserved)	EtherNet/IP Unit → CPU Unit
16	n+16	Registered Target Node (4 words only)	EtherNet/IP Unit → CPU Unit
17	n+17		
18	n+18		
19	n+19		
20	n+20	Normal Target Node	EtherNet/IP Unit → CPU Unit
21	n+21	(4 words only)	
22	n+22		
23	n+23		
24	n+24	FINS/TCP Connection Status	EtherNet/IP Unit → CPU Unit

Note The reserved words are regularly refreshed with all zeroes.

User Settings

■ **CS1W/CJ1W-EIP21, CJ2H-CPU6□-EIP or CJ2M-CPU3□**

	Offset	Bit 15 8 7 0	Data direction
0	n	Unit control bits	CPU Unit → EtherNet/IP Unit
1	n+1	(Reserved)	EtherNet/IP Unit → CPU Unit
2	n+2		
3	n+3		
4	n+4		
5	n+5		
6	n+6		
7	n+7		
8	n+8		
9	n+9		
10	n+10	Unit status 1	EtherNet/IP Unit → CPU Unit
11	n+11	Unit status 2	
12	n+12	Communications status 1	EtherNet/IP Unit → CPU Unit
13	n+13	Communications status 2	
14	n+14	Communications status 3	
15	n+15	(Reserved)	EtherNet/IP Unit → CPU Unit
16	n+16		
17	n+17		
18	n+18		
19	n+19		
20	n+20		
21	n+21		
22	n+22		
23	n+23		
24	n+24	FINS/TCP Connection Status	EtherNet/IP Unit → CPU Unit

Note The reserved words are regularly refreshed with all zeroes.

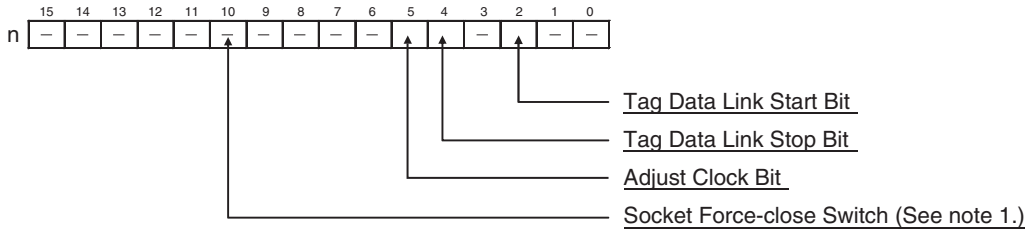
■ **CS1W/CJ1W-EIP21S or CJ3M-CPU3□**

Offset		Bit 15 – 8	Bit 7 – 0	Data direction
0	n	Unit control bits		CPU Unit → EtherNet/IP Unit
1	n+1	Socket Service Request Switch 2	Socket Service Request Switch 1	CPU Unit → EtherNet/IP Unit
2	n+2	Socket Service Request Switch 4	Socket Service Request Switch 3	
3	n+3	Socket Service Request Switch 6	Socket Service Request Switch 5	
4	n+4	Socket Service Request Switch 8	Socket Service Request Switch 7	
5	n+5	(Reserved)		
6	n+6			
7	n+7			
8	n+8			
9	n+9			
10	n+10	Unit status 1		EtherNet/IP Unit → CPU Unit
11	n+11	Unit status 2		
12	n+12	Communications status 1		EtherNet/IP Unit → CPU Unit
13	n+13	Communications status 2		
14	n+14	Communications status 3		
15	n+15	(Reserved)		
16	n+16	UDP Socket No. 2 Status	UDP Socket No. 1 Status	EtherNet/IP Unit → CPU Unit
17	n+17	UDP Socket No. 4 Status	UDP Socket No. 3 Status	
18	n+18	UDP Socket No. 6 Status	UDP Socket No. 5 Status	
19	n+19	UDP Socket No. 8 Status	UDP Socket No. 7 Status	
20	n+20	TCP Socket No. 2 Status	TCP Socket No. 1 Status	EtherNet/IP Unit → CPU Unit
21	n+21	TCP Socket No. 4 Status	TCP Socket No. 3 Status	
22	n+22	TCP Socket No. 6 Status	TCP Socket No. 5 Status	
23	n+23	TCP Socket No. 8 Status	TCP Socket No. 7 Status	
24	n+24	FINS/TCP Connection Status		EtherNet/IP Unit → CPU Unit

Note The reserved words are regularly refreshed with all zeroes.

4-2-2 Details of the Allocated CIO Area Words

Unit Control Bits (CPU Unit to EtherNet/IP Unit) (n)



Bit	Switch	Status	Manipulated by	Unit operation
0 to 1	(Not used.)	---	---	---
2	Tag Data Link Start Bit	ON	User	The tag data link starts when this bit is switched from OFF to ON.
		OFF	Unit	Turned OFF by Unit after the tag data link starts operating.
3	(Not used.)	---	---	---
4	Tag Data Link Stop Bit	ON	User	The tag data link stops when this bit is switched from OFF to ON.
		OFF	Unit	Turned OFF by Unit after the tag data link stops operating.
5	Adjust Clock Bit	ON	User	The clock time is automatically adjusted when this bit is switched from OFF to ON.
		OFF	Unit	Turned OFF by Unit after the clock time has been adjusted.
6 to 9	(Not used.)	---	---	---
10	Socket Force-close Switch (See note 1.)	ON	User	All sockets are forcibly closed when this bit is switched from OFF to ON.
		OFF	Unit	Turned OFF by Unit after sockets are closed.
11 to 15	(Not used.)			

Note (1) This switch is provided for CS1W/CJ1W-EIP21S or CJ3M-CPU3□ only.

Tag Data Link Start Bit (Bit 2)

Start the tag data links by switching this bit from OFF to ON. If the tag data links are already operating, the signal will be ignored. The tag data link starts operating automatically after the tag data link parameter settings are downloaded from the Network Configurator, the CPU Unit's power is turned ON, or the Unit is restarted.

If the tag data links have been stopped by turning the Tag Data Link Stop Bit (n bit 04) from OFF to ON, the tag data links can be restarted by turning this Tag Data Link Start Bit (n bit 02) from OFF to ON.

Once the tag data links start, the EtherNet/IP Unit automatically turns OFF the Tag Data Link Start Bit. Do not force this bit ON or OFF until it is automatically turned OFF by the Unit.

Tag Data Link Stop Bit (Bit 4)

Stop the tag data links by switching this bit from OFF to ON. Once the tag data links have been stopped, they will remain stopped until the Unit is restarted or the Tag Data Link Start Bit is turned ON. (The tag data links will also start operating automatically when the tag data link parameter settings are downloaded from the Network Configurator.)

If the tag data links are already stopped, the signal will be ignored.

Message communications can be performed while the tag data links are stopped.

Once the tag data links have stopped, the EtherNet/IP Unit automatically turns OFF the Tag Data Link Stop Bit. Do not force this bit ON or OFF until it is automatically turned OFF by the Unit.

Adjust Clock Bit (Bit 5)

Automatically adjust the time on the clock by switching this bit from OFF to ON. The SNTP server used to adjust the time is set in the Unit Setup.

Once the clock time has been adjusted, the EtherNet/IP Unit automatically turns OFF the Adjust Clock Bit. Do not force this bit ON or OFF until it is automatically turned OFF by the Unit.

Socket Force-close Switch (Bit 10)

All UDP and TCP sockets used for socket services can be force-closed by turning ON this switch. This can be used for operations such as error processing.

Be careful not to force-close sockets during communications, or an error will occur. After all sockets have been force-closed, the EtherNet/IP Unit will turn the switch OFF again. Do not attempt to forcibly manipulate this switch before it is automatically turned OFF by the Unit.

The ports for other than socket service functions used uniquely by CS1W/CJ1W-EIP21S and CJ3M-CPU3☐ Units are not closed.

This is enabled for CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ only.

Target Node PLC Operating Information (EtherNet/IP Unit to CPU Unit) (n + 2 to n + 5)

These words show the operating status of the target node PLCs that are connected with the EtherNet/IP Unit as the originator. This status information is enabled when the PLC status is included in the communications data in both the originator and target node.

These words show the status of nodes 0 to 63 only. If it is necessary to show the status of nodes higher than node 63, select “user settings” as the layout pattern. For details, refer to *4-4 User Settings Area*.

The flags are valid only when the corresponding Normal Target Node Flag is ON. If the corresponding Normal Target Node Flag is OFF, the Target Node PLC Operating Flag indicates the previous operating status.

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
n+2	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
n+3	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
n+4	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32
n+5	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48

Bit	Name	Status	Manipulated by	Unit operation
---	Target Node PLC Operating Flags	ON	Unit	The corresponding PLC is operating. (The program is being executed.)
		OFF	Unit	The PLC is not operating.

Target Node PLC Error Information (EtherNet/IP Unit to CPU Unit) (n + 6 to n + 9)

These words show the error status (logical OR of fatal and non-fatal errors) of the target node PLCs that are connected with the EtherNet/IP Unit as the originator. This status information is enabled when the PLC status is included in the communications data in both the originator and target node.

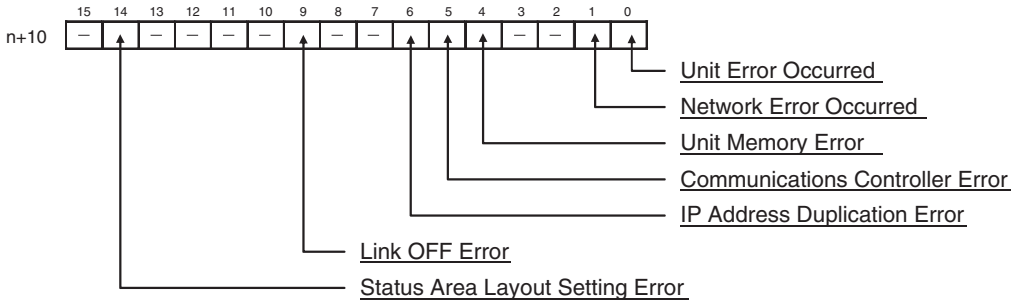
These words show the error status of nodes 0 to 63 only. If it is necessary to show the error status of nodes higher than node 63, select “user settings” as the layout pattern. For details, refer to *4-4 User Settings Area*.

The flags are valid only when the corresponding Normal Target Node Flag is ON. If the corresponding Normal Target Node Flag is OFF, the Target Node PLC Error Flag indicates the previous error status.

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
n+6	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
n+7	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
n+8	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32
n+9	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48

Bit	Name	Status	Manipulated by	Unit operation
---	Target Node PLC Error Flags	ON	Unit	A fatal or non-fatal error occurred in the corresponding PLC.
		OFF	Unit	No error occurred in the PLC.

Unit Status 1 (EtherNet/IP Unit to CPU Unit) (n + 10)

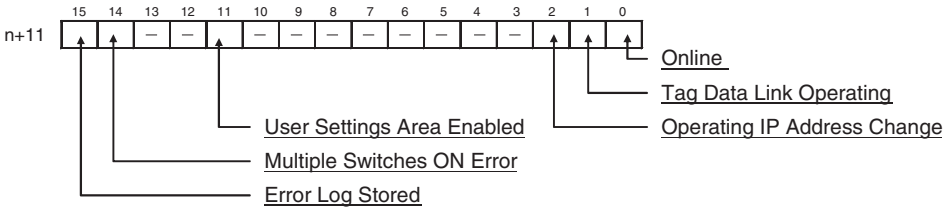


Bit	Name	Status	Manipulated by	Unit operation
0	Unit Error Occurred	ON	Unit	Indicates that an error occurred that is related to EtherNet/IP Unit operation. This flag is turned ON when any bit in Unit Status 1 is ON. (Bits 1 to 15 are logically ORed.)
		OFF	Unit	Indicates that a Unit error did not occur. This flag is turned OFF when the error is cleared.
1	Network Error Occurred	ON	Unit	One or more network-related errors occurred. (The bits in Communications Status 1 and 3 are logically ORed.)
		OFF	Unit	Indicates that a network error did not occur. This flag is turned OFF when the error is cleared.
2 to 3	(Not used)	---	---	---

Bit	Name	Status	Manipulated by	Unit operation
4	Unit Memory Error	ON	Unit	Indicates that an error occurred in accessing the Unit's internal non-volatile memory (device error).
		OFF	Unit	Indicates that a non-volatile memory error did not occur. This flag is not cleared even if it occurs one time. (Flag remains ON.)
5	Communications Controller Error	ON	Unit	Indicates that an error occurred in the communications controller.
		OFF	Unit	Indicates that a communications controller error did not occur. This flag remains ON until the power supply is turned OFF and ON again.
6	IP Address Duplication Error	ON	Unit	An ARP was sent with the specified IP address, indicating that an IP address duplication was detected. An address duplication is detected if there is an ARP response. This flag remains ON until the power supply is turned OFF and ON again. (The Ethernet interface will stop.)
		OFF	Unit	There was no ARP response.
7 to 8	(Not used)	---	---	---
9	Link OFF Error	ON	Unit	There was an error establishing a link with the switching hub.
		OFF	Unit	A link was established normally with the switching hub.
10 to 13	(Not used)	---	---	---

Bit	Name	Status	Manipulated by	Unit operation
14	Status Area Layout Setting Error	ON	Unit	Indicates that there was an error in the allocated CIO Area's layout settings. When this error occurs, the allocated CIO Area layout is set to the default pattern. In the following cases, however, the allocated CIO Area layout is set to the User defined pattern. In this case, the user settings area will not be refreshed. • The area (variable) is not defined in the Controller (only when a CJ2/CJ3 CPU Unit is connected). • The size of the area (variable) is not 64 words (only when a CJ2/CJ3 CPU Unit is connected). • The type of the area (variable) is TIM or CNT (only when a CJ2/CJ3 CPU Unit is connected). • The size of the area exceeds that of the specified area (e.g., CIO Area or DM Area). • A non-existent area has been specified.
		OFF	Unit	There was not an error in the layout settings.
15	(Not used)	---	---	---

Unit Status 2 (EtherNet/IP Unit to CPU Unit) (n + 11)



Bit	Name	Status	Manipulated by	Unit operation
0	Online	ON	Unit	Indicates that the Unit is online. (The EtherNet/IP Unit can perform communications processing.)
		OFF	Unit	Indicates that the Unit is not online. This bit is turned OFF in the following cases. • IP Address Duplication Error • Ethernet Communications Controller Error (hardware error) • BOOTP Server Error

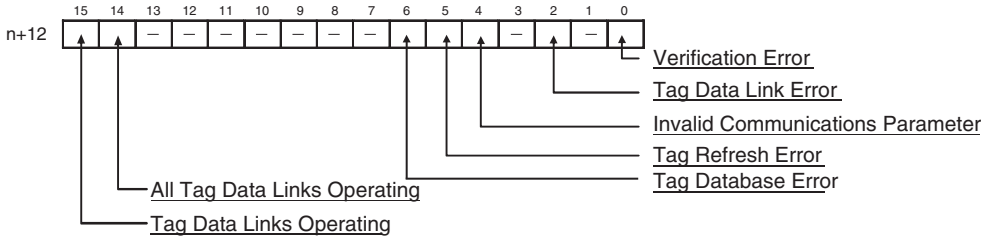
Bit	Name	Status	Manipulated by	Unit operation
1	Tag Data Link Operating	ON	Unit	Indicates that the tag data link is operating. Turned OFF when communications stop in the following cases. • Hardware error • IP Address Duplication Error • BOOTP Server Error • Basic Ethernet Setting Error • Memory Error (MAC Address Error)
		OFF	Unit	Indicates that the tag data link is stopped. Turned ON in the following cases. • The Unit is set as the originator and the power supply was turned ON or the Unit was restarted. • The Unit is set as the originator and the Tag Data Link Start Bit was turned ON.
2	Operating IP Address Change	ON	Unit	ON if the node address setting is different from the setting when the power was turned ON.
		OFF	Unit	OFF if the node address setting is the same as the setting when the power was turned ON.
3 to 9	(Not used)	---	---	---
10	User Authentication Setting Error (See note 1.)	ON	Unit	Indicates that a checksum error occurred in the user authentication settings.
		OFF	Unit	Indicates that the user authentication settings are normal.
11	User Setting Area Enabled	ON	Unit	Indicates that the user settings area data is enabled. ON when “user settings” have been specified as the layout of the allocated CIO Area, and refreshing of the user settings area has started.
		OFF	Unit	Indicates that the user settings area data is invalid. The bit is turned OFF in the following cases, because communications stop. • The allocated CIO Area layout is set to default settings. • The allocated CIO Area layout is set to user settings, but one of the following problems occurred. • A Layout Setting Error occurred.
12 to 13	(Reserved)	---	---	---

Bit	Name	Status	Manipulated by	Unit operation
14	Multiple Switches ON Error	ON	Unit	ON when two or more control bits are ON simultaneously. (Unused bits are ignored.)
		OFF	Unit	Turned OFF when the next control bit operation starts.
15	Error Log Stored	ON	Unit	Indicates that an error record is registered in the error log.
		OFF	Unit	Indicates that no error records are registered in the error log. Also turned OFF when an error log clear request is received.

Note (1) This is a status that exists in the CS1W/CJ1W-EIP21S or CJ3M-CPU3□ only.

Communications Status 1 (EtherNet/IP Unit to CPU Unit) (n + 12)

Word n+12 contains status flags related to the tag data links, as shown in the following diagram.



Bit	Name	Status	Manipulated by	Unit operation
0	Verification Error	ON	Unit	Indicates that the information registered for a target node in the tag data link parameters is different from the actual node information. Main causes: • The specified target does not exist. *1 • The variable name does not match. • The connection size is different. • Connection resources are insufficient.
		OFF	Unit	Indicates that a verification error has not occurred. Also turned OFF when a verification error is cleared.
1	(Not used)	---	---	---

Bit	Name	Status	Manipulated by	Unit operation
2	Tag Data Link Error	ON	Unit	Indicates that there were two or more errors in a connection as an originator. This status does not indicate the following errors. • Connection as a target • Connection timeout due to a Link OFF Error with the switching hub
		OFF	Unit	Indicates that the errors listed above did not occur.
3	(Not used)	---	---	---
4	Invalid Communications Parameter	ON	Unit	ON when there was an error in the validation check of tag data link parameters stored in the Unit's non-volatile memory, and a checksum error occurred. (Includes parameters related to basic Ethernet settings.) The tag data links will stop.
		OFF	Unit	OFF when the validation check of parameters in non-volatile memory was normal.
5	Tag Refresh Error	ON	Unit	ON when a specified data area or address range is not supported in tag data links.
		OFF	Unit	OFF when the specified data areas and addresses are supported in tag data links.
6	Tag Database Error	ON	Unit	ON if a tag database error occurs in the CPU Unit when a symbol name is used incorrectly in a setting for the EtherNet/IP Unit or built-in EtherNet/IP port (tag data link, status area allocations setting, etc.). *2
		OFF	Unit	OFF when a symbol name is not used in a setting for the EtherNet/IP Unit or built-in EtherNet/IP port, when a tag database error has not occurred, or when a previous error has been cleared.
7 to 13	(Not used)	---	---	---
14	All Tag Data Links Operating	ON	Unit	Indicates that tag data links are communicating in all connections as the originator.
		OFF	Unit	Indicates that a tag data link failed in one or more connections as the originator. (OFF even if some tag data links are communicating.)

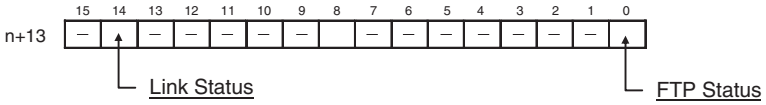
Bit	Name	Status	Manipulated by	Unit operation
15	Tag Data Links Operating	ON	Unit	Indicates that tag data links are communicating in one or more connections as the originator.
		OFF	Unit	Indicates that not even one tag data link is communicating in connections as the originator. (OFF even if the Unit is communicating as a target.)

*1 This error will not occur if the d5 error (verification error, target nonexistent) mask is enabled.

*2 This function is supported by the CJ2 CPU Units of CJ2H-CPU6□(-EIP) with unit version 1.6 or later, and CJ2M-CPU□□ with unit version 2.2 or later.

Communications Status 2 (EtherNet/IP Unit to CPU Unit) (n + 13)

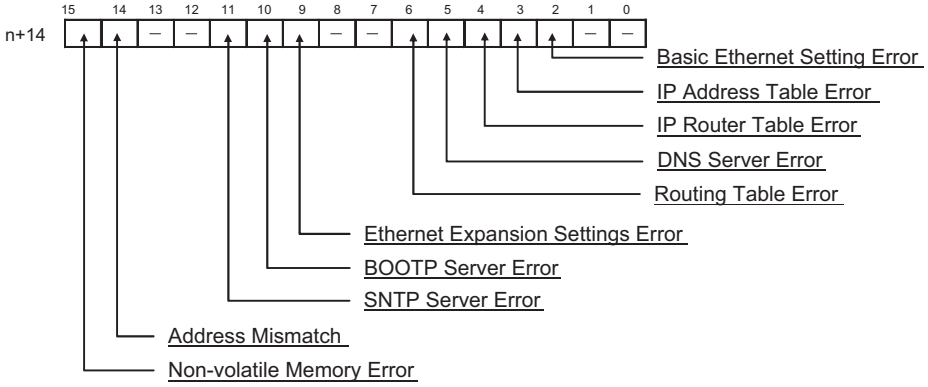
Word n+13 contains status flags related to the Ethernet, as shown in the following diagram.



Bit	Name	Status	Manipulated by	Unit operation
0	FTP Status	ON	Unit	ON when the FTP server is operating (i.e., when there is an FTP client connection).
		OFF	Unit	OFF when the FTP is on standby (i.e., waiting for a client connection).
1 to 13	(Not used)	---	---	---
14	Link Status	ON	Unit	ON when a link is established with the switching hub.
		OFF	Unit	OFF when the link with the switching hub is stopped.
15	(Not used)	---	---	---

Communications Status 3 (EtherNet/IP Unit to CPU Unit) (n + 14)

Word n+14 contains status flags related to the Ethernet errors, as shown in the following diagram.



Bit	Name	Status	Manipulated by	Unit operation
0 to 1	(Not used)	---	---	---
2	Basic Ethernet Setting Error	ON	Unit	One of the following parameters is invalid. • TCP/IP Configuration settings (IP address, subnet mask, or Link settings)
		OFF	Unit	OFF when the parameters above are valid.
3	IP Address Table Error	ON	Unit	ON when the IP address table information is incorrect.
		OFF	Unit	OFF when the IP address table information is correct.
4	IP Router Table Error	ON	Unit	ON when the IP router table information is incorrect.
		OFF	Unit	OFF when the IP router table information is correct.
5	DNS Server Error	ON	Unit	One of the following errors occurred when using the DNS server. • An illegal server IP address is set. • A communications timeout occurred with the server.
		OFF	Unit	OFF when the IP router table information is correct.
6	Routing Table Error	ON	Unit	ON when the routing table information is incorrect.
		OFF	Unit	OFF when the routing table information is correct.
7 to 8	(Not used)	---	---	---
9	Ethernet Expansion Settings Error	ON	Unit	One of the following parameters is invalid. • FINS settings
		OFF	Unit	OFF when the parameters above are valid.

Bit	Name	Status	Manipulated by	Unit operation
10	BOOTP Server Error	ON	Unit	One of the following errors occurred when using the BOOTP server. • The IP address received from the BOOTP server is incorrect. • A communications timeout occurred with the server.
		OFF	Unit	OFF when the errors listed above did not occur.
11	SNTP Server Error	ON	Unit	One of the following errors occurred when using the SNTP server. • An illegal server IP address or host name is set. • A communications timeout occurred with the server.
		OFF	Unit	OFF when the errors listed above did not occur.
12 to 13	(Not used)	---	---	---
14	Address Mismatch	ON	Unit	ON when the target IP address conversion method is set to *Automatic generation*, but the local IP address' host ID does not match the FINS node address.
		OFF	Unit	OFF when the values match.
15	Non-volatile Memory Error	ON	Unit	ON when an error occurred in the Unit's internal non-volatile memory.
		OFF	Unit	OFF when the Unit's internal non-volatile memory is operating normally.

Registered Target Node Table (EtherNet/IP Unit to CPU Unit) (n + 16 to n + 19)

Words n+16 to n+19 show the registration status of the target nodes that are connected with the EtherNet/IP Unit as the originator.

These words show the status of nodes 0 to 63 only. If it is necessary to show the status of nodes higher than node 63, select "user settings" as the layout pattern. For details, refer to *4-4 User Settings Area*.

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
n+16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
n+17	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
n+18	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32
n+19	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48

Bit	Name	Status	Manipulated by	Unit operation
---	Registered Target Node Flags	ON	Unit	Indicates that the node's tag data link is registered.
		OFF	Unit	Indicates that the node's tag data link is not registered.

Normal Target Node Table (EtherNet/IP Unit to CPU Unit) (n+20 to n+23)

Words n+20 to n+23 show the connection status of the target nodes that are connected with the EtherNet/IP Unit as the originator. The flag turns ON after all data for multiple connections for individual target devices is refreshed in the CPU Unit.

These words show the status of nodes 0 to 63 only. If it is necessary to show the status of nodes higher than node 63, select “user settings” as the lay-out pattern. For details, refer to *4-4 User Settings Area*.

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
n+20	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
n+21	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
n+22	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32
n+23	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48

Bit	Name	Status	Manipulated by	Unit operation
---	Normal Target Node Flags	ON	Unit	Flags turn ON after all data for multiple connections for the target device is refreshed in the CPU Unit. (See note 1.)
		OFF	Unit	Indicates that the connection is not established

Note (1) With CS1W/CJ1W-EIP21, CJ2H-CPU6□-EIP Rev.1(Unit Ver.1.0), each flag immediately turns ON when all of the connections are established.

FINS/TCP Connection Status (EtherNet/IP Unit to CPU Unit) (n+24)

Word n+24 shows the status of FINS/TCP connections. For details, refer to *SECTION 8 FINS Communications.*

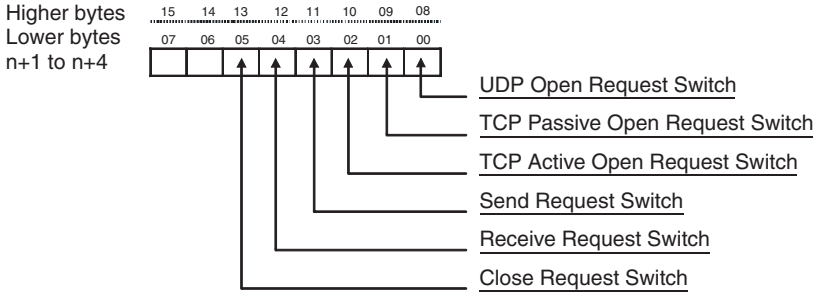
	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
n+24																

Bit	Name	Status	Manipulated by	Unit operation
0	FINS/TCP Connection 1	ON	Unit	Turned ON by the Unit when a connection is established.
		OFF	Unit	Turned OFF by the Unit when the connection is terminated.
1	FINS/TCP Connection 2	ON	Unit	Turned ON by the Unit when a connection is established.
		OFF	Unit	Turned OFF by the Unit when the connection is terminated.
:	:	:	:	:
14	FINS/TCP Connection 15	ON	Unit	Turned ON by the Unit when a connection is established.
		OFF	Unit	Turned OFF by the Unit when the connection is terminated.
15	FINS/TCP Connection 16	ON	Unit	Turned ON by the Unit when a connection is established.
		OFF	Unit	Turned OFF by the Unit when the connection is terminated.

Socket Service Request Switches 1 to 8 (CPU Unit to EtherNet/IP Unit) (n+1 to n+4)

■ **When the layout of the allocated CIO Area words is User defined**

When a socket service request is executed by control bit manipulation, it is the following bits that are manipulated. For details, refer to *SECTION 14 Socket Services*.

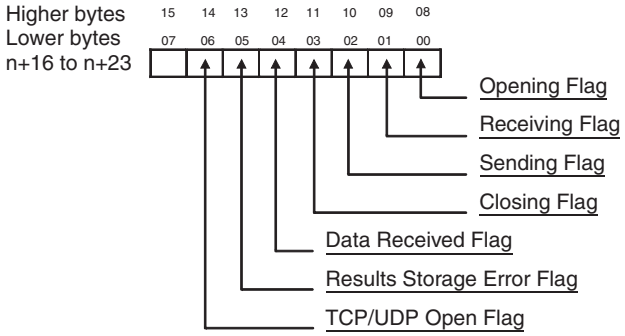


Bit	Switch	Status	Manipulated by	Unit operation	Reference
00/08	UDP Open Request Switch	ON	User	UDP socket opened when switch is turned ON.	*SECTION 14 Socket Services*
		OFF	Unit	Unit turns OFF switch when open processing has been completed (i.e., when a connection has been made).	
01/09	TCP Passive Open Request Switch	ON	User	Passive TCP socket opened when switch is turned ON.	
		OFF	Unit	Unit turns OFF switch when open processing has been completed (i.e., when a connection has been made).	
02/10	TCP Active Open Request Switch	ON	User	Active TCP socket opened when switch is turned ON.	
		OFF	Unit	Unit turns OFF switch when open processing has been completed (i.e., when a connection has been made).	
03/11	Send Request Switch	ON	User	Send processing executed when switch is turned ON. (The protocol (TCP/UDP) is determined when the socket is opened.)	
		OFF	Unit	Unit turns OFF switch when send processing has been completed.	
04/12	Receive Request Switch	ON	User	Receive processing executed when switch is turned ON. (The protocol (TCP/UDP) is determined when the socket is opened.)	
		OFF	Unit	Unit turns OFF switch when receive processing has been completed.	
05/13	Close Request Switch	ON	User	Close processing executed when switch is turned ON. (The protocol (TCP/UDP) is determined when the socket is opened.)	
		OFF	Unit	Unit turns OFF switch when close processing has been completed.	
06/14	(Not used.)	---	---	---	---
07/15	(Not used.)	---	---	---	---

Note These are enabled for CS1W/CJ1W-EIP21S or CJ3M-CPU3□ only.

Status of UDP/TCP Sockets 1 to 8 (EtherNet/IP Unit to CPU Unit) (n+16 to n+23)

■ **When the layout of the allocated CIO Area words is User defined**



Bit	Flag	Status	Manipulated by	Unit operation	Reference
00/08	Opening Flag	ON	Unit	ON during open processing. (Turns ON when open request is received.)	*SECTION 14 Socket Services*
		OFF	Unit	OFF when open processing has been completed.	
01/09	Receiving Flag	ON	Unit	ON during receive processing. (Turns ON when receive request is received if high-speed option is disabled and remains OFF when high-speed processing is enabled.)	
		OFF	Unit	OFF when receive processing has been completed.	
02/10	Sending Flag	ON	Unit	ON during send processing. (Turns ON when send request is received if high-speed option is disabled and remains OFF when high-speed processing is enabled.)	
		OFF	Unit	OFF when send processing has been completed.	
03/11	Closing Flag	ON	Unit	ON during close processing. (Turns ON when close request is received.)	
		OFF	Unit	OFF when close processing has been completed.	
04/12	Data Received Flag	ON	Unit	ON when data from a remote node has been received at an open TCP socket.	
		OFF	Unit	OFF when receive processing has been requested for an open TCP socket.	
05/13	Results Storage Error Flag	ON	Unit	ON if there is an error in storing the results when socket services are used by means of the CMND instruction. (Turns ON when either bits 0 to 3 or bits 8 to 11 complete changing from ON to OFF.)	
		OFF	Unit	Turns OFF when the next request is received. (Connected by TCP.)	
06/14	TCP/UDP Open Flag	ON	Unit	ON when open processing has been completed.	
		OFF	Unit	OFF when close processing has been completed. (Stays OFF for abnormal open processing completion.)	
07/15	(Not used.)	---	---	---	---

Note These are enabled for CS1W/CJ1W-EIP21S or CJ3M-CPU3□ only.

Opening Flag (Bit 00 or 08)

Turns ON when an open request is received either by control bit manipulation or the CMND/CMND2 instruction, and turns OFF again when the open processing has been completed. When CMND/CMND2 is used, the Results Storage Error Flag (bit 05 or 13) will turn ON at the same time as the Opening Flag turns OFF if there is an error in the Results Storage Area designation.

Receiving Flag (Bit 01 or 09)

Turns ON if the High-Speed Option is not selected when a receive request is received either by control bit manipulation or the CMND/CMND2 instruction. Remains OFF if the High-Speed Option is selected. Turns OFF again when the receive processing has been completed. When CMND/CMND2 is used, the Results Storage Error Flag (bit 05 or 13) will turn ON at the same time as the Receiving Flag turns OFF if there is an error in the Results Storage Area designation.

Sending Flag (Bit 02 or 10)

Turns ON if the High-Speed Option is not selected when a send request is received either by control bit manipulation or the CMND/CMND2 instruction and turns OFF again when the send processing has been completed. Remains OFF if the High-Speed Option is selected. When CMND/CMND2 is used, the Results Storage Error Flag (bit 05 or 13) will turn ON at the same time as the Sending Flag turns OFF if there is an error in the Results Storage Area designation.

Closing Flag (Bit 03 or 11)

Turns ON when a close request is received either by control bit manipulation or the CMND/CMND2 instruction, and turns OFF again when the close processing has been completed. When CMND/CMND2 is used, the Results Storage Error Flag (bit 05 or 13) will turn ON at the same time as the Closing Flag turns OFF if there is an error in the Results Storage Area designation.

Data Received Flag (Bit 04 or 12)

This bit turns ON when data is received from a remote node at an open TCP socket. Linked to this flag, the number of bytes of data saved in the reception buffer is stored in Number of Bytes Received at TCP Socket in the words allocated in the DM Area. The bit is turned OFF when a receive request is made by either bit manipulation or the CMND/CMND2 instruction. If any data remains in the reception buffer after the receive request processing is complete, the number of bytes is stored in Number of Bytes Received at TCP Socket and the Data Received Flag turns ON again.

The status of this flag is checked before a receive request is executed.

Results Storage Error Flag (Bit 05 or 13)

Turns ON if there is an error in the Results Storage Area for a socket service request (open, receive, send, close) made using CMND/CMND2. This flag turns ON at the same time as the services request processing flags (bits 00 to 03 or 08 to 11) turn OFF. It remains ON until the next services request is received, and then it turns OFF again. When this flag turns ON, check the set values in the Results Storage Area.

The Results Storage Error Flag does not operate when socket services are requested by control bit manipulation.

TCP/UDP Open Flag (Bit 06 or 14)

Remains ON while a socket is open by means of control bit manipulation or the CMND/CMND2 instruction. In the case of TCP, it indicates a connection. When the socket is closed, this flag turns OFF again. (If the socket did not close properly, the flag remains ON.)

Check to be sure that this flag is ON before executing a send or receive request.

4-3 DM Area Allocations

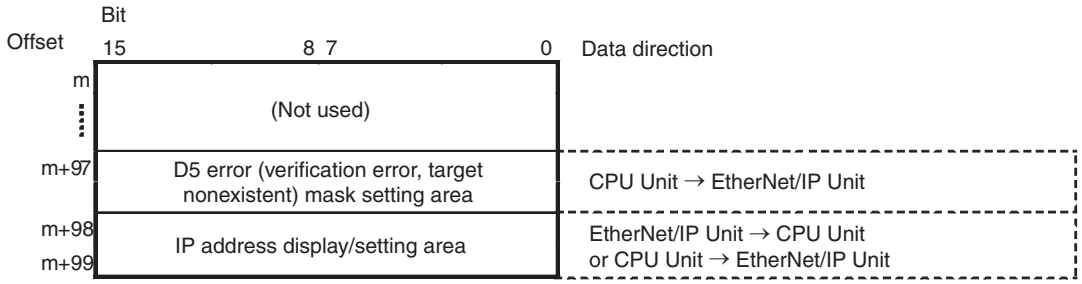
4-3-1 Overview of the Allocated DM Area Words

The various kinds of data are stored in the offset positions shown in the following diagram, from the beginning word in the area for each Unit.

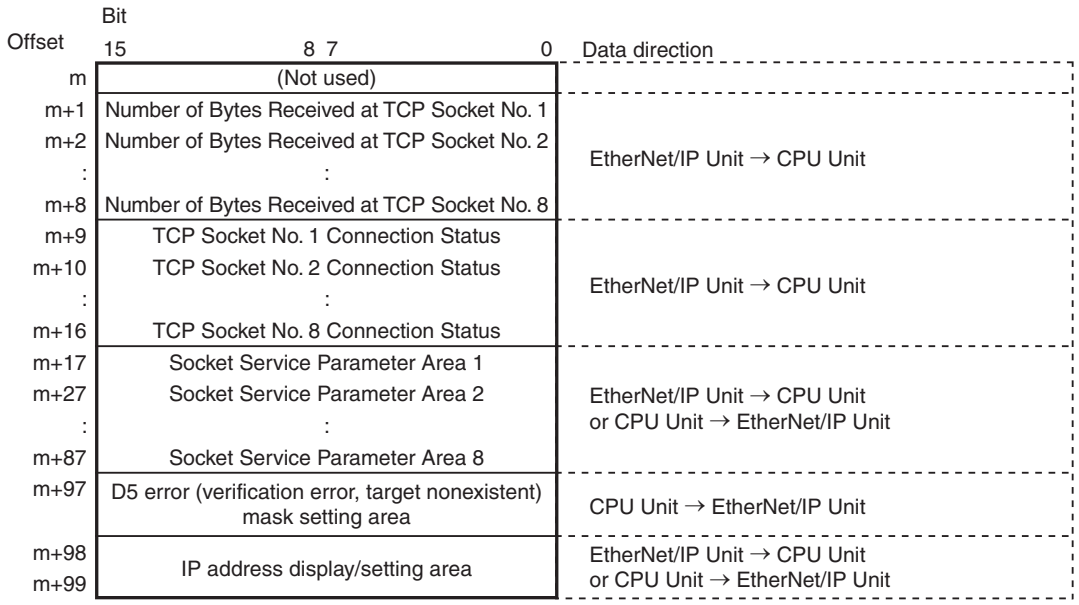
The beginning word m is calculated by the following equation:

Beginning word m = D30000 + (100 x unit number)

■ **CS1W/CJ1W-EIP21, CJ2H-CPU6□-EIP, or CJ2M-CPU3□**



■ **CS1W/CJ1W-EIP21S or CJ3M-CPU3□**



4-3-2 Details of the Allocated DM Area Words

D5 Error (Verification Error, Target Nonexistent) Mask Setting Area

If d5d5 was set in the d5 error (verification error, target nonexistent) mask setting area, the EtherNet/IP Unit will read this area when the power supply is turned ON or the Unit is restarted and enable the d5 error (verification error, target nonexistent) mask. If the d5 error (verification error, target nonexistent) mask is enabled, error notification is not provided even if a verification error (target nonexistent) occurs. Make this setting when the status is to be considered normal even when the target is nonexistant. If you enable this function, the right dot on the hexadecimal display of the lower 8 bits of the IP address on the 7-segment display will light.

Note For EtherNet/IP Units or built-in EtherNet/IP ports that are manufactured in January 2014 or later, you can use a d5 error (verification error, target nonexistent) mask.

IP Address Display/Setting Area (m+98 and m+99)

	15 14 13 12	11 10 9 8	7 6 5 4	3 2 1 0
m+98	(1)	(2)	(3)	(4)
m+99	(5)	(6)	(7)	(8)

(1)(2).(3)(4).(5)(6).(7)(8) (Hex)

IP address: (1)(2).(3)(4).(5)(6).(7)(8) (Hex)

If the local IP address is set to a value other than 0.0.0.0 in the TCP/IP Configuration, this area (words m+98 and m+99) will act as an IP Address Display Area and the local IP address set in the TCP/IP Configuration will be read and stored here when the power is turned ON or the Unit restarted.

If the local IP address in the TCP/IP Configuration is set to 0.0.0.0, this value is read by the EtherNet/IP Unit when the power is turned ON or the Unit restarted and is used as the local IP address.

If the local IP address in these words and the TCP/IP Configuration are both set to 0.0.0.0, the default IP address (192.168.250.Node_address) will be used. For details on the IP address settings, refer to *SECTION 5 Determining IP Addresses*.

Application	Setting device	Setting area	Remarks
Simple operation (i.e., The TCP/IP Configuration is left at its default settings. Only the IP address is set.)	Programming Console (CX-Programmer can also be used.)	Allocated words in the DM Area	• The setting in the allocated DM Area words is enabled only when the IP address is set to 0.0.0.0 in the TCP/IP Configuration. • If the IP address is set to a value other than 00.00.00.00 in the TCP/IP Configuration, this value is stored in the allocated words in the DM Area.
Operation with the desired IP address set in the TCP/IP Configuration.	CX-Programmer (Unit Setup)	Setup TCP/IP Configuration Dialog Box	The IP address set in the Setup TCP/IP Configuration Dialog Box is stored in the allocated DM Area words.

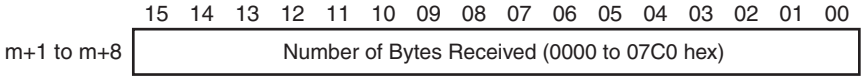
Note

(1) If an IP address other than 00.00.00.00 is set as the local IP address in the TCP/IP Configuration, the IP Address Display/Setting Area words (m+98 and m+99) will be overwritten with the TCP/IP Configuration's IP address, even if a non-zero IP address was set in the IP Address Display/Setting Area words beforehand.

(2) It is not possible to set the following IP addresses. If any of these values are set, the ERH indicator will flash.

- IP addresses where all network number bits are 0 or 1.
- IP addresses where all host number bits are 0 or 1.
- IP addresses where all subnet number bits are 1.
- IP addresses that start with 127 (7F hexadecimal, e.g., 127.35.21.16).

TCP Socket No. (1 to 8): Number of Bytes Received (EtherNet/IP Unit to CPU Unit)



For each TCP socket, the number of bytes of data in the reception buffer is stored in one word. A maximum of 4,096 bytes of data can be held in the reception buffer, but a value of only up to the maximum value (1,984 bytes) that can be set for receive requests by manipulating control bits or using CMND is stored.

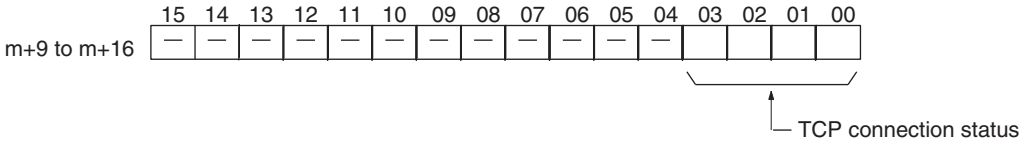
0000 hex: 0 bytes

07C0 hex: 1,984 bytes

The Data Received Flag in the CIO Area turns ON and OFF linked to this word. This area is given a value of 0000 hex when a receive request is executed by manipulating control bits or using the CMND instruction. If any data remains in the reception buffer after the receive request processing is completed, the remaining number of bytes is stored and the Data Received Flag turns ON again.

Before a receive request is executed, a check is performed to confirm that the required data is available.

TCP Socket No. (1 to 8): Connection Status (EtherNet/IP Unit to CPU Unit)



This is enabled for CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ only.

The connection status for each TCP socket is stored by code in this word. For details, refer to *Appendix C TCP Status Transitions*.

Socket Service Parameter Area 1 to 8 (EtherNet/IP Unit to CPU Unit)

Offset	Socket No. 1	...	Socket No. 8	15 14 13 12 11 10 09 08 07 06 05 04 03 02 01 00
+0	m+17	···	m+87	Socket option / UDP/TCP socket number (1 to 8)
+1	m+18		m+88	Local UDP/TCP port number (0000 to FFFF Hex)
+2	m+19		m+89	Remote IP address (00000000 to FFFFFFFF Hex)
	m+20		m+90	
+4	m+21	···	m+91	Remote UDP/TCP port number (0000 to FFFF Hex)
+5	m+22		m+92	Number of send/receive bytes (0000 to 07C0 Hex (1984))
+6	m+23		m+93	Send/receive data address (Same as FINS variable area designation method.)
	m+24		m+94	
+8	m+25		m+95	Timeout value (0000 to FFFF Hex)
+9	m+26	···	m+96	Response code

This is enabled for CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ only.

When socket services are requested by control bit manipulation, the settings must be made in advance in a Socket Service Parameter Area. The parameters used will vary depending on the service requested. For details, refer to *SECTION 14 Socket Services*.

4-4 User Settings Area

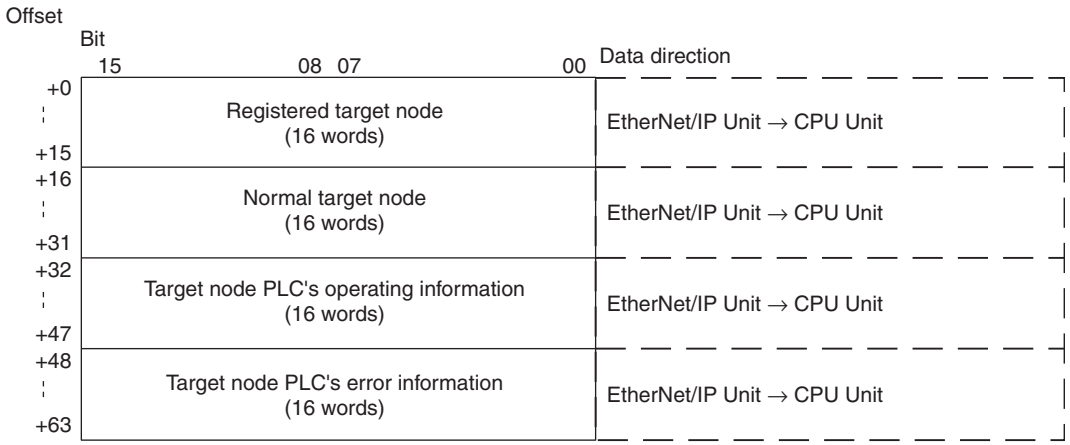
4-4-1 Overview of the User Settings Area

When the layout of the allocated CIO Area words is set to user settings, the user settings area can be used in addition to the allocated CIO Area words and allocated DM Area words.

The beginning word of the user settings area can be set in the Status Area Tab Page in the Edit Parameters Dialog Box of the CX-Programmer.

4-4-2 User Settings Area

The user can allocate any available area to contain the registered target node information, normal target node information, target node PLC operating information, and target node PLC error information.



Registered Target Node Table (EtherNet/IP Unit to CPU Unit)

These flags indicate the registration status of the target nodes, and are valid only when the EtherNet/IP Unit is the originator of the connection. For details on the default settings, refer to *4-2-2 Details of the Allocated CIO Area Words*.

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
+0	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
+1	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
+2	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32
+3	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48
+4	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64
+5	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81	80
+6	111	110	109	108	107	106	105	104	103	102	101	100	99	98	97	96
+7	127	126	125	124	123	122	121	120	119	118	117	116	115	114	113	112
+8	143	142	141	140	139	138	137	136	135	134	133	132	131	130	129	128
+9	159	158	157	156	155	154	153	152	151	150	149	148	147	146	145	144
+10	175	174	173	172	171	170	169	168	167	166	165	164	163	162	161	160
+11	191	190	189	188	187	186	185	184	183	182	181	180	179	178	177	176
+12	207	206	205	204	203	202	201	200	199	198	197	196	195	194	193	192
+13	223	222	221	220	219	218	217	216	215	214	213	212	211	210	209	208
+14	239	238	237	236	235	234	233	232	231	230	229	228	227	226	225	224
+15	255	254	253	252	251	250	249	248	247	246	245	244	243	242	241	240

Bit	Name	Status	Manipulated by	Unit operation
---	Registered Target Node Flags	ON	Unit	Indicates that the node's tag data link is registered.
		OFF	Unit	Indicates that the node's tag data link is not registered.

Normal Target Node Table (EtherNet/IP Unit to CPU Unit)

These flags indicate the connection status of the target nodes. The flag turns ON after all data for multiple connections for individual target devices is refreshed in the CPU Unit. However, with EtherNet/IP Units or built-in EtherNet/IP ports with revision 1 excluding CS1W/CJ1W-EIP21S, each flag immediately turns ON when all of the connections are established.

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
+16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
+17	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
+18	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32
+19	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48
+20	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64
+21	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81	80
+22	111	110	109	108	107	106	105	104	103	102	101	100	99	98	97	96
+23	127	126	125	124	123	122	121	120	119	118	117	116	115	114	113	112
+24	143	142	141	140	139	138	137	136	135	134	133	132	131	130	129	128
+25	159	158	157	156	155	154	153	152	151	150	149	148	147	146	145	144
+26	175	174	173	172	171	170	169	168	167	166	165	164	163	162	161	160
+27	191	190	189	188	187	186	185	184	183	182	181	180	179	178	177	176
+28	207	206	205	204	203	202	201	200	199	198	197	196	195	194	193	192
+29	223	222	221	220	219	218	217	216	215	214	213	212	211	210	209	208
+30	239	238	237	236	235	234	233	232	231	230	229	228	227	226	225	224
+31	255	254	253	252	251	250	249	248	247	246	245	244	243	242	241	240

Bit	Name	Status	Manipulated by	Unit operation
---	Normal Target Node Flags	ON	Unit	Flags turn ON after all data for multiple connections for the target device is refreshed in the CPU Unit. (See note 1.)
		OFF	Unit	Indicates that all connections are not established

Note (1) With CS1W/CJ1W-EIP21 or CJ2H-CPU6□-EIP Rev.1 (Unit version 1.0), each flag immediately turns ON when all of the connections are established.

Target Node PLC Operating Information (EtherNet/IP Unit to CPU Unit)

These flags indicate the operating status of the target node PLCs, and are valid only when the EtherNet/IP Unit is the originator. The flags are valid only when the corresponding Normal Target Node Flag is ON. If the corresponding Normal Target Node Flag is OFF, the Target Node PLC Operating Flag indicates the previous operating status.

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
+32	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
+33	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
+34	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32
+35	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48
+36	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64
+37	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81	80
+38	111	110	109	108	107	106	105	104	103	102	101	100	99	98	97	96
+39	127	126	125	124	123	122	121	120	119	118	117	116	115	114	113	112
+40	143	142	141	140	139	138	137	136	135	134	133	132	131	130	129	128
+41	159	158	157	156	155	154	153	152	151	150	149	148	147	146	145	144
+42	175	174	173	172	171	170	169	168	167	166	165	164	163	162	161	160
+43	191	190	189	188	187	186	185	184	183	182	181	180	179	178	177	176
+44	207	206	205	204	203	202	201	200	199	198	197	196	195	194	193	192
+45	223	222	221	220	219	218	217	216	215	214	213	212	211	210	209	208
+46	239	238	237	236	235	234	233	232	231	230	229	228	227	226	225	224
+47	255	254	253	252	251	250	249	248	247	246	245	244	243	242	241	240

Bit	Name	Status	Manipulated by	Unit operation
---	Target Node PLC Operating Flags	ON	Unit	The corresponding PLC is operating. (The program is being executed.)
		OFF	Unit	The PLC is not operating.

Target Node PLC Error Information (EtherNet/IP Unit to CPU Unit)

These flags indicate the error status (logical OR of fatal and non-fatal errors) of the target node PLCs, and are valid only when the EtherNet/IP Unit is the originator. The flags are valid only when the corresponding Normal Target Node Flag is ON. If the corresponding Normal Target Node Flag is OFF, the Target Node PLC Error Flag indicates the previous error status.

For details on the default settings, refer to *4-2-2 Details of the Allocated CIO Area Words*.

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
+48	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
+49	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
+50	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32
+51	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48
+52	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64
+53	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81	80
+54	111	110	109	108	107	106	105	104	103	102	101	100	99	98	97	96
+55	127	126	125	124	123	122	121	120	119	118	117	116	115	114	113	112
+56	143	142	141	140	139	138	137	136	135	134	133	132	131	130	129	128
+57	159	158	157	156	155	154	153	152	151	150	149	148	147	146	145	144
+58	175	174	173	172	171	170	169	168	167	166	165	164	163	162	161	160
+59	191	190	189	188	187	186	185	184	183	182	181	180	179	178	177	176
+60	207	206	205	204	203	202	201	200	199	198	197	196	195	194	193	192
+61	223	222	221	220	219	218	217	216	215	214	213	212	211	210	209	208
+62	239	238	237	236	235	234	233	232	231	230	229	228	227	226	225	224
+63	255	254	253	252	251	250	249	248	247	246	245	244	243	242	241	240

Bit	Name	Status	Manipulated by	Unit operation
---	Target Node PLC Error Flags	ON	Unit	A fatal or non-fatal error occurred in the corresponding PLC.
		OFF	Unit	No error occurred in the PLC.

4-5 Auxiliary Area Data

The following table and descriptions cover the words and bits in the CPU Unit's Auxiliary Area that are related to the EtherNet/IP Unit.

4-5-1 Read-only Bits/Words

Word(s)	Bit(s)	Name	Function	Settings
A202	A20200 to A20207	Communications Port Enabled Flags	Bits A20200 to A20207 turn ON when a network instruction (SEND, RECV, CMND, or PMCR) can be executed with the corresponding port number. Bits 00 to 07 correspond to communications ports 0 to 7.	0: Network communications running 1: No network communications running
A203 to A210	---	Communications Port Completion Codes	These words contain the completion codes for the corresponding port numbers when network instructions (SEND, RECV, CMND, or PMCR) have been executed. Words A203 to A210 correspond to communications ports 0 to 7.	0000: No error Not 0000: Error code
A219	A21900 to A21907	Communications Port Error Flags	Bits A21900 to A21907 turn ON when an error occurred during execution of a network instruction (SEND, RECV, CMND, or PMCR). Bits 00 to 07 correspond to communications ports 0 to 7.	0: Normal end 1: Error end
A302	A30200 to A30215	CPU Bus Unit Initializing Flags	Bits A30200 through A30215 turn ON while the corresponding CPU Bus Units (Units #0 through #15, respectively) are initializing. The bits will turn ON either when power is turned ON or when a CPU Bus Unit Restart Bit (A50100 to A50115) is turned ON.	0: Not initializing 1: Initializing (System will automatically turn the flag OFF when initialization has been completed.)
A402	A40203	CPU Bus Unit Setting Error Flag (Non-fatal error)	Bit A40203 is turned ON when the CPU Bus Units actually installed differ from the Units registered in the I/O tables. The ERR/ALM indicator on the front of the CPU Unit will flash, but CPU operation will continue. The unit number of the CPU Bus Unit involved is stored in word A427.	0: No setting error 1: Setting error
	A40207	CPU Bus Unit Error Flag (Non-fatal error)	Bit A40207 is turned ON when an error occurs during the transmission of data between the CPU and CPU Bus Units. The ERR/ALM indicator on the front of the CPU Unit will flash, but CPU operation will continue. The Unit where the error occurred will stop. The unit number of the CPU Bus Unit involved is stored in word A422.	0: No unit number error 1: Unit number error
A403	A40300 to A40308	Memory Error Location	When a memory error occurs, the Memory Error Flag (A40115) is turned ON and one of the following flags is turned ON to indicate the memory area where the error occurred. A40300: User program A40304: PLC Setup A40305: Registered I/O Tables A40307: Routing Tables The ERR/ALM indicator on the front of the CPU Unit will light and CPU operation will stop.	0: Normal 1: Error
A410	A41000 to A41015	CPU Bus Unit Number Duplication Flags	The Duplication Error Flag (A40113) and the corresponding flag in A410 will be turned ON when a CPU Bus Unit's unit number has been duplicated. Bits 00 to 15 correspond to unit numbers 0 to F. The ERR/ALM indicator on the front of the CPU Unit will light and CPU operation will stop.	0: No duplication 1: Duplication

Word(s)	Bit(s)	Name	Function	Settings
A417	A41700 to A41715	CPU Bus Unit Error, Unit Number Flags	When an error occurs in a data exchange between the CPU Unit and a CPU Bus Unit, the CPU Bus Unit Error Flag (A40207) and the corresponding flag in A417 are turned ON. Bits 00 to 15 correspond to unit numbers 0 to F. The ERR/ALM indicator on the front of the CPU Unit will flash, but CPU operation will continue.	0: No error 1: Error
A427	A42700 to A42715	CPU Bus Unit Setting Error, Unit Number Flags	When a CPU Bus Unit Setting Error occurs, A40203 and the corresponding flag in A27 are turned ON. Bits 00 to 15 correspond to unit numbers 0 to F. The ERR/ALM indicator on the front of the CPU Unit will flash, but CPU operation will continue.	0: No setting error 1: Setting error

4-5-2 Read/Write Bits

Word	Bits	Name	Description	Settings
A501	A50100 to A50115	CPU Bus Unit Restart Bits	Bits A50100 through A50115 can be turned ON to reset CPU Bus Units number #0 through #15, respectively. **Note** The CPU Bus Unit Initializing Flags (A30200 to A30215) will turn ON when initialization of the Units begins and turn OFF when it is completed. **Note** When turning ON the CPU Bus Unit Restart Bit from a ladder program, use the SET instruction.	OFF to ON: Unit restarted. Automatically turned OFF by system after restart processing has been completed.

SECTION 5
Determining IP Addresses

This section explains how to manage and use IP addresses.

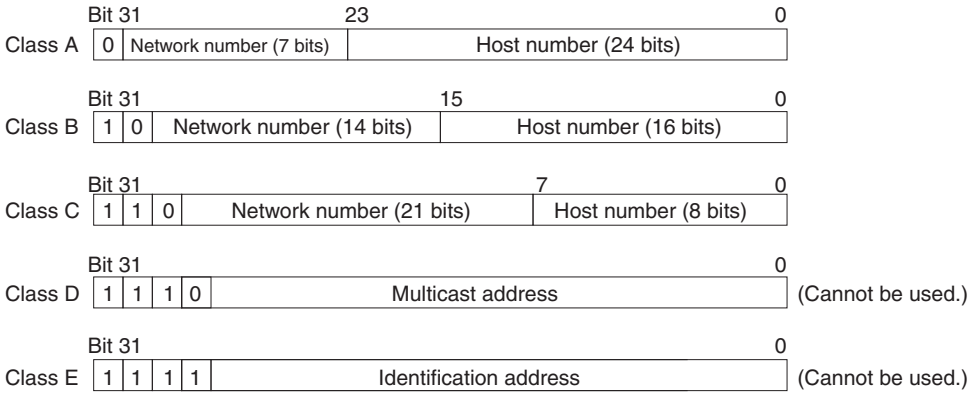
5-1 IP Addresses 124
5-1-1 IP Address Configuration 124
5-1-2 Allocating IP Addresses 124
5-1-3 EtherNet/IP Unit IP Address Settings 125
5-1-4 Subnet Masks 125
5-1-5 CIDR 126
5-2 IP Addresses in FINS Communications 126
5-2-1 Specifying Nodes in FINS Communications Services. 126
5-2-2 Pairing Addresses in Internal Tables 128
5-2-3 Application Examples 134
5-2-4 Related Products and Communications/Setting Methods. . . . 135
5-2-5 Pairing IP Addresses and FINS Node Addresses 137
5-3 Private and Global Addresses 138
5-3-1 Private and Global Addresses. 138
5-3-2 Using a Private Address for the EtherNet/IP Unit 139
5-3-3 EtherNet/IP Unit with a Global Address 141

5-1 IP Addresses

5-1-1 IP Address Configuration

IP addresses are made up of 32 bits of binary data divided into four 8-bit fields called octets. These four octets provide the network number (net ID) and host number (host ID). The network number identifies the network, and the host number identifies the node (or host) on the network.

The network numbers in an IP address are divided into three classes, A, B, and C, so that the address system can be selected according to the scale of the network. (Classes D and E are not used.) The configuration of the IP address for each of these classes is shown in the following diagram.



The number of networks in each class and the number of nodes possible on the network differ according to the class.

Class	Number of networks	Number of hosts
Class A	Small	2^{24}–2 max. (16,777,214 max.)
Class B	Medium	2^{16}–2 max. (65,534 max.)
Class C	Large	2^{8}–2 max. (254 max.)

The 32 bits of an IP address are divided into four sections of eight bits each, and expressed as a punctuated number. IP addresses are represented by the decimal equivalent of each of the four octets in the 32-bit address, each separated by a period. For example, the binary address 10000010 00111010 00010001 00100000 would be represented as 130.58.17.32.

Note The same network number must be set for every node on the same Ethernet network.

5-1-2 Allocating IP Addresses

IP (Internet Protocol) is a standard communications protocol used throughout the world.

5-1-3 EtherNet/IP Unit IP Address Settings

An IP address must be set even for the EtherNet/IP Unit or built-in EtherNet/IP port before Ethernet communications can proceed. Use one of the following methods to set the IP address of the EtherNet/IP Unit or built-in EtherNet/IP port. Either use the default IP address setting, use a Programming Device to set a particular IP address in the DM Area words (CS/CJ Series only) allocated to the Unit as a CPU Bus Unit, or set a particular IP address in the EtherNet/IP Unit or built-in EtherNet/IP port.

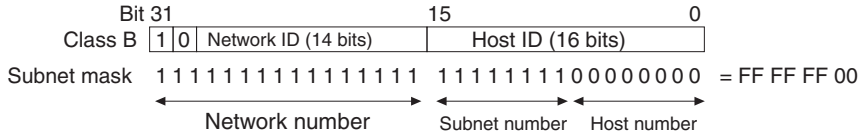
- If you want to connect the EtherNet/IP Unit or built-in EtherNet/IP port immediately, the default IP address is 192.168.250.Node_address. (The node address is set with the Node Address Setting Switches on the front of the EtherNet/IP Unit or CPU Unit.)
- If you want to set a particular IP address and store that local IP address in the CPU Unit, set it with the CPU Unit's allocated DM Area words (CS/CJ Series only).
- If you want to set a particular IP address and store that local IP address in the EtherNet/IP Unit or CPU Unit, set the IP address in the TCP/IP settings of the Unit Setup from the CX-Programmer.
- If you want to set a particular IP address and obtain the IP address automatically from the BOOTP server, TCP/IP settings of the Unit Setup from the CX-Programmer. For details, refer to *3-8 TCP/IP and Link Settings*.

5-1-4 Subnet Masks

Operation and management of a network can become very difficult if too many nodes are connected on a single network. In such a case it can be helpful to configure the system so that a single network is divided up into several subnetworks. This can be done by using part of the host number as a subnet number. Internally the network can be treated as a number of subnetworks, but from the outside it acts as a single network and uses only a single Network ID.

To establish subnetworks, the Host ID in the IP address is divided into a Subnet ID and a Host ID by using a setting called the Subnet Mask. The Subnet Mask indicates which part of the Host ID is to be used as the Subnet ID. All bits in the Subnet Mask that correspond to the bits in the IP address used either as the Network ID or Subnet ID are set to "1," and the remaining bits, which correspond to the bits in the IP address actually used for the Host ID, are set to "0."

The following example shows the Subnet Mask for an 8-bit Subnet ID used in a class-B IP address.



Set the same Subnet Mask value for all of the nodes on that subnetwork. If no subnetworks are used, there is no need to set Subnet Masks. In that case, the following Subnet Mask values will be used depending on the IP address class.

Class	Subnet Mask value
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

5-1-5 CIDR

CIDR, or classless interdomain routing, is used to assign IP addresses that do not use classes. IP addresses that use classes are separated into blocks according to net IDs and host IDs, resulting in inefficient usage of IP address space.

CIDR does not use classes, so IP address space can be divided as required to more efficiently use IP address space. For example, using a subnet mask setting with CIDR enables building a horizontally distributed network exceeding 254 nodes even if a class C address block (e.g., 192, 168...).

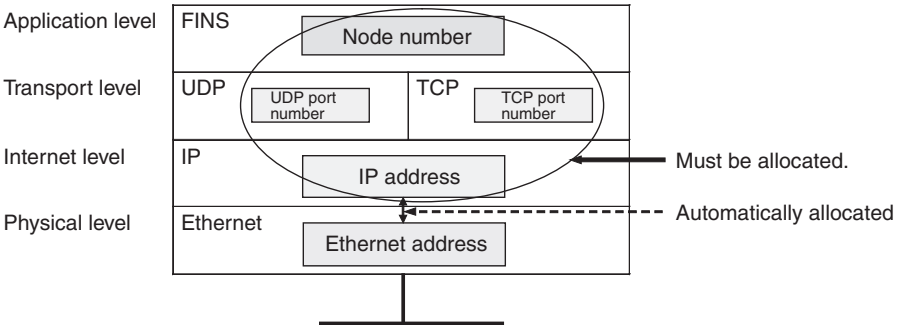
Subnet mask range
192.0.0.0 to 255.255.255.252

Note The CIDR is not supported by the CS1W/CJ1W-EIP21 and CJ2H-CPU6□-EIP (Unit version 1.0).

5-2 IP Addresses in FINS Communications

5-2-1 Specifying Nodes in FINS Communications Services

With FINS communications services on an Ethernet network, IP addresses, UDP port numbers, and TCP port numbers are paired with FINS node addresses to specify nodes on the network.

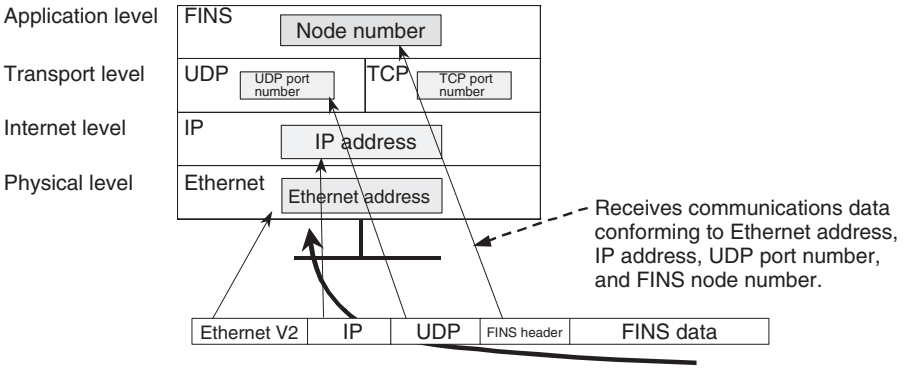


Note Use the Node Address Setting Switches (NODE NO.) on the front of the EtherNet/IP Unit or, for the built-in EtherNet/IP port, on the front of the CPU Unit to set the FINS node address.

Allocating Addresses to EtherNet/IP Units and Built-in EtherNet/IP Ports

FINS Message Reception for EtherNet/IP Units or Built-in EtherNet/IP Ports

The IP address, FINS/UDP port number, and FINS/TCP port number set for the EtherNet/IP Unit or built-in EtherNet/IP port are mainly used when receiving FINS communications messages.



- Ethernet address:A fixed number is assigned to each EtherNet/IP Unit or built-in EtherNet/IP port and it cannot be changed.
- IP address:Use the default IP address (192.168.250.*FINS_node number*), set the address in the allocated DM Area words, or set the address on the TCP/IP Tab Page of the Edit Parameters Dialog Box from the CX-Programmer.
- FINS/UDP port No.:Use the default FINS/UDP port number (9600) or set the number on the FINS/UDP Tab Page of the Edit Parameters Dialog Box from the CX-Programmer.
- FINS/TCP port No.:Use the default FINS/TCP port number (9600) or set the number on the FINS/UDP Tab Page of the Edit Parameters Dialog Box from the CX-Programmer.
- FINS node address:Set the number using the Node Address Setting Switches (NODE NO.) on the front of the EtherNet/IP Unit or built-in EtherNet/IP port.

Pairing IP Addresses with FINS Node Addresses at Local Nodes

A particular IP address is allocated to each communications node, including EtherNet/IP Units and built-in EtherNet/IP ports. The IP address must be paired with the FINS node address (1 to 254) by one of the following methods.

■ Automatic Generation Method (Dynamic/Static)

Set the relationship between the IP address and the FINS node address setting in the EtherNet/IP Unit or built-in EtherNet/IP port according to the following equation. If the setting does not conform to this equation, a setting error will be generated and the MS Indicator will flash red.

FINS node address = IP address host number

■ IP Address Table Method and Combined Method

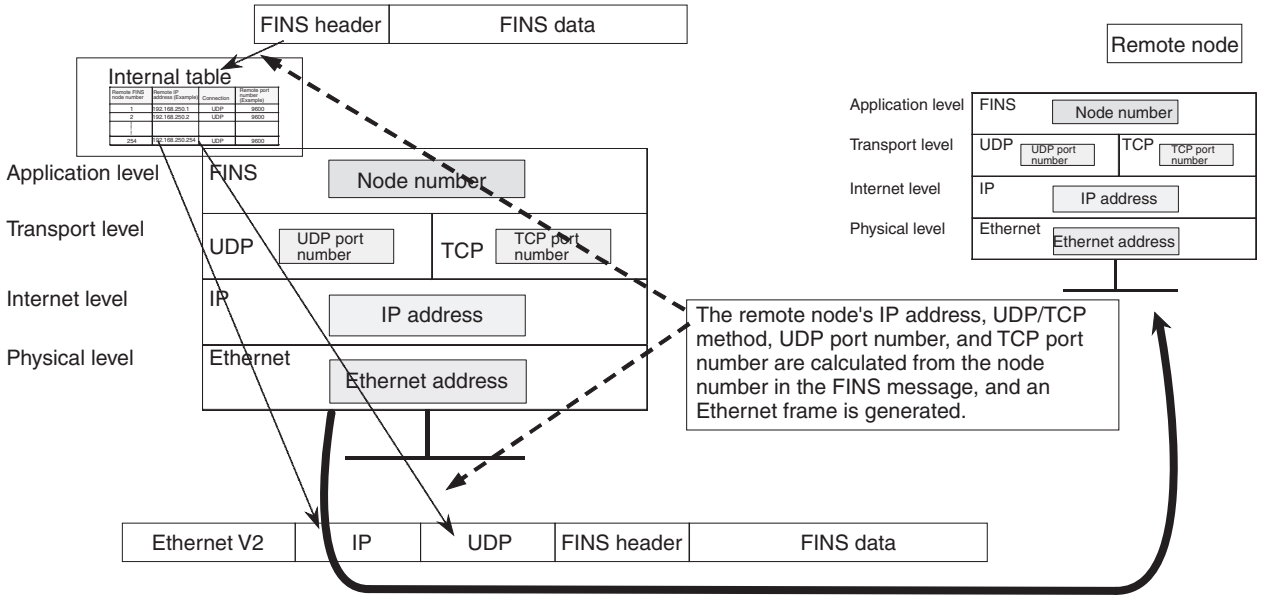
With these methods, the IP address and the FINS node address setting in the EtherNet/IP Unit or built-in EtherNet/IP port have no particular relationship. Set both the FINS node address and the IP address so that they are not duplicated in the network.

Sending FINS Messages from EtherNet/IP Units or Built-in EtherNet/IP Ports

When the EtherNet/IP Unit or built-in EtherNet/IP port sends a FINS message, it is necessary to determine the remote node's IP address, UDP port number, and TCP port number. The relationships between all addresses, such as remote FINS node addresses and IP addresses, are managed by an internal table at the EtherNet/IP Unit or built-in EtherNet/IP port.

Remote FINS node address	Remote IP address (Example)	Connection	Remote port number (Example)
1	192.168.250.1	UDP	9600
2	192.168.250.2	UDP	9600
to			
254	192.168.250.254	UDP	9600

When the EtherNet/IP Unit or built-in EtherNet/IP port is turned ON or restarted, the internal table is generated automatically from the various settings that have been made. Depending on the setting method used, data such as remote IP addresses may be changed dynamically. (Dynamic changes can be prohibited.)



5-2-2 Pairing Addresses in Internal Tables

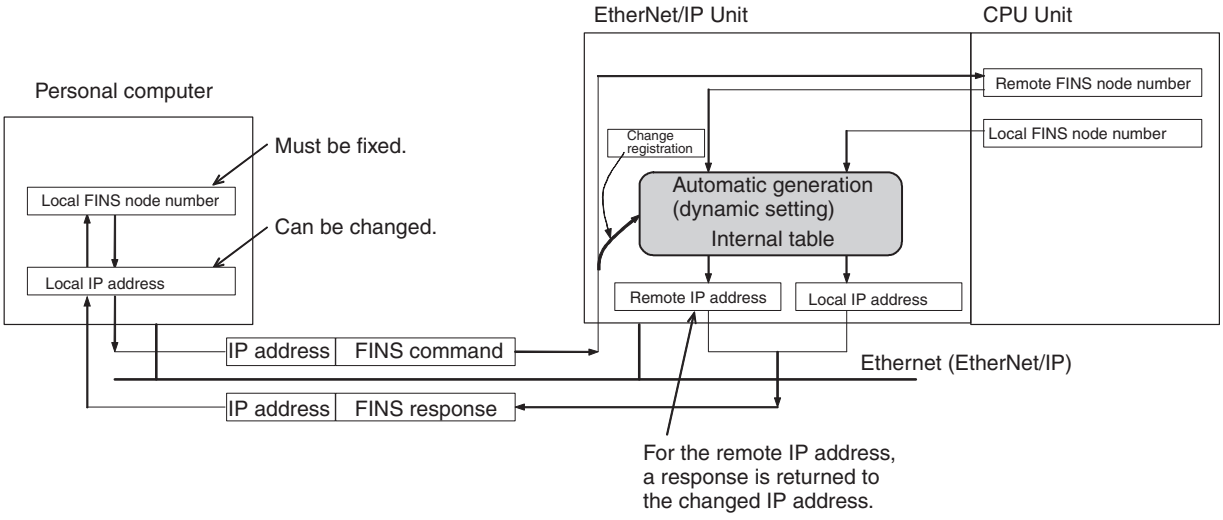
FINS/UDP Communications Methods

Automatic Generation (Dynamic)

When the EtherNet/IP Unit or built-in EtherNet/IP port is turned ON or restarted, the following values are set for addresses in the internal table.

- Remote IP address:Local IP address network number + remote FINS node address
- Remote UDP port number:UDP port number set for local Unit
- Connection method:FINS/UDP

With the dynamic method, data in an internal table that has been generated can be dynamically converted according to FINS messages received from remote nodes. This is enabled when the remote node is a device such as a personal computer and IP addresses are dynamically changed by a method such as DHCP.

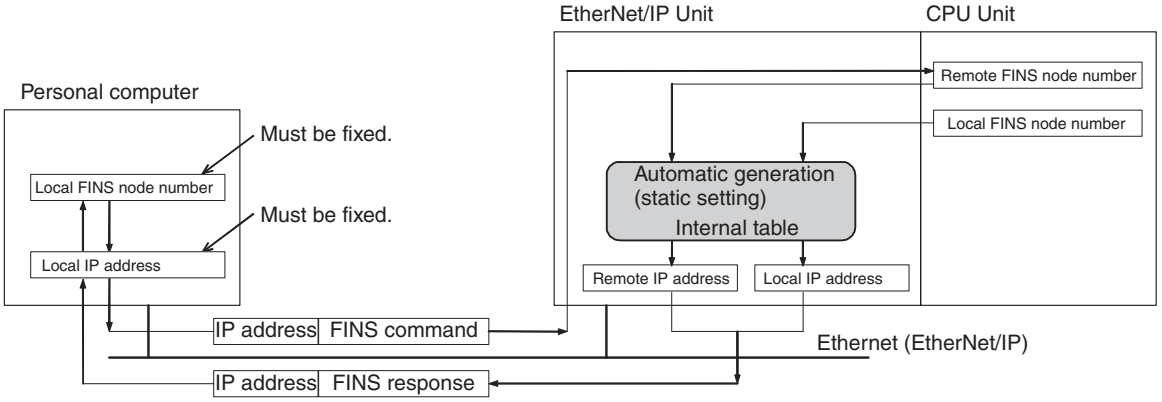


Automatic Generation (Static)

With the static method as well, the following values are set for addresses in the internal table when the EtherNet/IP Unit or built-in EtherNet/IP port is turned ON or restarted.

- Remote IP address:Local IP address network number + remote FINS node address
- Remote UDP port number:UDP port number set for local Unit
- Connection method:FINS/UDP

With the static method, however, data in an internal table that has been generated is not freely changed.



IP Address Table Method

With this method, FINS node addresses are converted to IP addresses based on a preset correspondence table (IP address table).

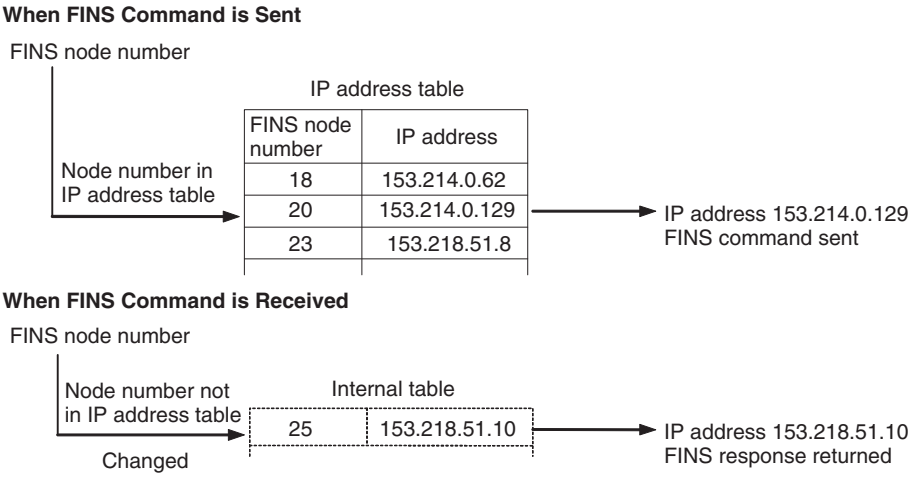
The IP address table is set on the FINS/UDP Tab Page of the Edit Parameters Dialog Box of the CX-Programmer. Nodes can be registered even if they are in different segments and have different network IDs

The internal table will be as follows:

- FINS Node Address Registered to IP Address Table
  The following address is registered to the internal table.
  - Remote IP address: IP address registered to IP address table
  - Remote UDP port number: UDP port number set for local Unit
  - Connection method: FINS/UDP
- FINS Node Address Not Registered to IP Address Table
  The following address is registered to the internal table.
  - Remote IP address: 0.0.0.0
  - Remote UDP port number: UDP port number set for local Unit
  - Connection method: FINS/UDP

With the IP address table method, records of FINS nodes registered to the IP address table are not changed dynamically. When the Unit is turned ON or restarted, the IP addresses of remote FINS nodes registered with an IP address of 0.0.0.0 can be changed dynamically according to FINS messages received from remote nodes. This can be used effectively when the remote node is a device such as a personal computer and IP addresses are dynamically changed by a method such as DHCP.

Example



Combined Method

The combined method combines the IP address table method and the automatic generation method (dynamic).

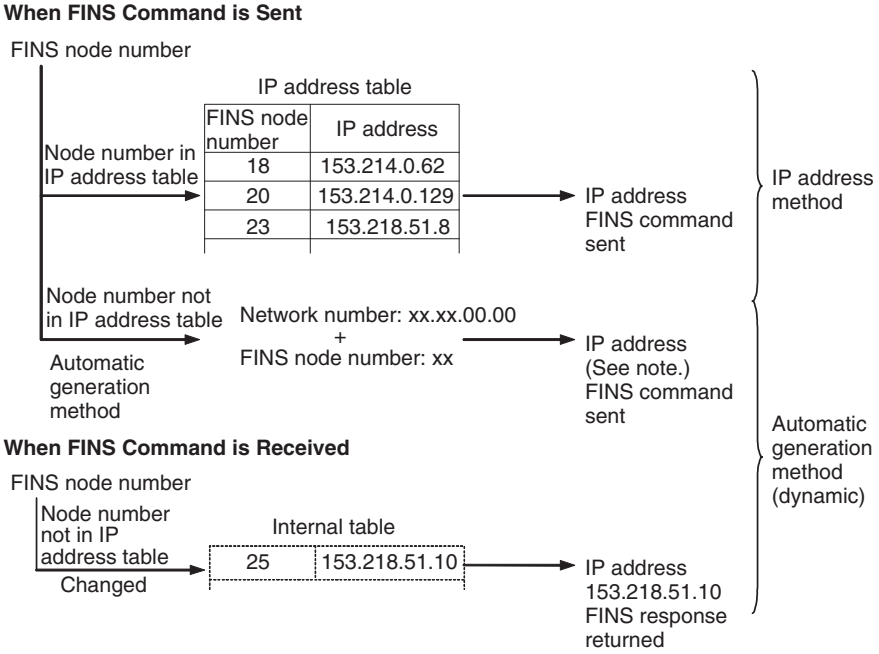
First the IP address table is referenced. Then, if the applicable FINS node address is found, the corresponding IP address is read. If the FINS node address is not found, the IP address is calculated using the automatic generation method (dynamic).

The internal table will be as follows:

- FINS Node Address Registered to IP Address Table
  The following address is registered to the internal table.
  - Remote IP address: IP address registered in IP address table
  - Remote UDP port number: UDP port number set for local Unit
  - Connection method: FINS/UDP
- FINS Node Address Not Registered to IP Address Table
  The following address is registered to the internal table.
  - Remote IP address: Local IP address network number + FINS node address
  - Remote UDP port number: UDP port number set for local Unit
  - Connection method: FINS/UDP

With the combined method, records of FINS nodes registered to the IP address table are not dynamically changed. When the Unit is turned ON or restarted and the IP address of a remote FINS node is not registered in the IP table, the IP address can be changed dynamically according to FINS messages received from the remote node. This can be used effectively when the remote node is a device such as a personal computer and IP addresses are dynamically changed by a method such as DHCP.

Example



Note When an internal table IP address has been changed with the reception of a FINS command, this is sent to the IP address in the internal table.

Prohibiting Dynamically Changing Remote IP Addresses

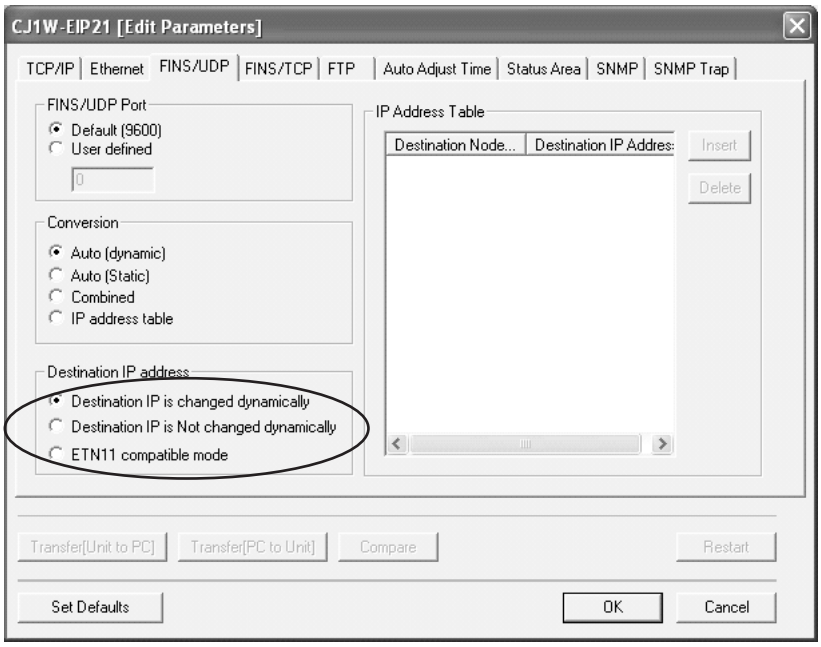
With EtherNet/IP Units and built-in EtherNet/IP ports, it is possible to prohibit (protect against) dynamic changes to remote IP addresses by each method (automatic generation, IP address table, or combined method). Use the CX-Programmer to make this setting.

When dynamically changing remote (destination) IP addresses is prohibited, the internal table for each method is maintained in the same state it had when the power was turned ON or restarted. Therefore, protection can be provided against access using FINS/UDP from personal computers or other devices that have dynamically changing IP addresses. To prohibit dynamic changes, clear the selection of the *Destination IP is changed dynamically* Option on the FINS/UDP Tab Page in the Edit Parameters Dialog Box of the CX-Programmer.

Using the ETN11-compatible Mode

With EtherNet/IP Units and built-in EtherNet/IP ports, operating specifications can be made compatible with the CS1W-ETN11/CJ1W-ETN11 for all methods (automatic generation (dynamic), I/O address table, or combined). (Dynamic changes, however, are prohibited for the destination IP address in ETN11-compatible mode.) While in ETN11-compatible mode, the following operations will be performed the same as they are for the CS1W-ETN11/CJ1W-ETN11 for FINS/UDP command data sent from a UDP port number other than the local FINS/UDP port number (default: 9600) set in the FINS/UDP Tab Page.

- If the command data is addressed to an Ethernet Unit, a FINS response will be sent to the source UDP port number.
- If the command data is for any other Unit, such as the CPU Unit, a FINS response will be sent to the UDP port number set as the FINS/UDP port number.



Note If the ETN11-compatible mode is used, the internal table will retain the same content from when it was created after the EtherNet/IP Unit was turned ON or restarted. This feature provides protection from access via FINS/UDP from computers that dynamically change their IP address.

FINS/TCP Communications Method

Pairing in the FINS/TCP Method

With the FINS/TCP method, communications are first established for each connection, and then remote FINS node addresses are mutually converted. (See note.) After the FINS node address is converted, FINS message communications are executed.

In this way, remote FINS node addresses and remote IP addresses are paired for each connection. Therefore, with the FINS/TCP method, there is no need to set IP address conversions (i.e., pairing FINS node addresses with IP addresses) as with FINS/UDP. On the other hand, it is necessary to set the remote IP address for each connection in the FINS/TCP Tab Page of the Network Configurator's Edit Parameters Dialog Box.

Note The internal table is changed after connections are established.

Internal Processing

The EtherNet/IP Unit or built-in EtherNet/IP port executes the following processing when the FINS/TCP method is used.

■ Local Device: FINS/TCP Client

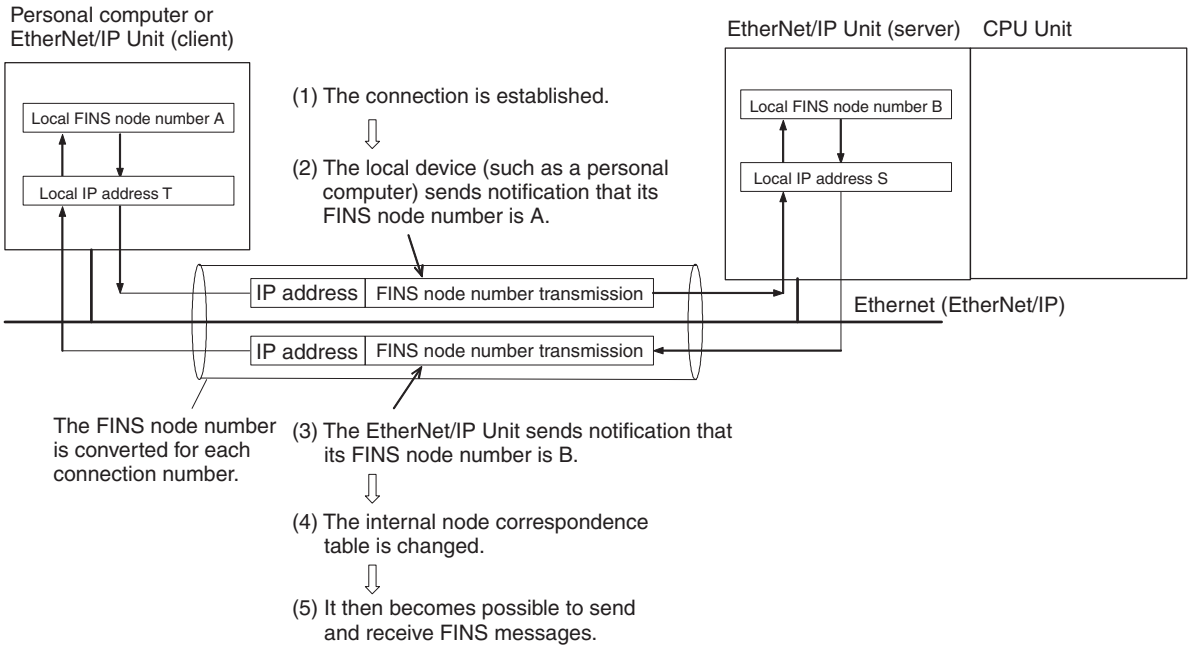
1,2,3...

1. Connections are established in TCP/IP protocol with the remote IP addresses set for FINS/TCP connections in the FINS/TCP Tab Page of the CX-Programmer's Edit Parameters Dialog Box.
2. The remote node (i.e., the server) is notified of the FINS node address for the local device.
3. Notification is received from the remote node (i.e., the server) of the remote node's FINS node address.
4. The EtherNet/IP Unit or built-in EtherNet/IP port changes the internal table (FINS node address, IP address, and TCP port number).
5. FINS messages can then be sent and received.

■ Local Device: FINS/TCP Server

1,2,3...

1. A request to open a connection is received in TCP/IP protocol from the remote device (i.e., the client, either a personal computer, an EtherNet/IP Unit or built-in EtherNet/IP port), and the connection is established.
2. Notification is received from the remote node (i.e., the client) of the remote node's FINS node address.
3. The local device provides notification of the local FINS node address.
4. The EtherNet/IP Unit or built-in EtherNet/IP port changes the internal node correspondence table (FINS node address, IP address, and TCP port number).
5. FINS messages can then be sent and received.



Setting FINS/TCP Connections

The procedure for setting FINS/TCP connections involves the items described below. The settings are made individually for each connection (numbers 1 to 16) on the FINS/TCP Tab Page of the Edit Parameters Dialog Box of the CX-Programmer.

■ Local Device: Server

1,2,3...

1. Set the server.
2. Set IP addresses for the devices to be connected.
   If the option for protection of IP addresses is selected, set the IP addresses for clients where connections are permitted. (This step can be omitted.)
3. Automatic FINS node address allocation:
   If the client (generally a personal computer) supports FINS/TCP, and if it is to be used without setting a FINS node address, the value set here (from 239 to 254) can be allocated to the client. The default settings should normally be used.

■ Local Device: Client

1,2,3...

1. Set the client.

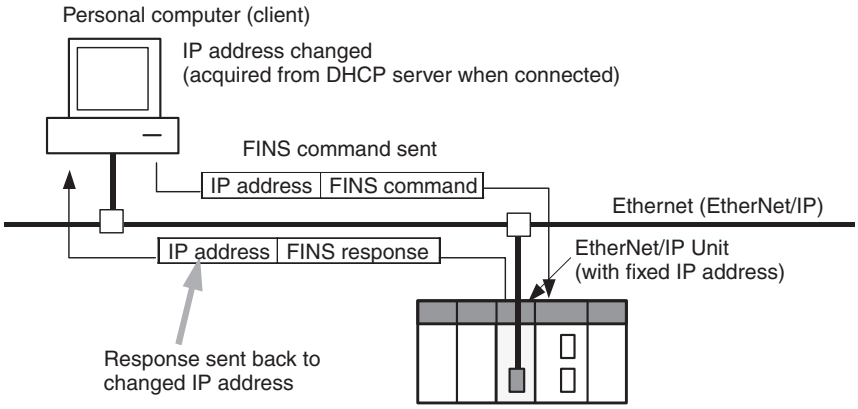
2. Set IP addresses for the devices to be connected.
   Set the IP address for the remote EtherNet/IP Unit or built-in EtherNet/IP port (i.e., the server) connected by FINS/TCP.
   This setting must be made if this EtherNet/IP Unit will be used as a FINS/TCP client.

5-2-3 Application Examples

Responding to Computers with Changed IP Addresses

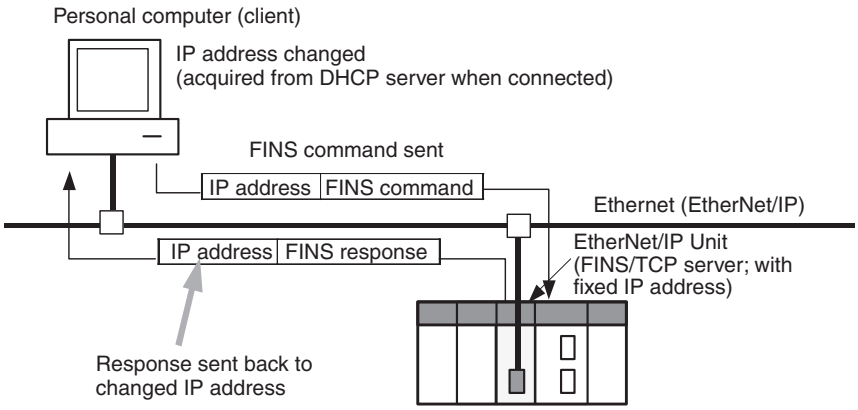
FINS/UDP Communications Method

With FINS/UDP, whether using the automatic conversion method (dynamic), the IP address table method, or the combined method, remote FINS node addresses and remote IP addresses in the internal table are changed after FINS messages are received. Therefore, even when a FINS command has been received from a personal computer (a DHCP client computer) for which the IP address is dynamically changed, a response can still be sent back to the computer (the DHCP client computer) from which the command originated.



FINS/TCP Communications Method

With FINS/TCP, FINS node addresses and IP addresses in the internal table are changed with each connection that is established. Therefore, even when a FINS command has been received from a personal computer (a DHCP client computer) for which the IP address is dynamically changed, a response can still be sent back to the computer (the DHCP client computer) from which the command originated.



Note Automatic IP Address Setting by DHCP Service
DHCP service is a method whereby a DHCP server collectively manages all of the IP address in a network.
Nodes that are functioning as clients acquire IP addresses from the DHCP

server whenever the system is started. Therefore, at a personal computer using the DHCP service, IP addresses may be different with each system startup.
DHCP service is mainly used for automatic settings in devices such as personal computers that are used for client applications. Nodes used for server applications are normally allocated fixed IP addresses. EtherNet/IP Units and built-in EtherNet/IP ports in PLC systems are also allocated fixed IP addresses.

Simultaneously Running Multiple Applications on a Personal Computer

In communications involving previous models, multiple communications applications were configured on personal computers according to data accessing uses, and the fact that no more than one UDP port number for FINS communications could be used on any given computer created a problem. This EtherNet/IP Unit provides a practical solution with an internal table that pairs remote nodes (applications) with FINS node addresses, enabling dynamic changes.

FINS/UDP Communications Method

FINS nodes are allocated individually for each application on the computer, and the respective FINS/UDP port numbers that are used are also allocated individually. When FINS/UDP FINS commands are sent from individual applications to the EtherNet/IP Unit or built-in EtherNet/IP port, the respective remote IP addresses and remote port numbers in the internal table are dynamically changed.

FINS/TCP Communications Method

With this method as well, FINS nodes are allocated individually for each application on the computer, and the respective FINS/TCP port numbers that are used are also allocated individually. Each application is positioned with a FINS/TCP client, and requests the opening of a connection with the FINS/TCP server of the EtherNet/IP Unit or built-in EtherNet/IP port. When the connection is established, the respective remote IP address and remote port number in the internal table are dynamically changed.

5-2-4 Related Products and Communications/Setting Methods

Models Supporting Automatic Generation Method (Dynamic)

<table>
<tr><th colspan="2">Product</th><th>Model/Series/ Version</th><th>Supports automatic generation method (dynamic)?</th></tr>
<tr><td rowspan="3">CS-series Ethernet Unit</td><td>100BASE-TX</td><td>CS1W-ETN21</td><td>Yes</td></tr>
<tr><td>10BASE-5</td><td>CS1W-ETN01</td><td rowspan="3">No: Set by automatic generation method or combined method. Communications are not possible with personal computers with variable IP addresses.</td></tr>
<tr><td>10BASE-T</td><td>CS1W-ETN11</td></tr>
<tr><td rowspan="2">CJ-series Ethernet Unit</td><td>100BASE-TX</td><td>CJ1W-ETN21</td><td>Yes</td></tr>
<tr><td>10BASE-T</td><td>CJ1W-ETN11</td><td rowspan="3">No: Set by automatic generation method or combined method. Communications are not possible with personal computers with variable IP addresses.</td></tr>
<tr><td>CV/CVM1-series Ethernet Unit</td><td>10BASE-5</td><td>CV500-ETN01</td></tr>
<tr><td colspan="2" rowspan="2">FinsGateway</td><td>Version 4.xx or lower</td></tr>
<tr><td>Version 2003 or higher</td><td>Yes</td></tr>
</table>

Product		Model/Series/ Version	Supports automatic generation method (dynamic)?
Programmable Terminal		NS Series	No: Set manually so that automatic settings can be used with the automatic generation method.
Open Network Controller (ONC)		---	

Models Supporting Automatic Generation Method (Static)

Product		Model/Series/ Version	Supports automatic generation method (static)?
CS-series Ethernet Unit	100BASE-TX	CS1W-ETN21	Yes
	10BASE-5	CS1W-ETN01	Yes: Simply called “automatic generation method.”
	10BASE-T	CS1W-ETN11	
CJ-series Ethernet Unit	100BASE-TX	CJ1W-ETN21	Yes
	10BASE-T	CJ1W-ETN11	Yes: Simply called “automatic generation method.”
CV/CVM1-series Ethernet Unit	10BASE-5	CV500-ETN01	
FinsGateway		Version 4.xx or lower	
		Version 2003 or higher	Yes
Programmable Terminal		NS Series	No: Set manually so that automatic settings can be used with the automatic generation method.
Open Network Controller (ONC)		---	

Models Supporting IP Address Table Method

Product		Model/Series/ Version	Supports IP address table method?
CS-series Ethernet Unit	100BASE-TX	CS1W-ETN21	Yes
	10BASE-5	CS1W-ETN01	
	10BASE-T	CS1W-ETN11	
CJ-series Ethernet Unit	100BASE-TX	CJ1W-ETN21	
	10BASE-T	CJ1W-ETN11	
CV/CVM1-series Ethernet Unit	10BASE-5	CV500-ETN01	
FinsGateway		Version 4.xx or lower	
		Version 2003 or higher	
Programmable Terminal		NS Series	No: Set manually. FINS communications are not possible with personal computers set automatically by DHCP.
Open Network Controller (ONC)		---	

Models that Can Use the Combined Method

Product		Model/Series/ Version	Supports combined method?
CS-series Ethernet Unit	100BASE-TX	CS1W-ETN21	Yes
	10BASE-5	CS1W-ETN01	No
	10BASE-T	CS1W-ETN11	No
CJ-series Ethernet Unit	100BASE-TX	CJ1W-ETN21	Yes
	10BASE-T	CJ1W-ETN11	No
CV/CVM1-series Ethernet Unit	10BASE-5	CV500-ETN01	No
FinsGateway		Version 4.xx or lower	No
		Version 2003 or higher	Yes
Programmable Terminal		NS Series	No: Set manually. FINS communications are not possible with personal computers set automatically by DHCP.
Open Network Controller (ONC)		---	

5-2-5 Pairing IP Addresses and FINS Node Addresses

The following table shows the methods for pairing IP address and FINS node addresses, and the relation between fixed and variable address, for both FINS/UDP and FINS/TCP.

Communications method	Method of pairing of IP addresses and FINS node addresses	IP address determination		Client (personal computer or PLC)		Server (PLC)	
				FINS node address	IP address	FINS node address	IP address
FINS/UDP	By pairing FINS node addresses with IP addresses in Ethernet	IP address conversion	Automatic generation method (static)	Fixed	Fixed	Fixed	Fixed
			Automatic generation method (dynamic)	Fixed	Fixed or variable	Fixed	Fixed
			IP address table method	Fixed	Fixed or variable	Fixed	Fixed
			Combined method	Fixed	Fixed or variable	Fixed	Fixed
FINS/TCP	By automatic conversion of FINS node addresses at EtherNet/IP Unit and remote node (and then sending and receiving data)	Automatic	Connection method (automatic FINS node address conversion)	Fixed or can be allocated automatically when not determined.	Fixed or variable	Fixed	Fixed

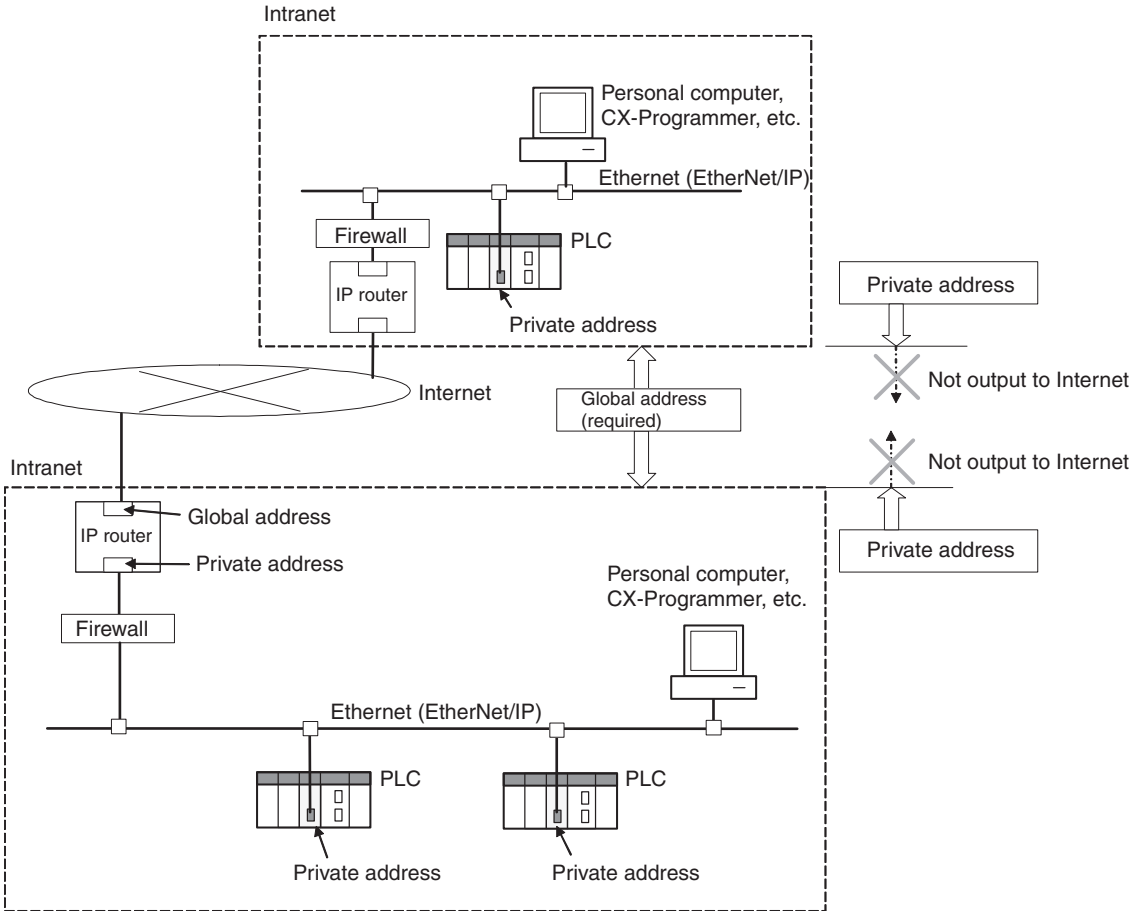
5-3 Private and Global Addresses

5-3-1 Private and Global Addresses

There are two kinds of IP addresses, private and global.

- Global addresses: These are IP addresses that connect directly to the Internet. Allocated by application to NIC, each address is unique in the world, and as many as 4.3 million can be allocated worldwide.
- Private addresses: These are IP addresses for Intranet (LAN) use, and cannot connect directly to the Internet. Frames that include private IP addresses are restricted by the router from being sent outside the LAN.

Generally, as shown below, global addresses in the intranet are allocated only to IP routers (such as broadband routers) interfacing with the Internet. All other nodes in the intranet, including the EtherNet/IP Unit or built-in EtherNet/IP port, are allocated private addresses.

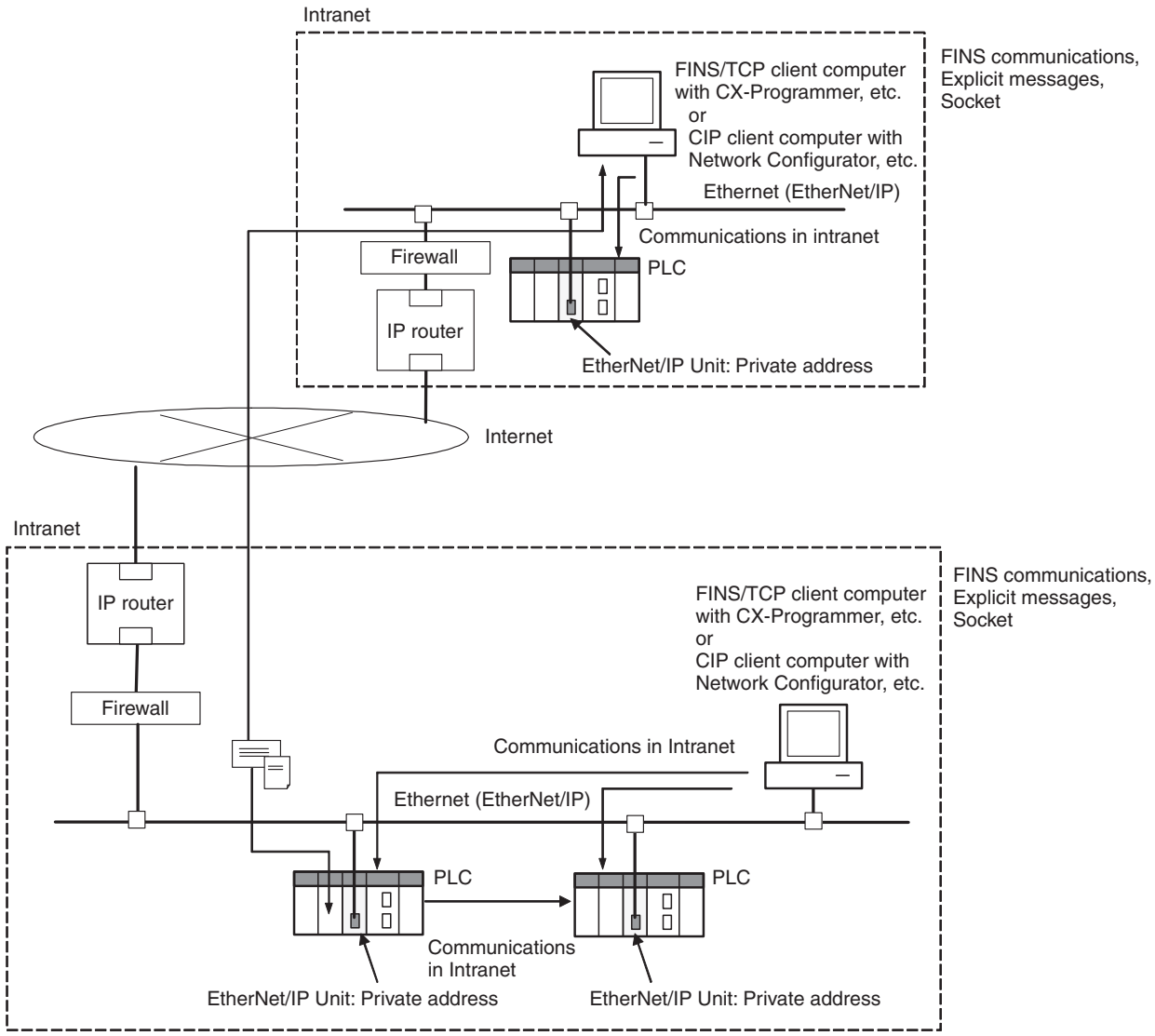


Communications Services That Require Global Addresses for EtherNet/IP Units and built-in EtherNet/IP ports

A global address is required for the IP addresses of the EtherNet/IP Units and built-in EtherNet/IP port when the following communications services are used over the Internet.

- FINS communications services
- Explicit message communications services
- Socket services

5-3-2 Using a Private Address for the EtherNet/IP Unit



Conditions for Using Communications Applications

When the EtherNet/IP Unit or built-in EtherNet/IP port has a private address, communications applications can be used under the following conditions:

■ **FINS Communications Service**

- The FINS communications service can be executed on the intranet between EtherNet/IP Units and built-in EtherNet/IP ports with private addresses only.
  A device such as a personal computer (with a FINS application, including the CX-Programmer) cannot connect online and communicate over the Internet with an EtherNet/IP Unit or built-in EtherNet/IP port that has a private address. FINS communications are also not possible over the Internet between EtherNet/IP Units and or built-in EtherNet/IP ports with private addresses.
- Either FINS/TCP or FINS/UDP can be used for the FINS communications service.
- With FINS/UDP, all of the EtherNet/IP Unit or built-in EtherNet/IP port IP address conversion methods can be used.

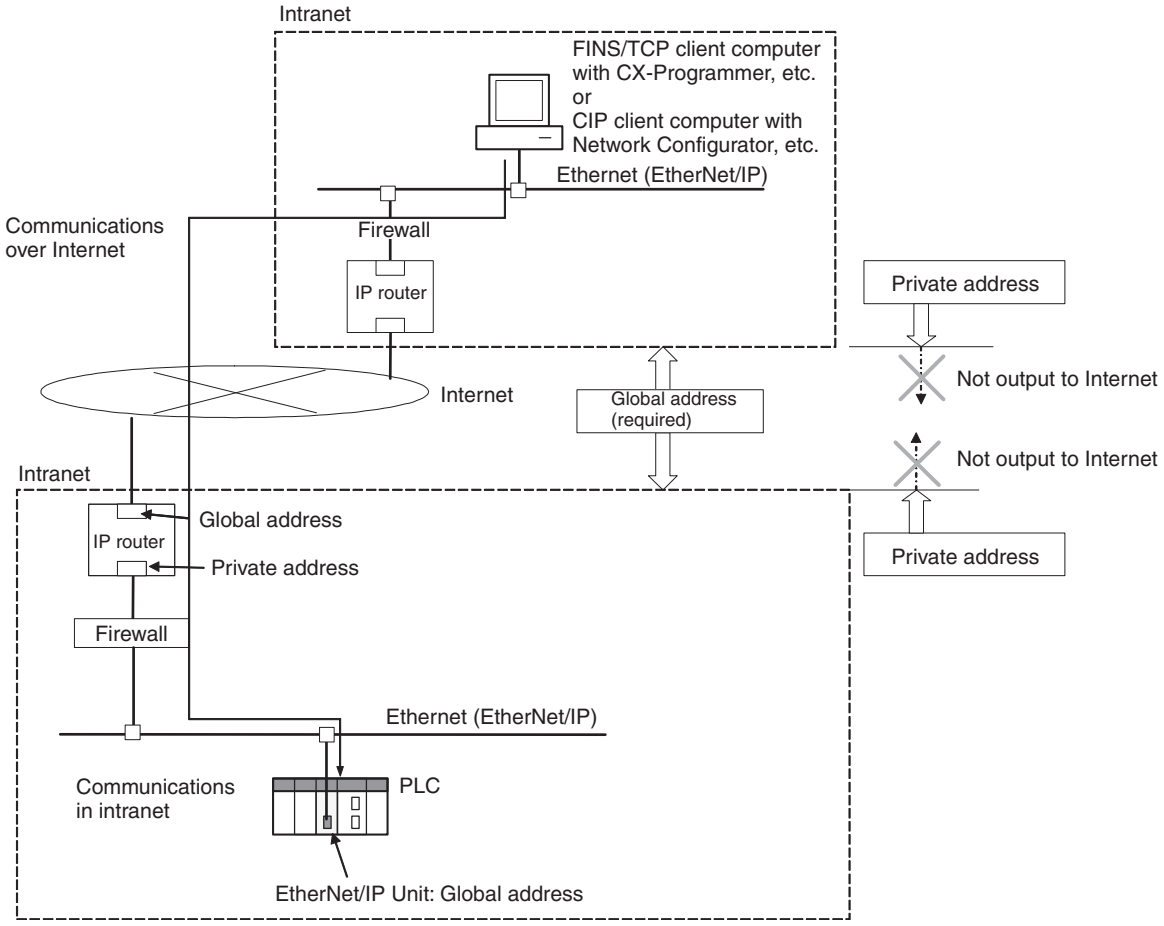
- With FINS/UDP, when the IP address (private address) of a computer serving as a DHCP client is changed, the IP address conversion method of the EtherNet/IP Unit or built-in EtherNet/IP port will be the automatic generation method (dynamic), the combined method, or the IP address table method. When FINS/TCP is used, IP addresses can be changed automatically.

■ **Explicit Message Communications Service**

- The explicit message communications service can be executed on the intranet between EtherNet/IP Units and built-in EtherNet/IP ports with private addresses only.
- A device such as a personal computer (CIP applications including the Network Configurator) cannot connect online and communicate over the Internet with an EtherNet/IP Unit or built-in EtherNet/IP port that has a private address. Explicit message communications are also not possible over the Internet between EtherNet/IP Units and built-in EtherNet/IP ports with private addresses.

Note Network Security and Firewalls
Setting up an intranet through a global address involves network security considerations. Before doing so, be sure to consult with a network specialist and consider installing a firewall.
Once a firewall has been set up by a communications technician, on the other hand, there may be some applications that cannot be used. Be sure to check first with the communications technician.

5-3-3 EtherNet/IP Unit with a Global Address



Conditions for Using Communications Applications

Communications applications can be used over the Internet under the following conditions:

■ **FINS Communications Service**

- A device such as a personal computer (a FINS application, including the CX-Programmer) can connect online and communicate over the Internet with an EtherNet/IP Unit or built-in EtherNet/IP port that has a global address.
- FINS/TCP is recommended as the FINS communications service method. FINS/TCP is more reliable than FINS/UDP in terms of communications errors involving IP routers.
- The IP address table method is used as the IP address conversion method of the EtherNet/IP Unit or built-in EtherNet/IP port.
- The TCP port number to be used for FINS/TCP cannot be used if prohibited by a firewall in the communications path.

■ **Explicit Message Communications Service**

- A device such as a personal computer (a CIP application including the Network Configurator) can connect online and communicate over the Internet with an EtherNet/IP Unit or built-in EtherNet/IP port that has a global address.

- The TCP port number (44818) or UDP port number (44818) that is used for EtherNet/IP cannot be used if prohibited by a firewall in the communications path.

Note Network Security and Firewalls
Setting a global IP address for an EtherNet/IP Unit or built-in EtherNet/IP port involves network security considerations. It is recommended that the user contract with a communications company for a dedicated line, rather than using a general line such as a broadband line. Also, be sure to consult with a network specialist and consider security measures such as a firewall.
Once a firewall has been set up by a communications technician, on the other hand, there may be some applications that cannot be used. Be sure to check first with the communications technician.

SECTION 6
Tag Data Link Functions

This section describes tag data link functions and related Network Configurator operations.

6-1 Overview of Tag Data Links 144
6-1-1 Tag Data Links 144
6-1-2 Overview of Operation 145
6-1-3 Tag Data Link Functions and Specifications 148
6-1-4 Data Link Data Areas 149
6-2 Setting Tag Data Links 153
6-2-1 Starting the Network Configurator 153
6-2-2 Tag Data Link Setting Procedure 156
6-2-3 Registering Devices 157
6-2-4 Creating Tags and Tag Sets 159
6-2-5 Connection Settings 174
6-2-6 Setting Tags Using Data Link Tool 183
6-2-7 Creating Connections Using the Wizard 189
6-2-8 Creating Connections by Device Dragging and Dropping 192
6-2-9 Connecting the Network Configurator to the Network 194
6-2-10 Downloading Tag Data Link Parameters 204
6-2-11 Uploading Tag Data Link Parameters 208
6-2-12 Verifying the Tag Data Links 209
6-2-13 Starting and Stopping Tag Data Links 212
6-2-14 Clearing the Device Parameters 213
6-2-15 Saving the Network Configuration File 214
6-2-16 Reading a Network Configuration File 215
6-2-17 Checking Connections 216
6-2-18 Changing Devices 217
6-2-19 Displaying Device Status 218
6-3 Ladder Programming with Tag Data Links 220
6-3-1 Ladder Programming Related to Tag Data Links 220
6-3-2 Status Flags Related to Tag Data Links 224
6-4 QuickConnect 225

6-1 Overview of Tag Data Links

6-1-1 Tag Data Links

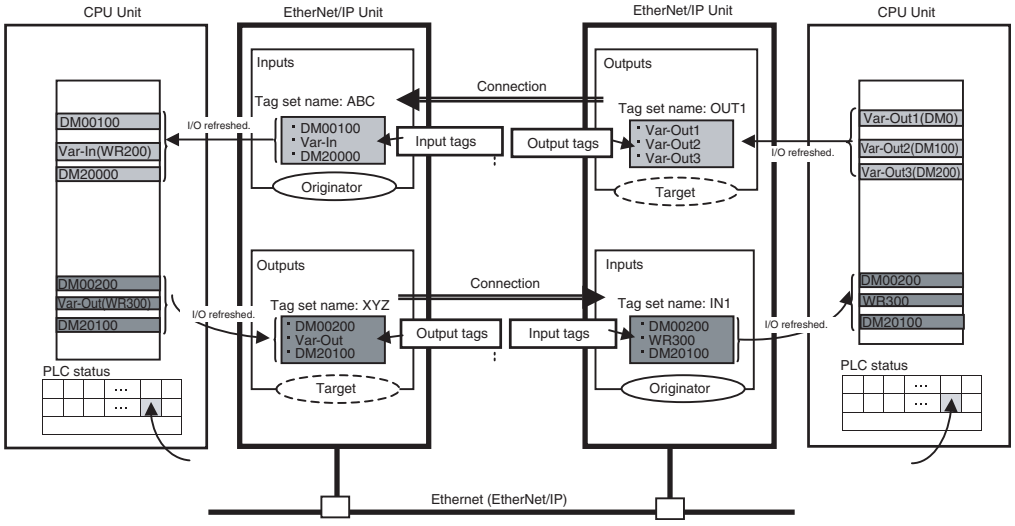
Tag data links enable cyclic data exchanges on an EtherNet/IP network between PLCs or between PLCs and another device. I/O memory addresses (e.g., in the CIO or DM Area) and symbols can be assigned to tags. The settings for tag data links are made using the Network Configurator. Refer to *6-2 Setting Tag Data Links* for information on how to make the settings.

Note

(1) Symbols can be used in tags for the Symbols can be used in tags for the CJ2H-CPU6□-EIP with unit version 1.6 or later, and CJ2M-CPU□□ with unit version 2.2 or later. If you are using a EtherNet/IP Unit that is mounted to any other CPU Unit, use I/O memory addresses to set the tag data links.

(2) If you clear the *Use CIP message server* Check Box, the tag data links cannot be used. Select the *Use CIP message server* Check Box. Refer to *CIP Message Server* in *13-4 Opening and Closing the Port* for information on the CIP message server settings.

With tag data links, one node requests the opening of a communications line called a connection to exchange data with another node. The node that requests opening the connection is called the originator, and the node that receives the request is called the target.



For communications between PLCs, the connection information is set in the EtherNet/IP Unit or built-in EtherNet/IP port of the PLC that receives data (i.e., the originator).

Note For communications between a PLC and an I/O device, the connection information is set in the EtherNet/IP Unit or built-in EtherNet/IP port that is the originator. If an I/O device is used, the Network Configurator must have an EDS file installed that includes connection information for the I/O device. Refer to *Appendix F EDS File Management* for the installation procedure. The output words and input words for each node for which data is exchanged must be set in the connection information. These words are called an output tag set and an input tag set, respectively. Each tag set must contain at least one tag.

The size of data for data exchange is the total size of tags included in the tag set. The size of the output tag set and the size of the input tag set must match. The set connection information is called tag data link parameters in this manual.

The following describes how to set tag data link parameters using the Network Configurator.

6-1-2 Overview of Operation

Setting and Downloading Tag Data Link Parameters

The tag data link parameters (e.g., connection information) that are described below are created using the Network Configurator, and then the parameters are downloaded to all originator devices on the EtherNet/IP network.

Make the following settings using the Network Configurator if tag data link functionality is used.

Tag Settings

Create input (reception) tags and output (send) tags for addresses in the CPU Unit's I/O memory areas or for symbols.

With the CJ2/CJ3 CPU Unit, you can create tags by importing network symbols (i.e., I/O allocation settings) that were created using the CX-Programmer into the Network Configurator. Output tags can be defined to clear output data to 0 or to hold the output data when PLC outputs are turned OFF.

Note The maximum number of tags that can be used is as shown in “6-1-3 Tag Data Link Functions and Specifications.”

Setting Tag Sets

Create output tag sets and input tag sets and position them.

The PLC status can be specified in a tag set to indicate the CPU Unit’s operating status (operating information and error information).

Note The maximum number of tags that can be used is as shown in “6-1-3 Tag Data Link Functions and Specifications.”

Setting Connections

The target device output tag set and the originator device input tag set are associated as connections.

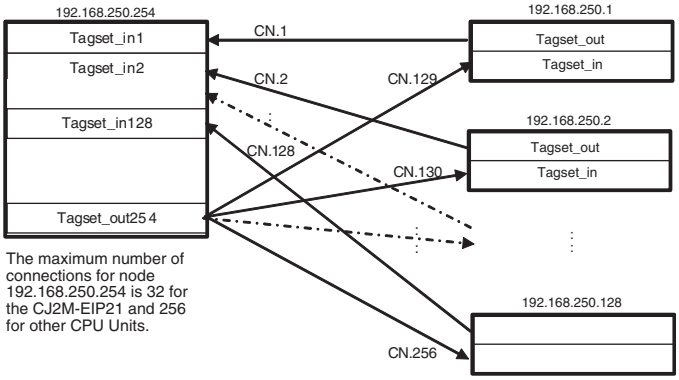
Note The maximum number of tags that can be used is as shown in “6-1-3 Tag Data Link Functions and Specifications.”

Counting Connections

The number of connections is the total of the number of input tag sets that receive data and the number of nodes that send data for output tag sets. (Refer to the following figure.) One connection is consumed for each connection setting whether the connection is a multicast connection or a unicast (point-to-point) connection.

Example of Calculating the Number of Connections

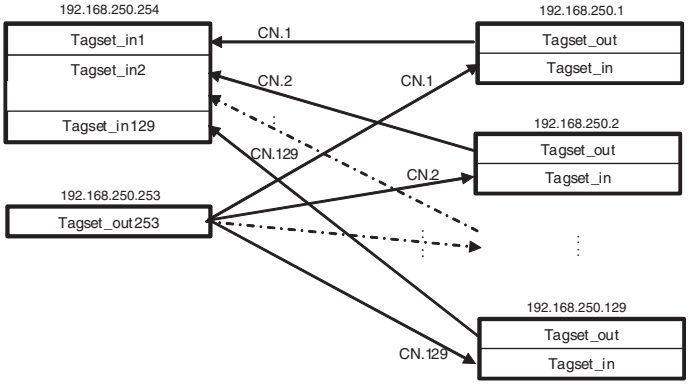
- EtherNet/IP Unit or built-in EtherNet/IP port with IP address of 192.168.250.254 in bidirectional connection with 128 nodes



Another EtherNet/IP Unit must be mounted to the PLC to increase the maximum number of connections. (Refer to the following figure.)

Example of Calculating the Number of Connections

- The maximum number of connections (32 for the CJ2M-EIP21 and 256 for other CPU Units) per Unit would be exceeded if an EtherNet/IP Unit or built-in EtherNet/IP port with an IP address of 192.168.250.254 is used in a bidirectional connection with 129 nodes. In this case, bidirectional communications can be performed with 129 nodes or more by adding an EtherNet/IP Unit with the IP address of, for example, 192.168.250.253 to the same PLC, creating an output tag set in the new EtherNet/IP Unit, and creating connections.



Setting the Packet Interval (RPI)

The packet interval is the data I/O refresh cycle in the Ethernet circuit when performing tag data links, and can be set separately for each connection.

With EtherNet/IP, data is exchanged on the communications line at the packet interval that is set for each connection, regardless of the number of nodes.

Note The setting value of the packet interval is as shown in “6-1-3 Tag Data Link Functions and Specifications.” The default setting is 50 ms.

Using Multicast and Unicast Communications

A multicast connection or unicast (point-to-point) connection can be selected as the connection type in the tag data link connection settings.

With a multicast connection, you can send an output tag set in one package to multiple nodes and make allocations to the input tag sets.

A unicast connection separately sends one output tag set to each node, and so it sends the same number of packets as the number of input tag sets.

Therefore, using multicast connections can decrease the communications load if one output tag set is sent to multiple nodes.

If multicast connections are used, however, use a switching hub that has multicast filtering, unless the tag set is received by all nodes in the network.

If a switching hub that does not have multicast filtering is used, the multicast packets will be broadcast to the entire network, and so packets will be sent to nodes that do not require them, which will cause the communications load on those nodes to increase.

This applies only if one output tag set is sent to multiple nodes using a multicast connection with one packet, the connection type of the connections that receive the output tag set is multicast, and the connection I/O types, packet intervals (RPI), and timeout values are all the same.

Note The performance of communications devices is limited to some extent by the limitations of each product’s specifications. Consequently, there are limits to the packet interval (RPI) settings. Refer to *10-2 Adjusting the Communications Load* and set an appropriate packet interval (RPI).

Starting and Stopping Tag Data Links

Tag data links are automatically started when the data link parameters are downloaded from the Network Configurator. Thereafter, tag data links can be stopped and started for the entire network or individual devices from the Network Configurator. Starting and stopping tag data links for individual devices must be performed for the originator.

Software switches in allocated words can also be used to start and stop tag data links for the entire network. Refer to *6-2-13 Starting and Stopping Tag Data Links* for details.

6-1-3 Tag Data Link Functions and Specifications

Item	CS1W-EIP21/EIP21S CJ1W-EIP21/EIP21S CJ2H-CPU□□-EIP CJ3M-CPU3□	CJ2M-CPU3
Communications type	Standard EtherNet/IP implicit communications (connection-type cyclic communications)	
Tags	Number of words per tag: 722 max. (1,444 bytes) Number of tags per Unit: 256 max. for other CPU Units	Number of words per tag: 640 max. (1,280 bytes) Number of tags per Unit: 32 max.
Tag sets	Number of tags per tag set: 8 max. (7 max. if PLC status is included) Number of words per tag set: 722 max. (1,444 bytes) (721 max. if PLC status is included) Number of tag sets per Unit: 256 max.	Number of tags per tag set: 8 max. (7 max. if PLC status is included) Number of words per tag set: 640 max. (1,280 bytes)*1 (639 max. if PLC status is included) Number of tag sets per Unit: 32 max.
Maximum link data size per node (total size of all tags)	184,832 words max. (722 words × 256)	640 words max.
Connections	Number of connections per Unit: 256 max.	Number of connections per Unit: 32 max.
Connection type	Each connection can be set for 1-to-1 (unicast) or 1-to-N (multicast) communications. (Default: Multicast)	
Packet interval (RPI)	0.5 to 10,000 ms (in 0.5-ms units) The packet interval can be set separately for each connection.	1 to 10,000 ms (in 0.5-ms units) The packet interval can be set separately for each connection.

*1 Unit version 2.0: 20 words (40 bytes) maximum.

System Configuration Conditions for Setting Tags Using Symbols or I/O Memory Addresses

Local tags for tag data links can be set using I/O memory addresses or network symbols. Support for network symbols, however, depends on the model of CPU Unit, as shown in the following table.

Communications with the remote node are possible regardless of whether the remote node tags are set using I/O memory addresses or network symbols.

Name in hardware list of Network Configurator	CPU Unit	EtherNet/IP Unit or built-in EtherNet/IP port	Symbol name specification	I/O memory address specification
CJ2B-EIP21	CJ2H-CPU6□-EIP	CJ2H-CPU□□-EIP	OK	OK
CJ2M-EIP21	CJ2M-CPU3□	CJ2M-CPU3□	OK	OK
CJ3M-CPU3□	CJ3M-CPU3□	CJ3M-CPU3□	OK	OK
CJ1W-EIP21(CJ2)	CJ2H-CPU6□(-EIP) CJ2M-CPU□□ CJ3M-CPU□□	CJ1W-EIP21	OK (CJ2H-CPU6□-EIP and CJ2M-CPU3□ only) (See note.)	OK
CJ1W-EIP21	CJ1/CP1H CPU Unit	CJ1W-EIP21	---	OK
CS1W-EIP21	CS1 CPU Unit	CS1W-EIP21	---	OK

Name in hardware list of Network Configurator	CPU Unit	EtherNet/IP Unit or built-in EtherNet/IP port	Symbol name specification	I/O memory address specification
CJ1W-EIP21S(CJ2)	CJ2H-CPU6□(-EIP) CJ2M-CPU□□ CJ3M-CPU□□	CJ1W-EIP21S	OK (See note.)	OK
CJ1W-EIP21S	CJ1/CP1H CPU Unit	CJ1W-EIP21S	No	OK
CS1W-EIP21S	CS1 CPU Unit	CS1W-EIP21S	No	OK

Note This function is supported by the CJ2 CPU Units of CJ2H-CPU6□(-EIP) with unit version 1.6 or later, and CJ2M-CPU□□ with unit version 2.2 or later.

6-1-4 Data Link Data Areas

Tags

A data link between the local I/O memory and a remote I/O memory is called a tag. A tag can be set using a network symbol name or an I/O memory address.

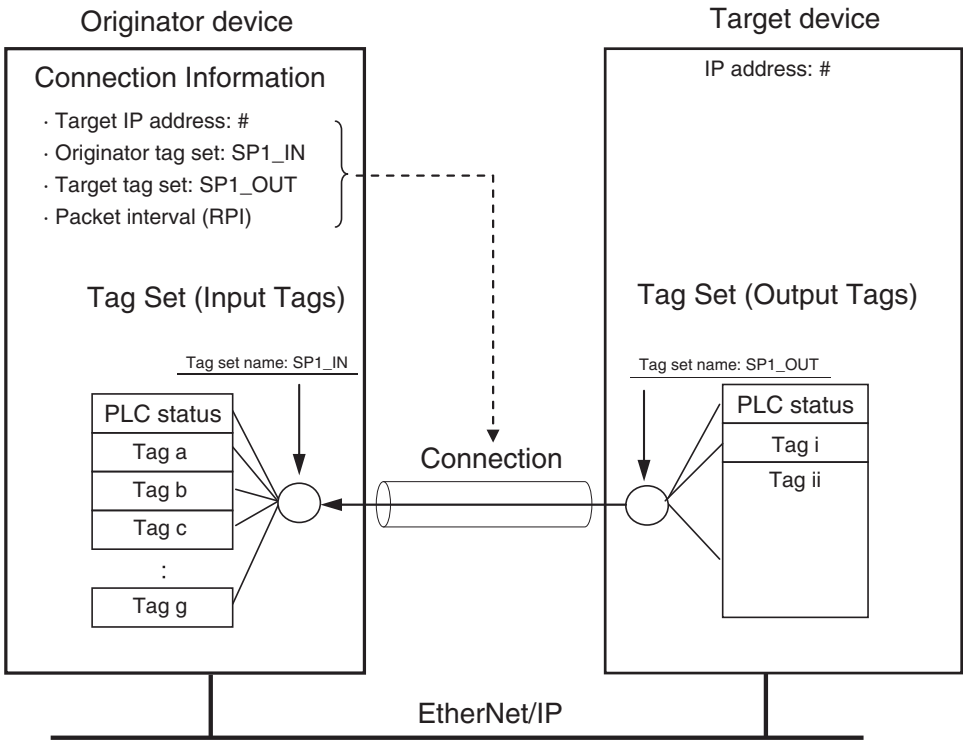
Tag Sets

When a connection is established, from 1 to 8 tags (including PLC status) is configured as a tag set. Each tag set represents the data that is linked for a tag data link connection. Tag data links are thus created by connecting one tag set to another tag set. A tag set name must be set for each tag set. Data is exchanged in the order that the tags are registered in the tag sets. The order of registration of the tags in the input tag sets and output tag sets must therefore be aligned.

Note A connection is used to exchange data as a unit within which data concurrency is maintained. Thus, data concurrency is maintained for all the data exchanged for the tags in one data set.

Example

In the following example, input tags a to g at the originator are a tag set named SP1_IN and output tags i and ii are a tag set named SP1_OUT). A connection is set between these two tag sets.



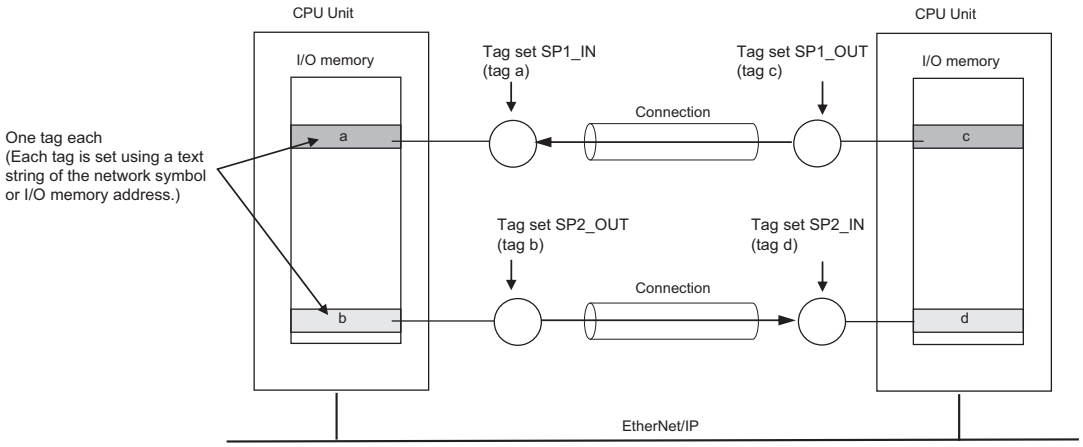
There are both input and output tag sets. Each tag set can contain only input tags or only output tags. The same input tag cannot be included in more than one input tag set.

Number of Tags in Tag Sets

Each tag set can contain one or more tags.

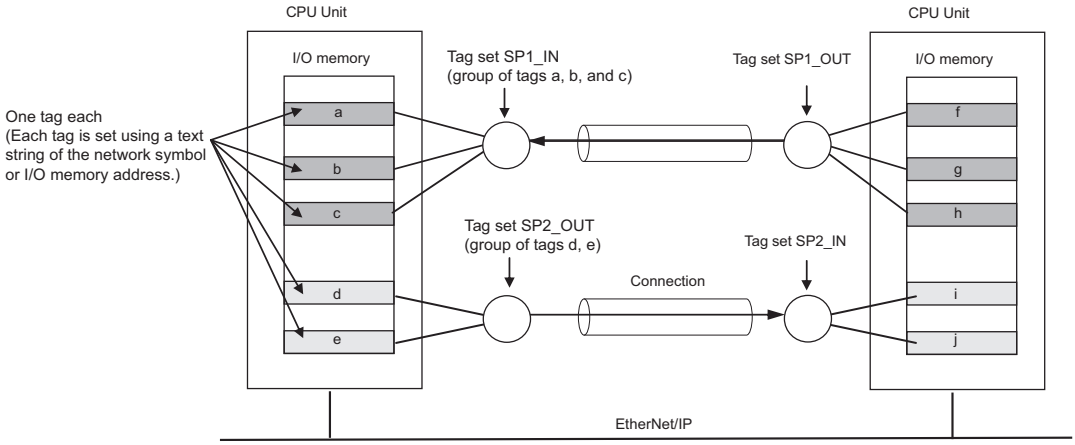
■ **Tag Sets with Only One Tag**

With basic Network Configurator procedures, each tag set contains only one tag.



■ **Tag Sets with Multiple Tags**

As shown below, tags can be created in groups. Each tag set can contain up to 8 tags totaling 640 words for the CJ2M-EIP21 (20 words for unit version 2.0) or 722 words for other CPU Units.



Note The I/O memory words used in tags in a tag set do not have continuous addresses. The tags can also be from different I/O memory areas. To enable a connection, however, each tag set must include only input tags or only output tags. (Both input and output tags cannot be included in the same tag set.)

Note Tag sizes can be set to odd numbers of bytes for any EtherNet/IP Units or built-in EtherNet/IP ports that were manufactured in October 2012 or later. However, the following precautions must be observed.

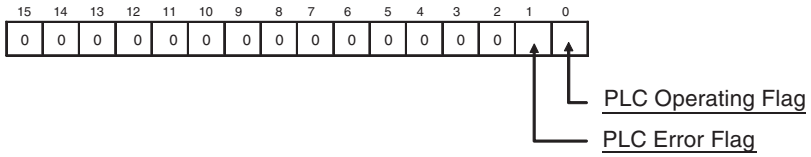
- I/O memory is consumed in units of words. Be sure that sufficient memory space is allocated.

- If you use variables to specify tags, specify any tag size with an odd number of bytes in bytes on the Network Configurator and then define the variable with a data size that is one byte larger as the size on the CX-Programmer.
- Do not use any EtherNet/IP Units or built-in EtherNet/IP ports that do not support tag sizes with an odd number of bytes.

PLC Status

A characteristic function of the CS1W-EIP21 and CJ1W-EIP21 EtherNet/IP Units and CJ2 built-in EtherNet/IP ports is the ability to specify the PLC status as a member of the tag set. This function reads the operating status (operating and error status) of the CPU Unit of the PLC in which the EtherNet/IP Unit is mounted, and includes the PLC status as status flags in the data transferred by the tag data links.

When the PLC status is specified as an output (produce) tag, it is actually transferred as the tag set's leading data in the following format.

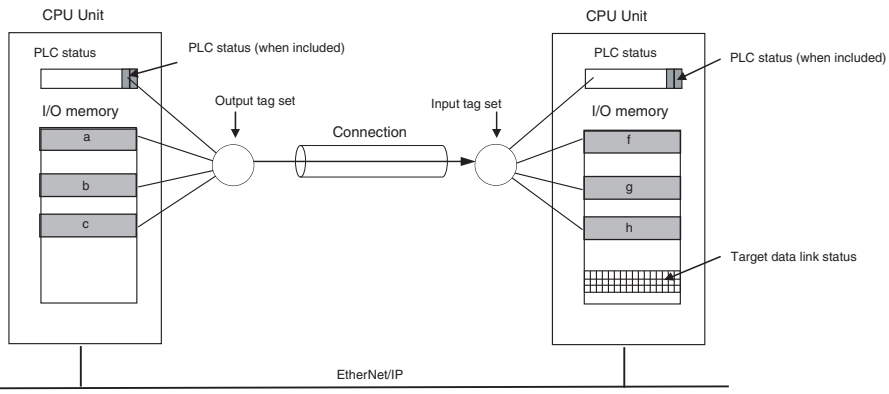


To receive the PLC status, specify the PLC status in an input (consume) tag in the reception tag set as well. When the PLC status is specified in an input tag, the PLC status flags will be reflected in the corresponding location in the tag data link's Target Node PLC Operating Flags and Target Node PLC Error Flags. The following example shows the relationship between the Target Node PLC Operating Flag location and target ID of the target node with 192.168.250.2.

IP address = 192.168.250.2 → (Last byte = 2) → Target ID = #002

Target Node PLC Operating Flags:

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
n+2	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
n+3	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
n+4	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32
n+5	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48



Note The target ID may be duplicated depending on the IP addresses of the target nodes. In this case, it is necessary to change the target ID with the Network Configurator. For information on how to change the device number, refer to step 4 under *Registering Devices in the Register Device List* on page 174.

The following table shows the operation of each the bits when multiple connections are used to communicate with a node, and the PLC status is specified in all of the connections.

Name (allocated area)	Contents
Target Node PLC Operating Flag Information Layout set to default settings: Words n+2 to n+5 Layout set to user settings: Words n+32 to n+47 **Note** Corresponds to the PLC status's PLC Operating Flag.	Each flag indicates the operating status of the corresponding target node PLC of connections in which the EtherNet/IP Unit is the originator. The flag corresponding to the target node's target ID will be ON when the PLC Operating Flags for all connections with that target node indicate that the PLC is operating. Each node address's flag location (i.e., target ID) can be changed from the Network Configurator. The PLC status flags are enabled when the PLC status is included in the communications data for both the originator and target. The data in this table is refreshed when necessary.
Target Node PLC Error Flag Information Layout set to default settings: Words n+6 to n+9 Layout set to user settings: Words n+48 to n+63 **Note** Corresponds to the PLC status's PLC Error Flag.	Each flag indicates the error status (logical OR of non-fatal and fatal errors) of the corresponding target node PLC of connections in which the EtherNet/IP Unit is the originator. The flag corresponding to the target node's target ID will be ON if even one error is indicated in any of the connections with that target node. Each node address's flag location (i.e., target ID) can be changed from the Network Configurator. The PLC status flags are enabled when the PLC status is included in the communications data for both the originator and target. The data in this table is refreshed when necessary.
Normal Target Node Flag Table Layout set to default settings: Words n+20 to n+23 Layout set to user settings: Words n+16 to n+31 **Note** Does not correspond to the PLC status.	Each flag indicates the connection status of the corresponding target node PLC of connections in which the EtherNet/IP Unit is the originator. The flag corresponding to the target node's target ID will be ON when connections are established for all connections with that target node indicate that the PLC is operating. Each node address's flag location (target ID) can be changed from the Network Configurator. The data in this table is refreshed when necessary.

Note When the PLC status is not selected in the input (consume) tags, the PLC status information (16-bit data) can be used as reception data.

6-2 Setting Tag Data Links

6-2-1 Starting the Network Configurator

Procedure

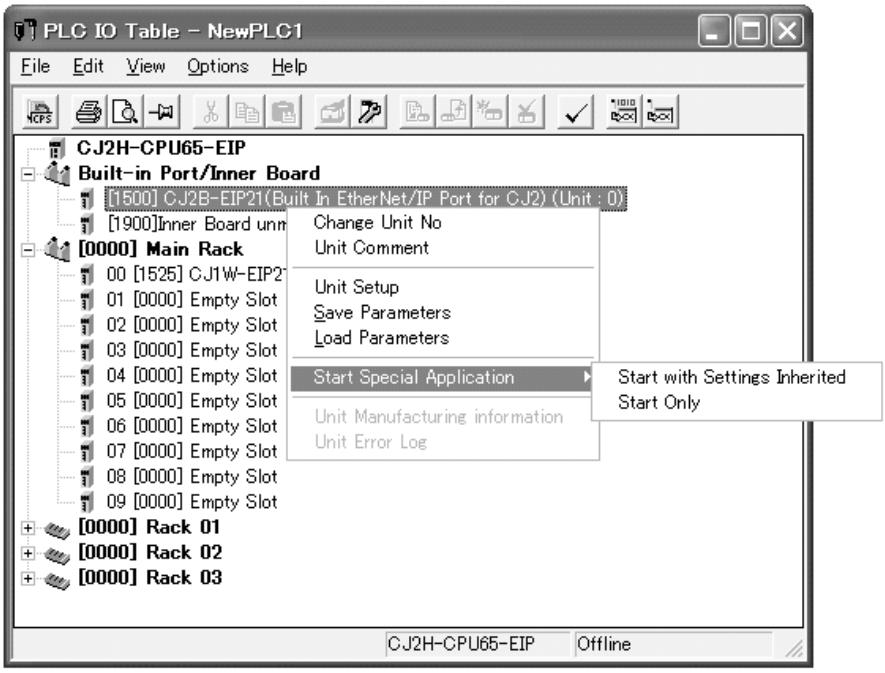
Tag data links are set by using the Network Configurator. Use the following procedure to start the Network Configurator.

■ **Starting from the Windows Start Menu**

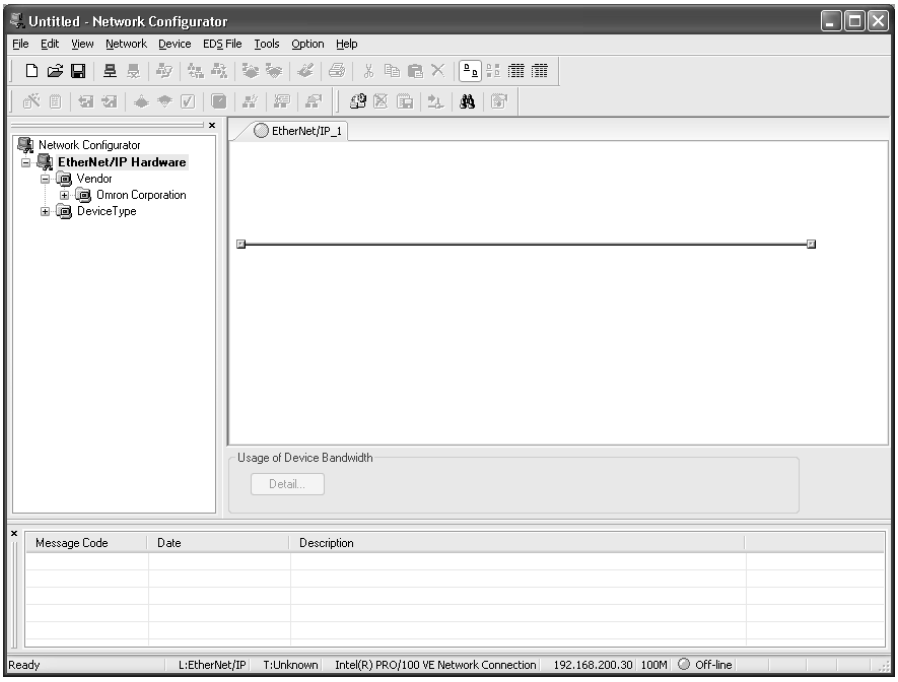
To start the Network configurator, select ***OMRON - CX-One - Network Configurator for EtherNet/IP - Network Configurator*** from the Windows Start Menu.

■ **Starting from the IO Table Dialog Box in CX-Programmer**

To start the Network configurator, select the Unit in the PLC IO Table Dialog Box and select either of the options for ***Start Special Application*** from the pop-up menu. Only operation will be started even if *Start with Settings Inherited* is selected.

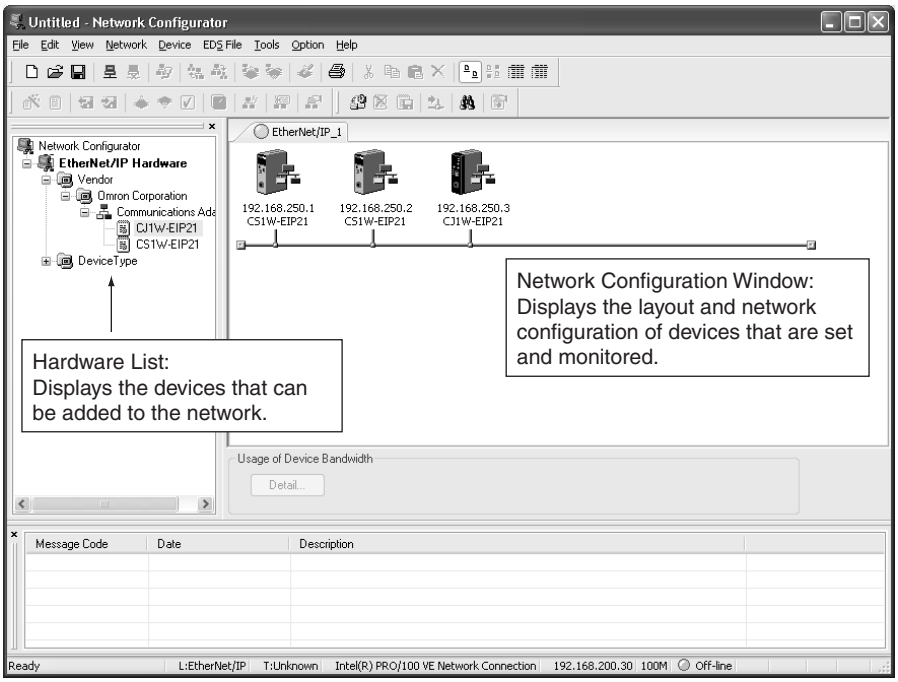


When the Network Configurator starts, the following window will be displayed.

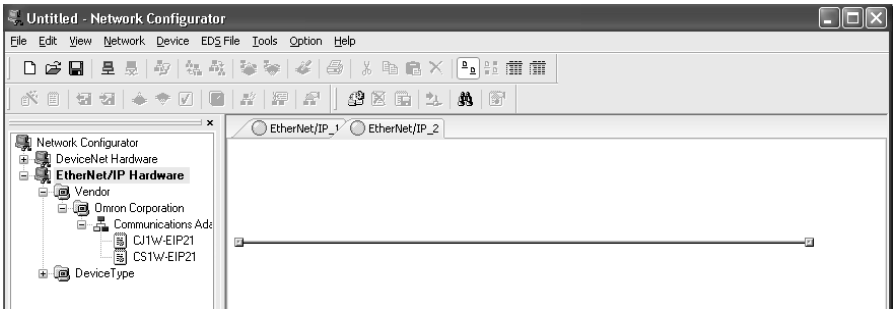


Main Window

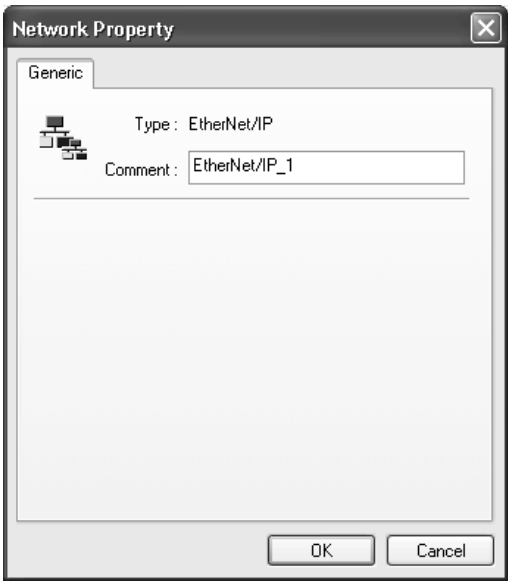
The Main Window consists of a Hardware List and a Network Configuration Window, as shown in the following diagram.



When two or more networks are being managed, a new Network Configuration Window can be added by selecting ***Network - Add***.



To change the name displayed in the Network Tab Page, select ***Network - Property***. The name set in the *Comment* Field of the Network Property Window can be changed.



6-2-2 Tag Data Link Setting Procedure

The section describes the procedure for setting tag data links (i.e., connection information).

For data links between PLCs, the connection information is set only in the originator, i.e., the node that receives data.

1. Creating a Network Configuration
   Register all EtherNet/IP Units or built-in EtherNet/IP ports for which connections will be created in the EtherNet/IP Network Configuration Window. (Refer to *6-2-3 Registering Devices*.)

Note If a system has already been installed, connect online to the EtherNet/IP network and upload the network configuration. (Refer to *6-2-11 Uploading Tag Data Link Parameters*.)

↓

2. Creating Connections

Set the connections using one of the following methods.

1) Basic Operation

1-1) Create tags and tag sets for all registered devices (EtherNet/IP Unit or built-in port). (Refer to *6-2-4 Creating Tags and Tag Sets*.)

1-2) Create a connection for the originator device (i.e., registered device that receives data as input data). (Refer to *6-2-5 Connection Settings*.)

2) Generating a Connection Using the EtherNet/IP Datalink Tool (Refer to *6-2-5 Connection Settings*.)
The EtherNet/IP Datalink Tool is used to create data links between PLCs by specifying I/O memory addresses in the same manner as for Controller Link. The following functions can be used with Network Configurator version 3.10 or higher.

3) Creating Connections Using the Wizard (Refer to *6-2-7 Creating Connections Using the Wizard*.)
Create connections between OMRON PLCs following the instructions. Tags and tag sets must be set for all devices before starting the Wizard. (Refer to *Basic Operation 1-1*.)

Note Select ***Device - Parameters - Wizard*** from the menus to start operation.

4) Creating Connections by Dragging and Dropping Registered Devices (Refer to *6-2-8 Creating Connections by Device Dragging and Dropping*.)
When a target device is dragged and dropped to the originator device, the Edit Connection Dialog Box will be displayed, and a connection can be created. OMRON EtherNet/IP Units or built-in EtherNet/IP ports are the only originator devices for which connections can be created in this way.

↓

Downloading Tag Data Link Parameters (Refer to *6-2-10 Downloading Tag Data Link Parameters*.)

↓

Check that tag data links are operating correctly by using the indicators on the EtherNet/IP Unit (refer to *18-2 Using the LED Indicators and Display for Troubleshooting* for Troubleshooting) and the Network Configurator monitor function (refer to *18-1 Checking Status with the Network Configurator*).

↓

Check that the output tag data is updated in the input tag by using the CX-Programmer's Watch Window or PLC memory function.

Note Refer to the *CX-Programmer Operation Manual* (Cat. No. W446) for the operating procedures.

Note Use the tag data link functions of the CJ2M-CPU3□ after sufficiently confirming that the communication specifications are suitable for the application because the specifications differ from those of the CS1W/CJ1W-EIP21S, CS1W/CJ1W-EIP21, CJ2H-CPU6□-EIP, and CJ3M-CPU3□.

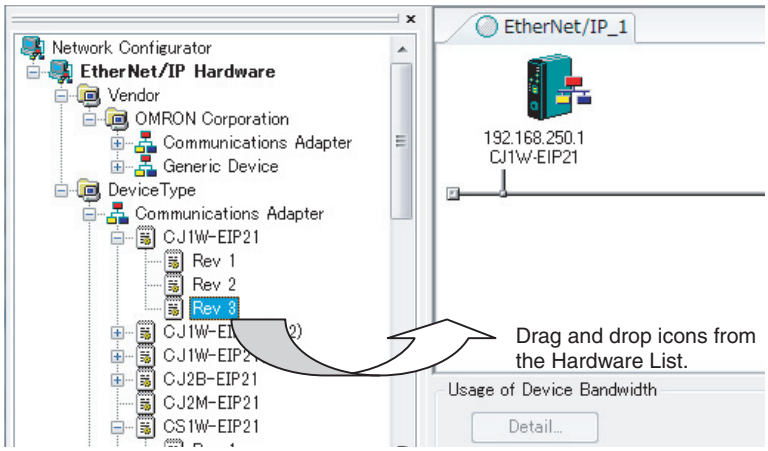
Refer to *2-1-3 Communications Specifications* for the communications specifications.

Note If the tag data links are performed with a device that do not have EDS files, use the Generic Device to make the settings.
Refer to *Appendix K Tag Data Link Settings with Generic Devices* for information on how to make the settings with the Generic Device.

6-2-3 Registering Devices

Register all of the devices required in the equipment (such as EtherNet/IP Units performing tag data links) as a network configuration.

1,2,3... 1. Register the devices that will participate in the tag data links by dragging the devices from the Hardware List and dropping them in the Network Configuration Window. (To drag and drop an icon, click and hold the left mouse button over the icon, move the icon to the destination, and release the mouse button.)
The icon will be displayed in the Network Configuration Window, as shown in the following diagram.



Hardware List

Name in hardware list	CIP revision	EtherNet/IP Unit
CJ2B-EIP21	Rev. 2 or 3	Built-in EtherNet/IP port on CJ2H CPU Unit (CJ2H-CPU□□-EIP)
CJ2M-EIP21	Rev. 2	Built-in EtherNet/IP port on CJ2M CPU Unit (CJ2M-CPU3□)
CJ1W-EIP21	Rev. 1, 2 or 3	CJ1W-EIP21 EtherNet/IP Unit connected to CJ1/CP1H CPU Unit
CS1W-EIP21	Rev. 1, 2 or 3	CS1W-EIP21 EtherNet/IP Unit connected to CJ1 CPU Unit
CJ1W-EIP21 (CJ2)	Rev. 2 or 3	CJ1W-EIP21 EtherNet/IP Unit connected to CJ2/CJ3 CPU Unit
CJ1W-EIP21S	Rev. 4	CJ1W-EIP21S EtherNet/IP Unit connected to CJ1/CP1H CPU Unit
CS1W-EIP21S	Rev. 4	CS1W-EIP21S EtherNet/IP Unit connected to CS1 CPU Unit

Name in hardware list	CIP revision	EtherNet/IP Unit
CJ1W-EIP21S (CJ2)	Rev. 4	CJ1W-EIP21S EtherNet/IP Unit connected to CJ2/CJ3 CPU Unit
CJ3M-CPU3□	Rev. 4	Built-in EtherNet/IP port on CJ3 CPU Unit (CJ3M-CPU3□)

Note (1) The following table shows the relation between the CIP revision and the unit version.

CS1W-EIP21, CJ1W-EIP21, and CJ2H-CPU□□-EIP

Unit version	CIP revision
Ver. 1.0	Revision 1.01
Ver. 2.0	Revision 2.01 to 2.03
Ver. 2.1	Revision 2.04 or 2.05
Ver. 3.0	Revision 3.01

CS1W-EIP21S/CJ1W-EIP21S

Unit version	CIP revision
Ver. 1.0	Revision 4.01

CJ2M-CPU3□

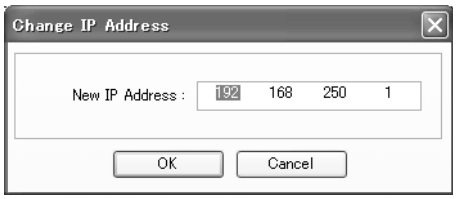
Unit version	CIP revision
Ver. 2.0	Revision 2.01
Ver. 2.1	Revision 2.02 or 2.03

CJ3M-CPU3□

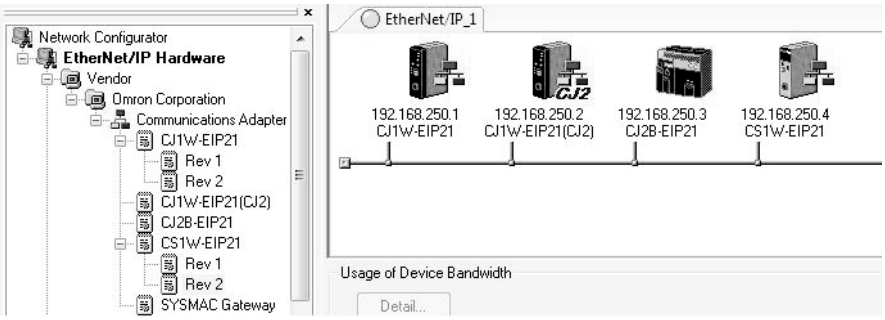
Unit version	CIP revision
Ver. 1.1	Revision 4.02

(2) When mounting the CJ1W-EIP21/CJ1W-EIP21S to a CJ2/CJ3 CPU Unit, select CJ1W-EIP21(CJ2)/CJ1W-EIP21S(CJ2) from the Hardware List.

2. Click the right mouse button over the registered device's icon to display the pop-up menu, and select ***Change Node Address***.



3. Set the IP address to match the node address (IP address) actually being used in the device.
4. Repeat steps 1 to 3, and register all of the devices participating in the tag data links.



6-2-4 Creating Tags and Tag Sets

Specifying I/O Memory Addresses

The tag sets and set member tags required to create connections for a registered EtherNet/IP Unit must be created. The I/O memory addresses or network symbols that are used in the control programs can be set for the tags. This section first describes the basic procedure for creating tags and tag sets for using the Network Configurator's device parameter editing function.

1. Creating Tags and Tag Sets Using the Network Configurator's Device Parameter Editing Function

Next, the following two procedures, which can be used to effectively use network symbols in tags, are described.

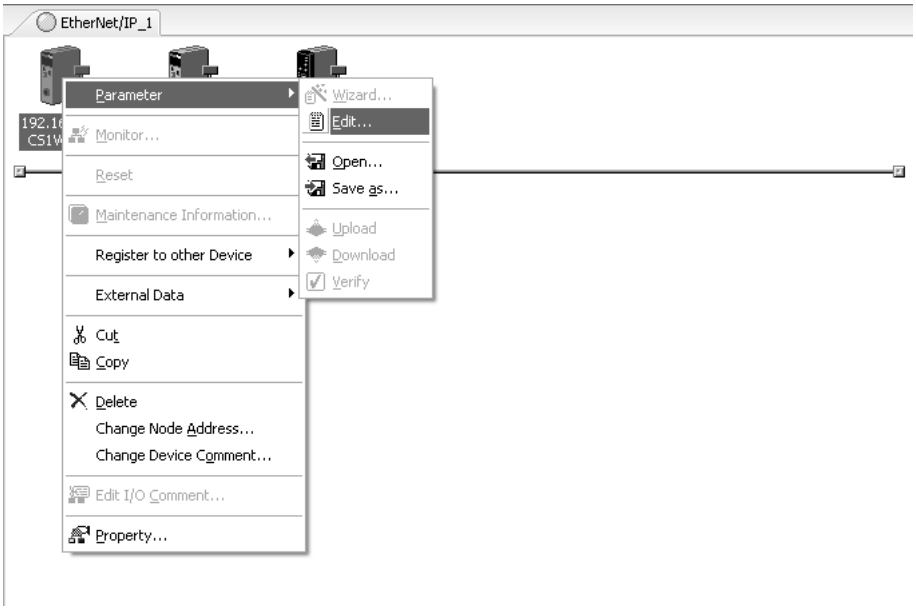
2. Importing Network Symbols Created with the CX-Programmer to the Network Configurator
3. Importing Network Symbols That Were Registered to Tags with the Network Configurator to the CX-Programmer

1. Creating Tags and Tag Sets Using the Network Configurator's Device Parameter Editing Function

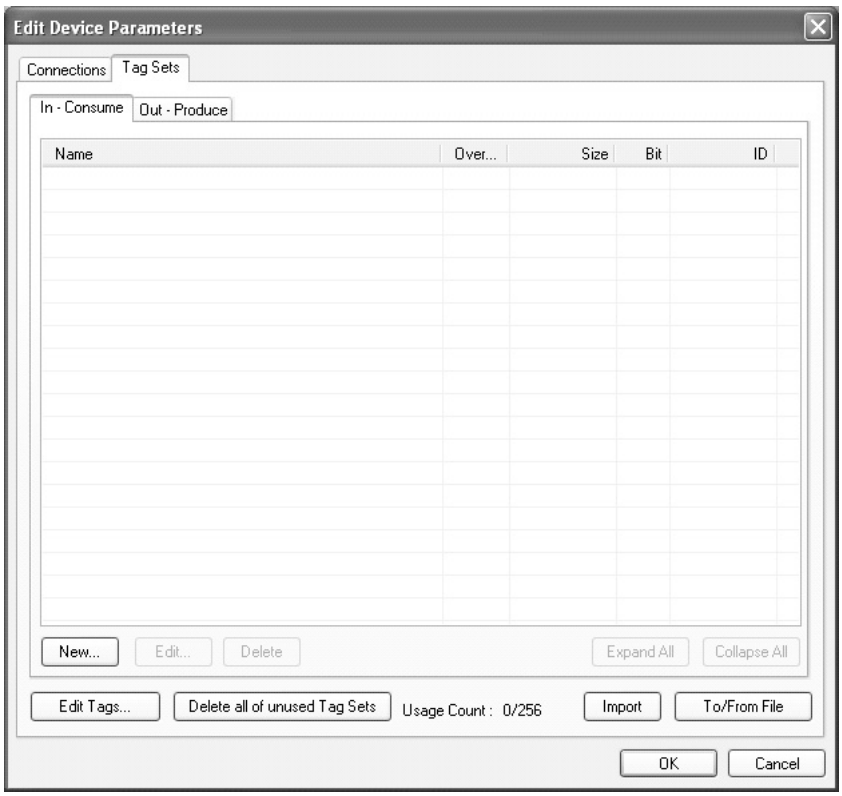
Note The network symbols are supported by the CJ2 CPU Units of CJ2H-CPU6□(-EIP) with unit version 1.6 or later, CJ2M-CPU□□ with unit version 2.2 or later, and CJ3M-CPU3□.

Creating a Tag Set

1,2,3... 1. Double-click the icon of the device (for which a tag set is being created) to display the Edit Device Parameters Dialog Box. Right-click the icon to display the pop-up menu, and select ***Parameter - Edit***.

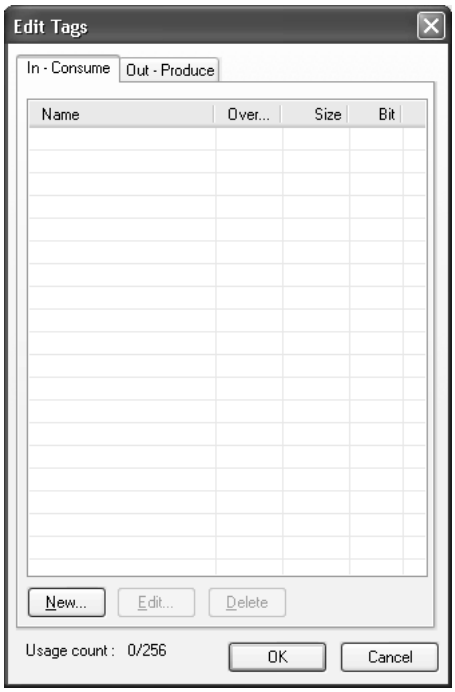


2. Click the **Tag Sets** Tab at the top of the Edit Device Parameters Dialog Box. There are two kinds of tag sets: input (consume) and output (produce).

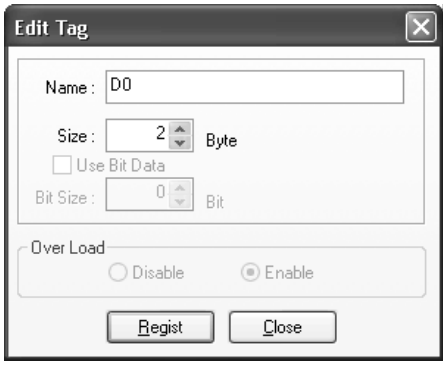


Creating and Adding Tags

3. Click the **Edit Tags** Button. The Edit Tags Dialog Box will be displayed. Register the input (consume) tags and output (produce) tags separately.



4. Click the **In - Consume** Tab, and click the **New** Button. The Edit Tag Dialog Box will be displayed.



5. In the Name Field, enter the character string for the CPU Unit's I/O memory address or a network symbol (e.g., 100, W100, D0, Input_signal). Addresses in the following I/O memory areas can be set.

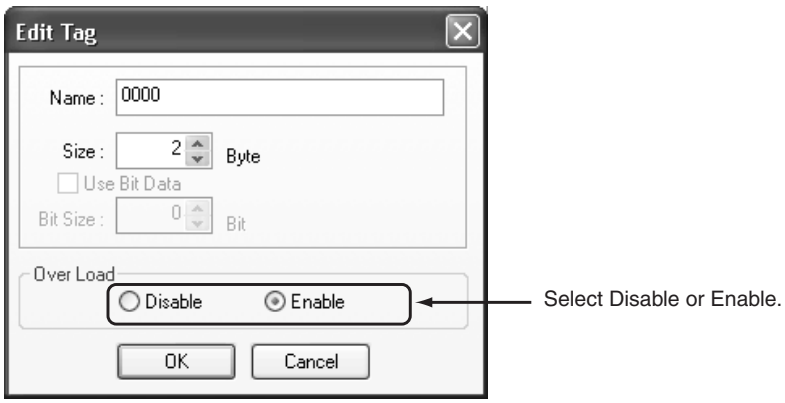
CPU Unit's data area		Address (Text to input in *Name* Field.)
CIO Area		0000 to 6143
Holding Area		H000 to H511
Work Area		W000 to W511
DM Area		D00000 to D32767
EM Area	Bank 0 hex	E0_00000 to E0_32767
	⋮	⋮
	Bank 18 hex	E18_00000 to E18_32767

Note (a) The H, W, D, and E characters can also be input in lower case as h, w, d, and e.

(b) Be sure to directly enter the CPU Unit's I/O memory address (e.g., 100, W100, D0) or a network symbol as a character string.

6. Input the size of the tag in the *Size* Field, in bytes.
7. Click the **Regist** Button to register the tag.

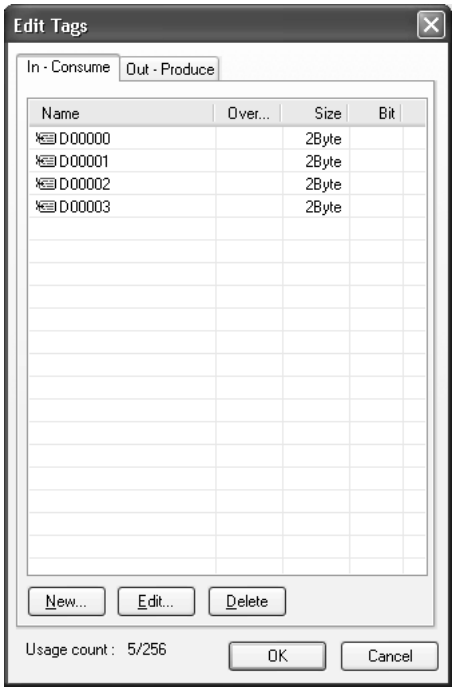
   If an I/O memory address is specified for a tag name, the Edit Tags Dialog Box will be displayed with the next consecutive address as the tag name for editing the next tag. Once you have registered the tags, click the **Cancel** Button.
8. Click the **Out - Produce** Tab, and click the **New** Button. The Edit Tag Dialog Box will be displayed, like the dialog box for input tags, except for the *Over Load* setting. The *Over Load* setting determines whether outputs are cleared or continue their previous status when outputs are turned OFF with the PLC's Output OFF function. Output inhibit settings are not required for input (reception) tag sets.
   - Follow the output inhibit function: Enabled (default)
     Output data is cleared to 0 when a PLC output inhibit occurs.
   - Do not follow the output inhibit function: Disabled
     Output data maintains its previous status even after a PLC output inhibit occurs.



Note When any of the following errors occurs in the originator PLC while tag data links are in progress, the connection will be forcibly disconnected.

- Fatal CPU Unit error
- I/O refreshing error
- CPU Unit WDT error
- I/O bus error

9. When you are finished registering the required tags, click the **OK** Button at the bottom of the Edit Tags Dialog Box.



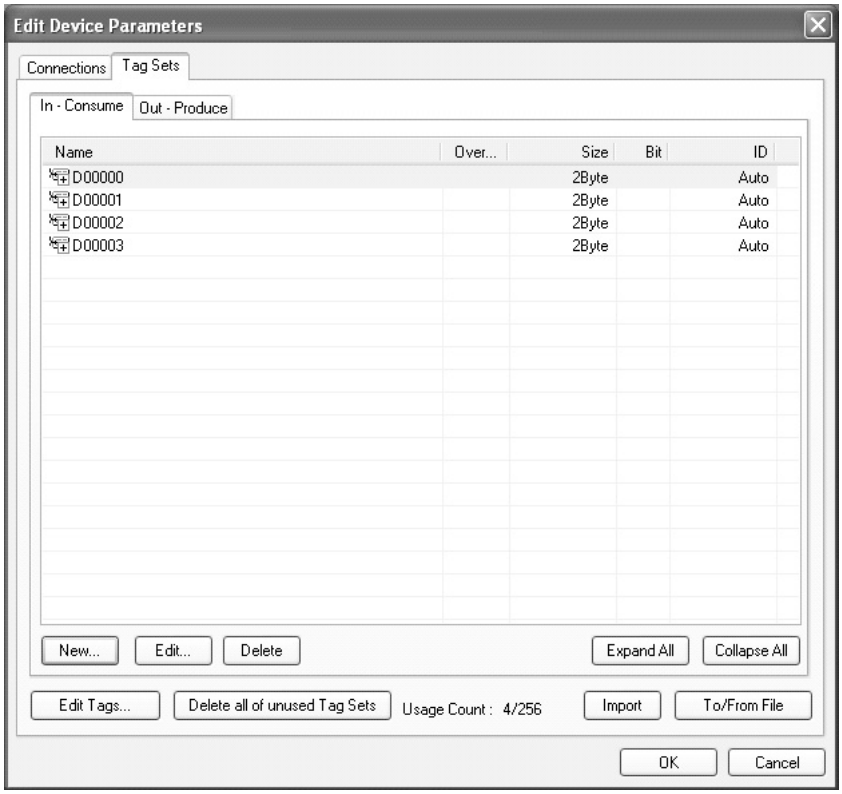
10. At this point, a confirmation dialog box will be displayed to check whether the registered tag names will registered without changes as tag sets. A tag set can contain up to 8 tags, but tag sets will be registered with one tag per tag set if the tags are registered as tag sets. In this case, the **Yes** Button is clicked to register one tag per tag set.



If the **No** Button is clicked, more tags can be registered at the end of the tag set. Refer to step 18 for details on adding tags to the end of the tag set.

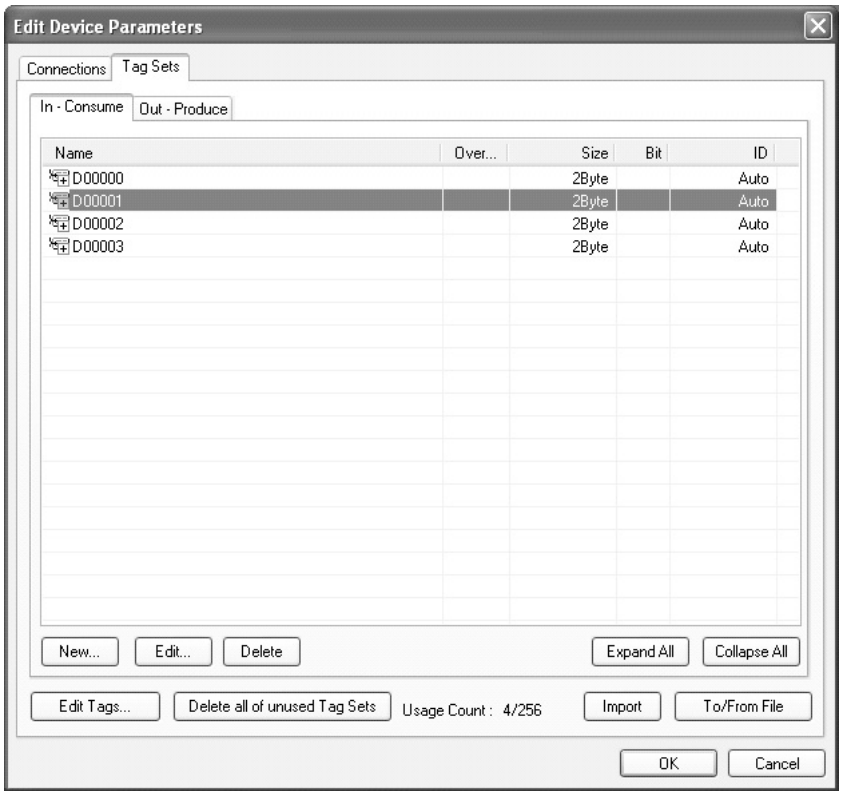
Changing and Registering Tag Sets

11. The following dialog box will be displayed when the tags in the Edit Tags Dialog Box are registered directly as tag sets.



12. If an input tag has already been registered in an input tag set, and you want to change its registration to a different input tag set, it is necessary to delete the tag from the tag set in which it was originally registered.

Open the Edit Device Parameters Dialog Box, select the tag set containing the tag that you want to delete, and click the **Delete** Button in the Edit Tag Dialog Box. (If there are other tags registered in that tag set, it is possible to delete just one tag by selecting the tag that you want to delete in the Edit Tag Set Dialog Box and clicking the Button.)

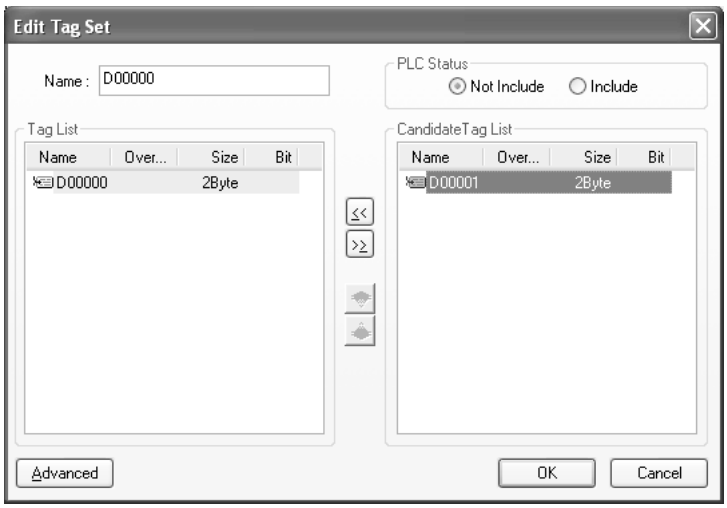


At this point, a confirmation dialog box will be displayed to confirm that you want to delete the selected tag set and the tags contained in that tag set.



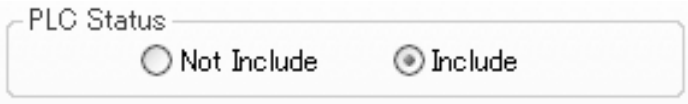
If the **No** Button is clicked, only the tag set will be deleted. Click the **No** Button.

13. In order to edit a registered tag set and add tags, either double-click the tag set, or select the tag set and click the **Edit** Button. The Edit Tag Set Dialog Box will be displayed.



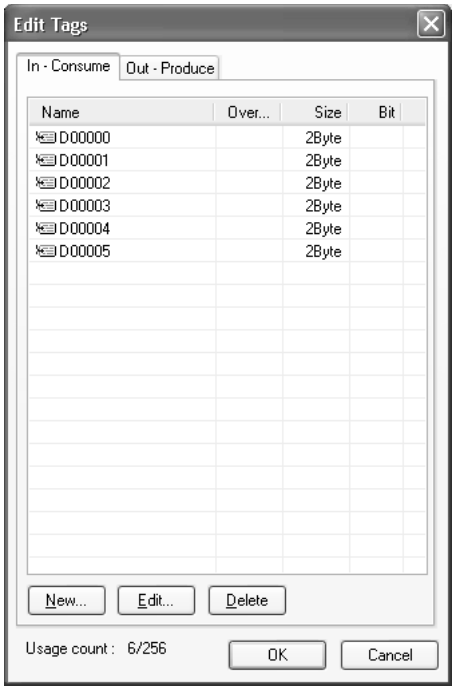
The *Tag List* on the left side of the dialog box shows the tags that are already registered, and the *Candidate Tag List* on the right side of the dialog box shows the other tags that have not been registered yet. To add a tag, select it in the *Candidate Tag List* and click the << Button.

14. When the PLC status is being included in the tag set, select the *Include* Option at the upper-right corner of the dialog box.



15. If you want to change the tag set's name, it can be changed in this dialog box.
16. To save the changes, click the **OK** Button at the bottom of the Edit Tag Set Dialog Box.
17. Click the **OK** Button at the bottom of the Edit Device Parameters Dialog Box.

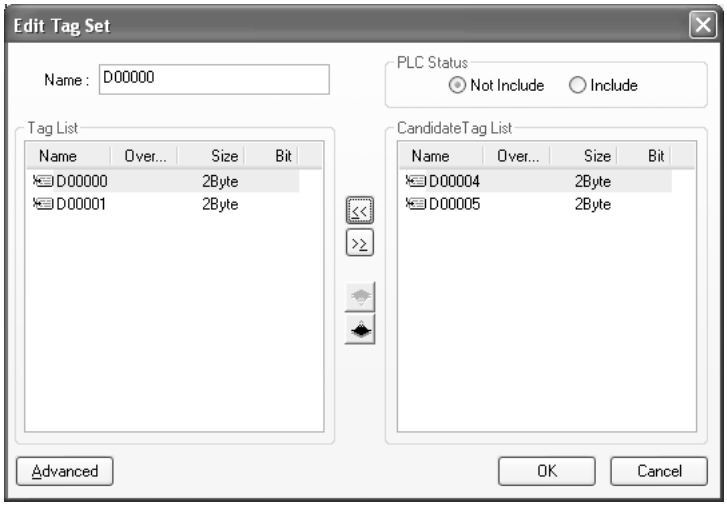
18. If you want to just add new tags and register the tag set, first register the tags with steps 1 to 9. In this example, input tags D00004 and D00005 have been newly added.



19. When you are finished registering the required tags, click the **OK** Button at the bottom of the Edit Tags Dialog Box.
20. At this point, a confirmation dialog box will be displayed to check whether the registered tag names will be registered without changes as tag sets. Tags are just being added in this case, so click the **No** Button. Just the tags will be registered, without registering the tags as tag sets.

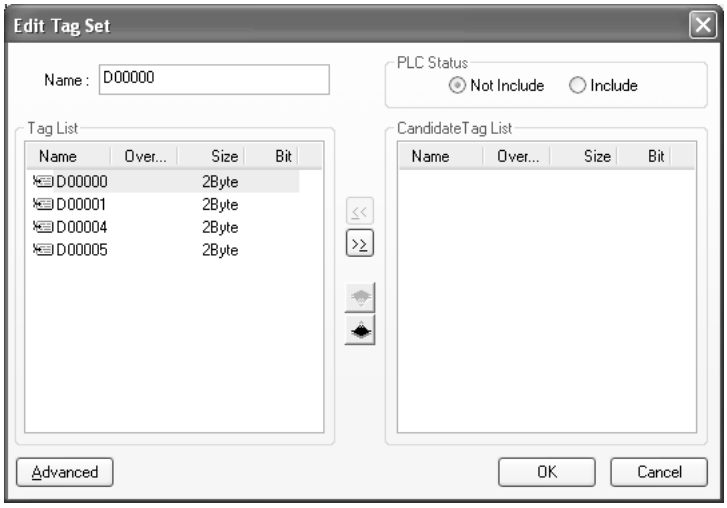


21. To register the newly added tags in a tag set, either double-click the desired tag set, or select the tag set and click the **Edit** Button.



The *Tag List* on the left side of the dialog box shows the tags that are already registered, and the *Candidate Tag List* on the right side of the dialog box shows the other tags that have not been registered yet.

22. Select the tags that you want to add from the *Candidate Tag List* and click the Button.



Up to 8 tags can be registered in a tag set, or up to 7 tags can be registered and two byes will be added to the size if the PLC status is included in the tag set.

23. To confirm the changes, click the **OK** Button at the bottom of the Edit Tag Set Dialog Box.
24. Click the **OK** Button at the bottom of the Edit Device Parameters Dialog Box.

2. Importing Network Symbols Created with the CX-Programmer to the Network Configurator

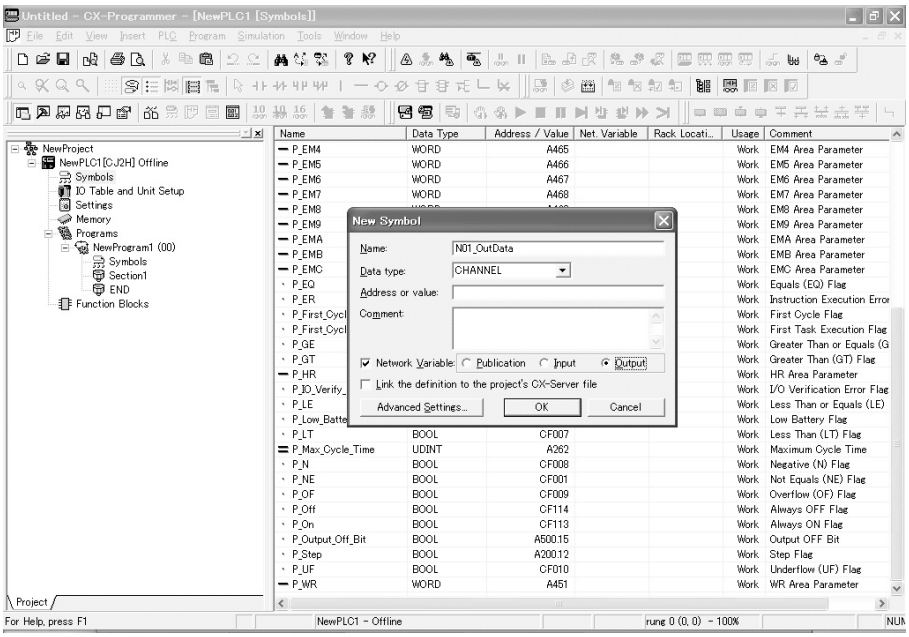
You can create network symbols using the CX-Programmer, import them into the Network Configurator, and then create tags and tag sets. Use the following procedure.

Note This function is supported by the CJ2 CPU Units of CJ2H-CPU6□(-EIP) with unit version 1.6 or later, CJ2M-CPU□□ with unit version 2.2 or later, and CJ3M-CPU□□.

Creating Global Symbols

Create global symbol with the Global Symbol Editor of the CX-Programmer and select *Input* or *Output* for the network variable properties. Safe the project when you are finished.

Any global symbols with *Input* or *Output* set for the network variable property will be imported when the import procedure is performed from the Edit Device Parameters Dialog Box.

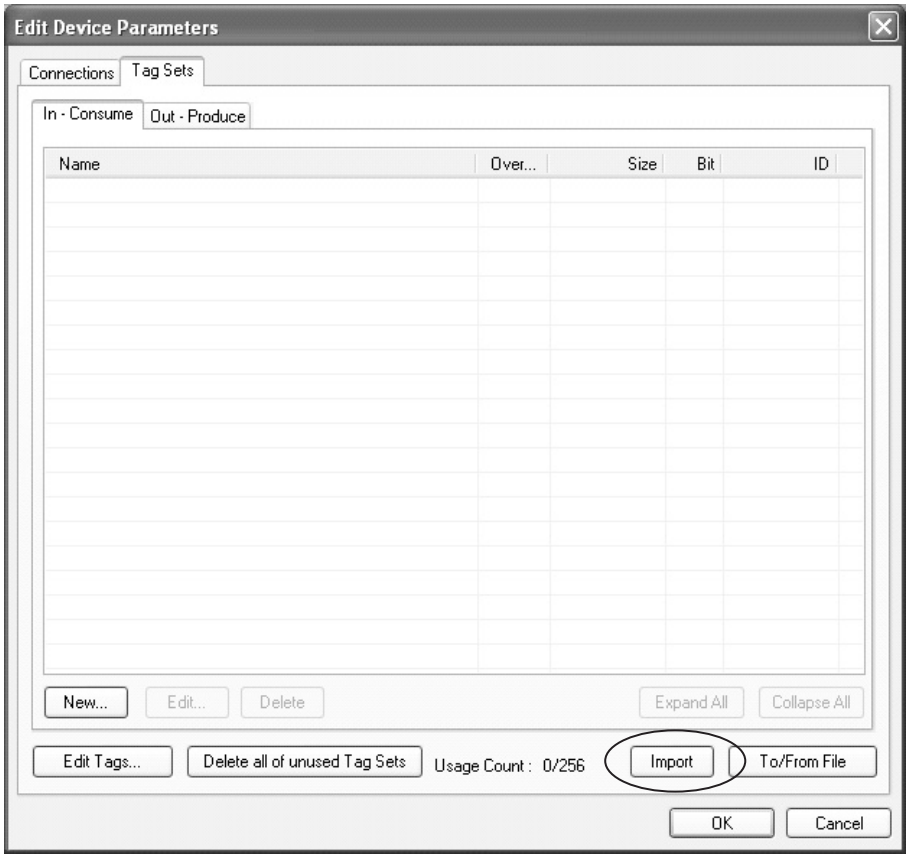


Importing Symbols to the Network Configurator

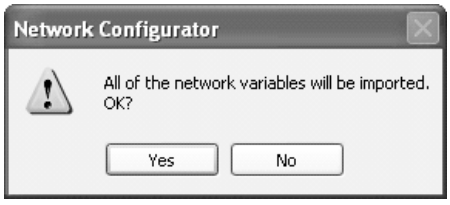
1,2,3... 1. Start the CX-Programmer and open the project that was saved.

Note When multiple copies of the CX-Programmer are running at the same time, it is possible to import only from the CX-Programmer project that was started first. If the global symbols that are to be imported are stored in multiple CX-Programmer project files, the projects must be started one by one to import the symbols.

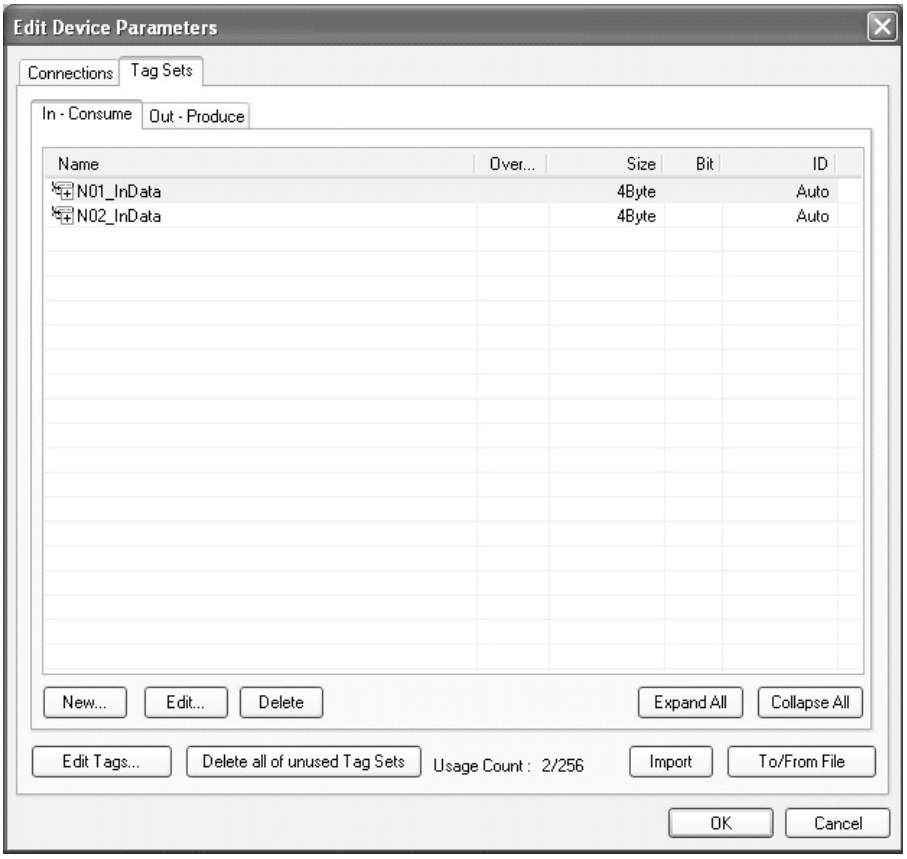
2. From the devices registered in the Network Configurator, double-click the icon of the device for which to import the network symbols. The Edit Device Parameter Dialog Box will be displayed. You can also right-click the icon and select ***Device - Parameters - Edit*** from the pop-up menu.
3. Click the **Import** Button on the Tag Sets Tab Page of the Edit Device Parameter Dialog Box.



A confirmation message will be displayed. Click the **Yes** Button.



The symbols will be imported as shown below on the Tag Sets Tab Page. Each symbol will be imported into a different tag set and the device parameters will be automatically edited. (The symbol name will be used for the tag set name.)



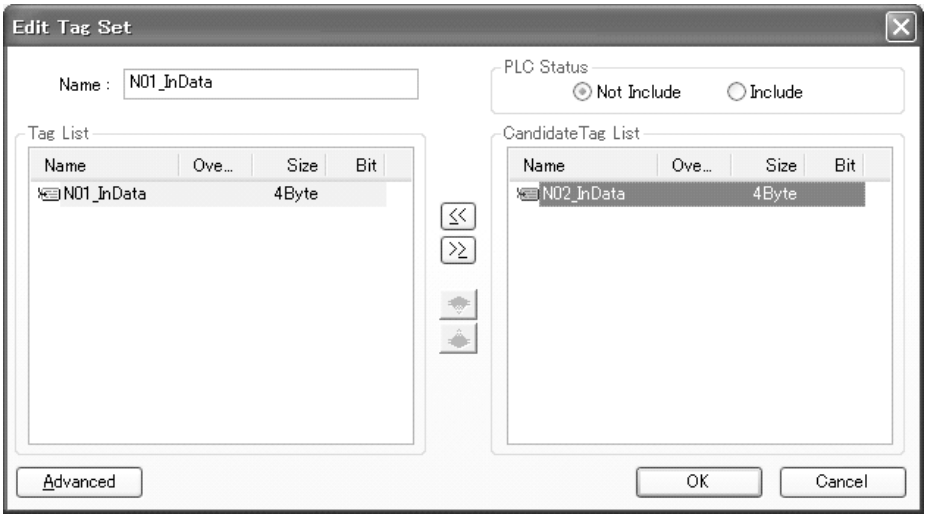
To place more than one input symbol (input tag) imported from the CX-Programmer into one tag set, you must delete the input tags that were registered to separate input tag sets.

Select the tag sets for the symbols that are included in the one tag set and click the **Delete** Button. A confirmation message will be displayed. Click the **No** Button to delete only the tag sets.



To create a new tag set for more than one tag, click the **New** Button. To place more than one tag in an existing tag set, double-click the tab set, or select it and click the **Edit** Button.

The Edit Tag Set Dialog Box will be displayed. Imported tags that are not registered in another tag set will be displayed in the Candidate Tag List Area on the right. Click the Right Arrow Button to add tags individually.



4. You can change tag set names in this dialog box. To confirm a change, click the OK Button in the dialog box.
5. Perform steps 1 to 3 for all the devices that will perform tag data links.

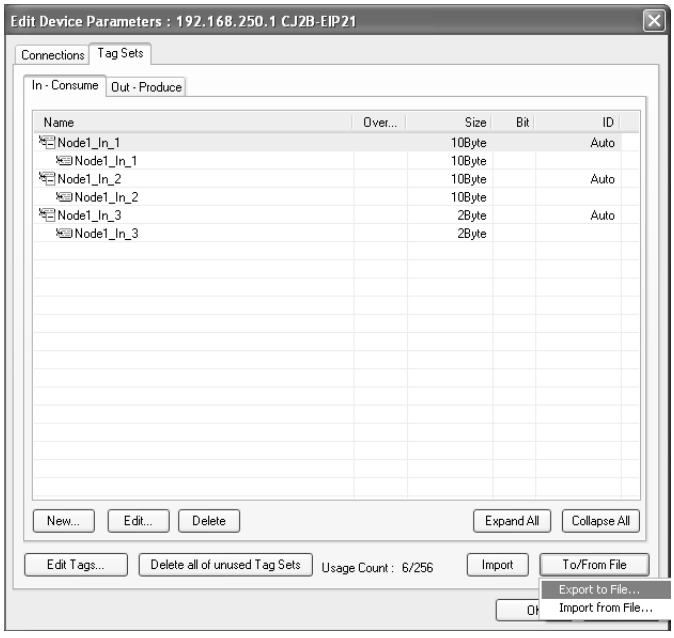
3. Importing Network Symbols That Were Registered to Tags with the Network Configurator to the CX-Programmer

You can specify network symbols for tags using the Network Configurator. The procedure to import network symbols that were created using the Network Configurator into the CX-Programmer is described below.

Note This function is supported by the CJ2 CPU Units of CJ2H-CPU6□(-EIP) with unit version 1.6 or later, CJ2M-CPU□□ with unit version 2.2 or later, and CJ3M-CPU□□.

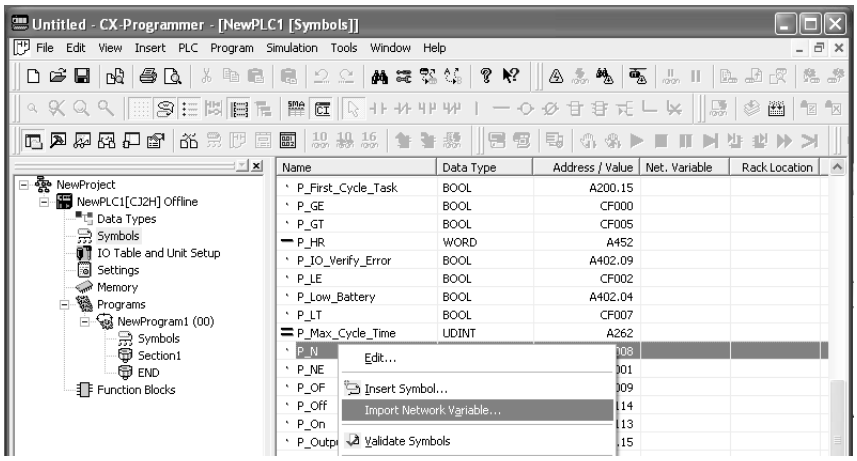
Exporting Tags and Tag Sets with the Network Configurator

1,2,3... 1. Select ***To/From File - Export to file*** on the Tag Sets Tab Page in the Edit Device Parameters Dialog Box to export the tag and tag set information to a CSV file.

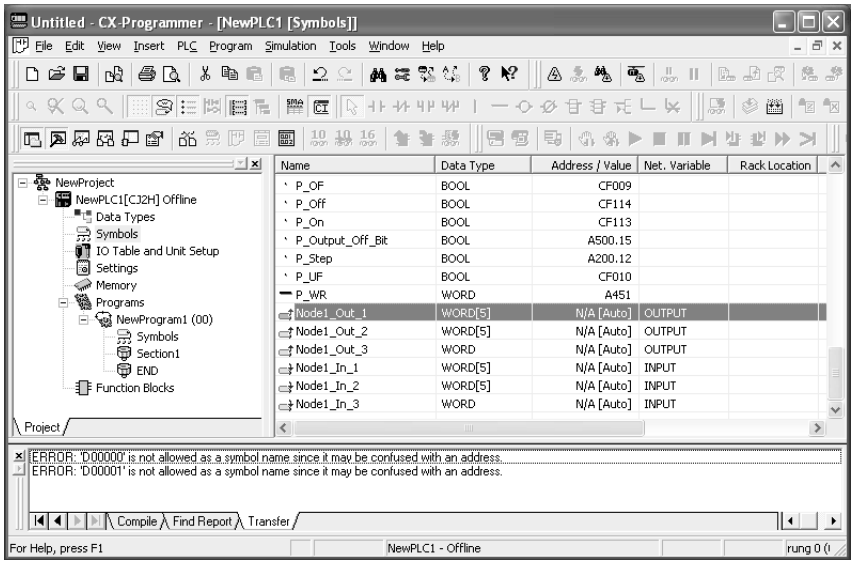


Importing the Tag and Tag Set CSV File with the CX-Programmer

1,2,3... 1. In the project global symbol table for a CPU Unit that can use network variables, right-click and select ***Import Network Variable*** from the pop-up menu.



2. You can add a tag as a network symbol by selecting and executing the CSV file exported using the Network Configurator.



Note The following precautions apply when importing.

- Tags that have a specified I/O memory address cannot be imported.
- Tags are imported as network symbols in a one-dimensional WORD array. To change the data type, use the Symbol Editor of the CX-Programmer.

6-2-5 Connection Settings

After creating the tag sets, click the **Connections** Tab at the top of the Edit Device Parameters Dialog Box, and set the following connection information.

- The target devices with which connections will be opened
- Whether the tag sets are input or output tag sets
- The length of the packet intervals (RPI)

Make the Connections settings in the originator only. The Connections settings are not necessary in the target device.

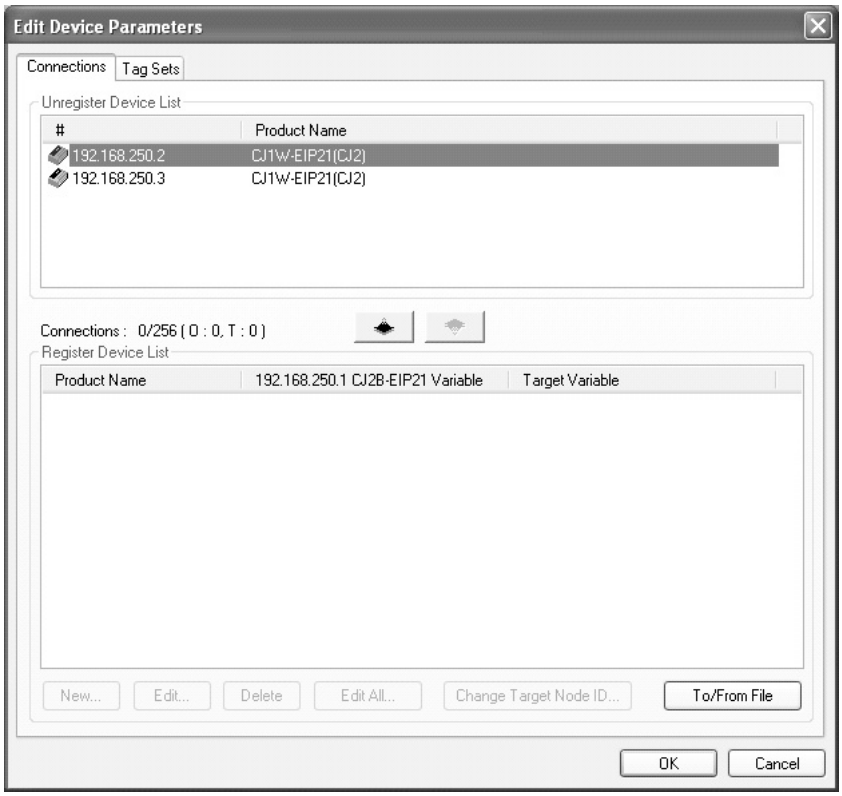
Note Make the Connections settings after creating tag sets for all of the devices involved in tag data links.

Connection Settings (Connections Tab)

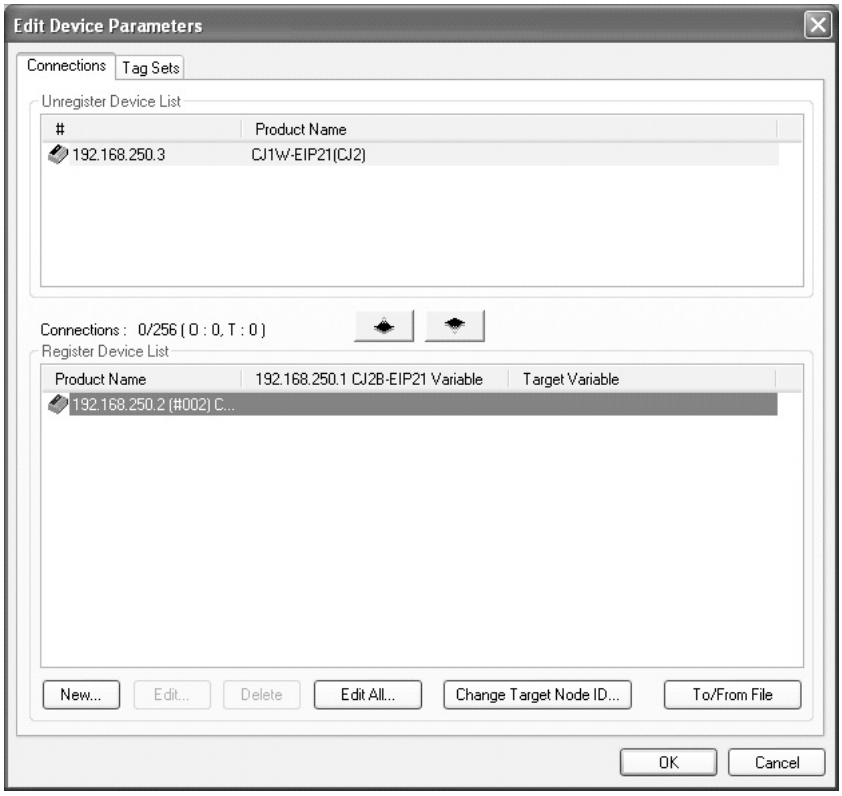
Registering Devices in the Register Device List

1,2,3...

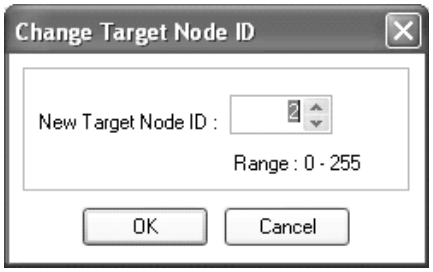
1. Display the originator device's Edit Device Parameters Dialog Box by double-clicking the device's icon in the Network Configuration Window, or right-clicking the device's icon and selecting ***Parameter - Edit*** from the pop-up menu.
2. Click the **Connections** Tab at the top of the Edit Device Parameters Dialog Box. All of the devices registered in the network (except the local node) will be displayed.



3. In the Unregister Device List, select the target device that requires connection settings by clicking the device so its color changes to gray, and click the Button. The selected target device will be displayed in the Register Device List, as shown in the following diagram.



4. Target node IDs are assigned to devices registered in the Register Device List. This target node ID determines the location in the originator node PLC of the Target Node PLC Operating Flag, Target Node PLC Error Flag, Registered Target Node Flag, and Normal Target Node Flag. By default, the target ID is automatically set to the rightmost 8 bits of the IP address. In the example above, the target device's IP address is 192.168.250.2, so the device number is #002. If a target node ID is duplicated and you want to change the device number, click the **Change Target Node ID** Button and change the target ID.



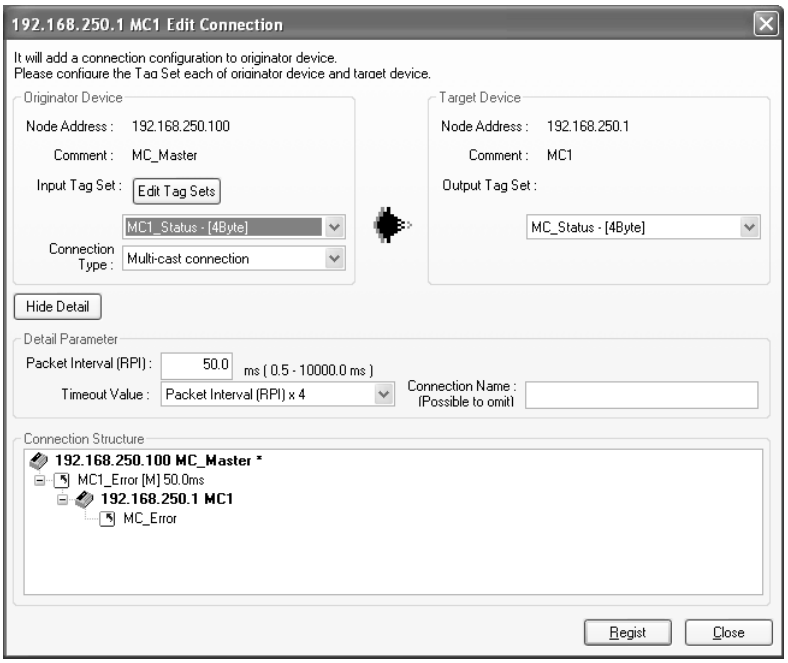
Editing Settings for Individual Connections

You can edit each connection separately.

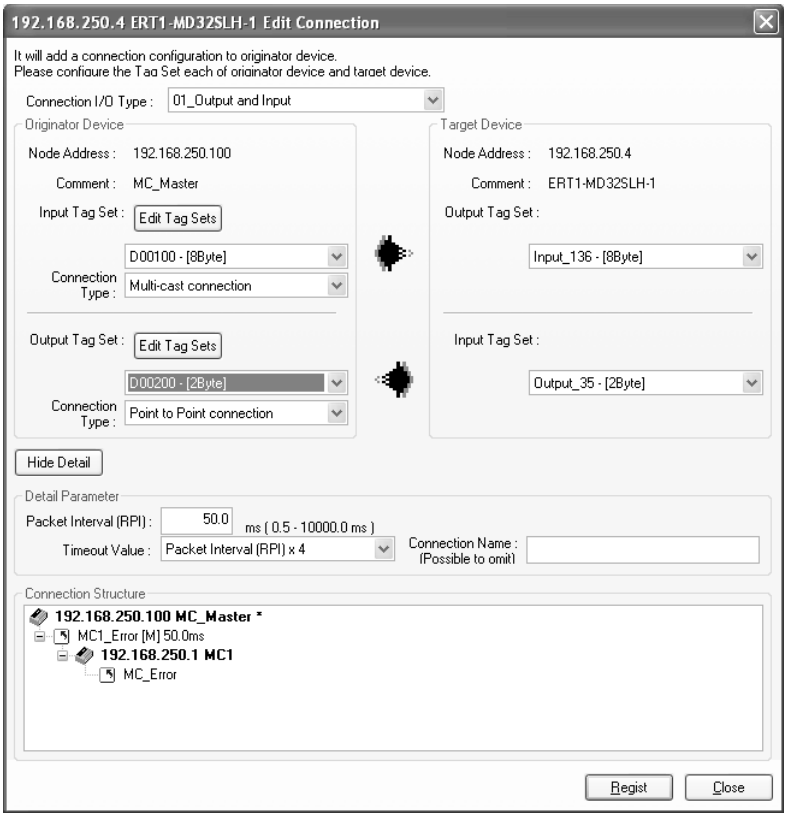
Note Refer to the following page for information on how to perform batch editing in a table format.

1,2,3... 1. Select the **Connection** Tab and then click the **New** Button.
The following Edit Connection Dialog Box will be displayed according to the type of device that is selected.

Using an OMRON EtherNet/IP Unit or Built-in EtherNet/IP Port as the Target



Using Other EtherNet/IP Devices as the Target



The settings are as follows:

Item	Description
Connection I/O Type	When creating tag data links for a CS1W-EIP21/EIP21S, CJ3M-CPU3□, CJ1W-EIP21/EIP21S, CJ2B-EIP21, or CJ2M-EIP21, select *Input Only (Tag Type)*. When creating tag data links for other target devices, select the connection I/O type specified in that device's EDS file. Use the *Input Only (ID type)* setting when another company's node is the originator and does not support connection settings with a Tag type setting.
Connection Type	Selects whether the data is sent in multicast or unicast (point-to-point). The default setting is multicast. • Multicast connection Select this type when the same data is shared by multiple nodes. This setting is usually used. • Point-to-Point connection Select this type when the same data is not shared by multiple nodes. In a unicast connection, other nodes are not burdened with an unnecessary load. **Note** Refer to *6-1-2 Overview of Operation* for details on using multicast and unicast connection as well as counting the number of connections.
The *Connection Structure* Field and the following items will not be displayed if the **Hide Detail** Button is pressed.	
Packet Interval (RPI)	Sets the data update cycle (i.e., the packet interval) of each connection between the originator and target. The interval can be set to between 1 and 10,000 ms for the CJ2M-EIP21 and 0.5 and 10,000 ms for other CPU Units in 0.5-ms increments. The default setting is 50 ms (i.e., data updated once every 50 ms).
Timeout Value	Sets the time until a connection times out. The timeout value is set as a multiple of the packet interval (RPI) and can be set to 4, 8, 16, 32, 64, 128, 256, or 512 times the packet interval. The default setting is 4 times the packet interval (RPI). The timeout value must be set so that the timeout will be 10 ms or longer.
Connection Name	Sets a name for the connection. (32 characters max.)

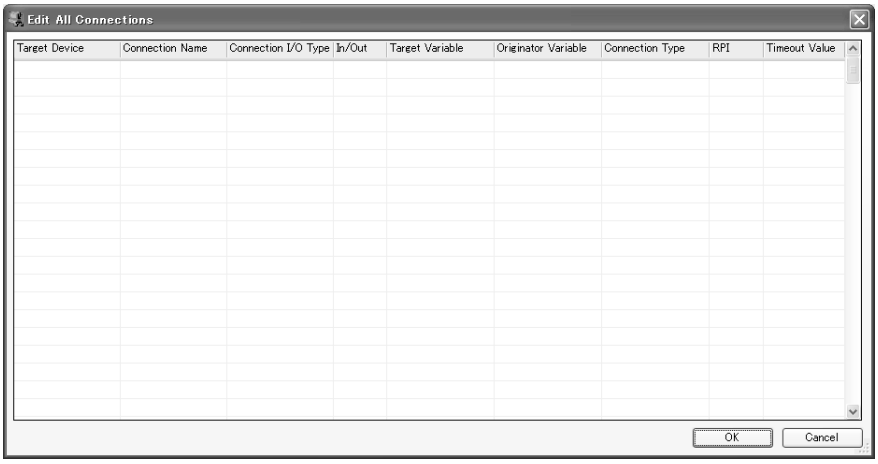
2. When the settings have been completed, press the **Regist** Button.

Connections Settings (Editing All Connections)

The connection settings between the originator and all of the target devices selected in the Register Device List can be edited together in a table.

1,2,3...

1. Select the **Connections** Tab, and click the **Edit All** Button. The following Edit All Connections Dialog Box will be displayed.



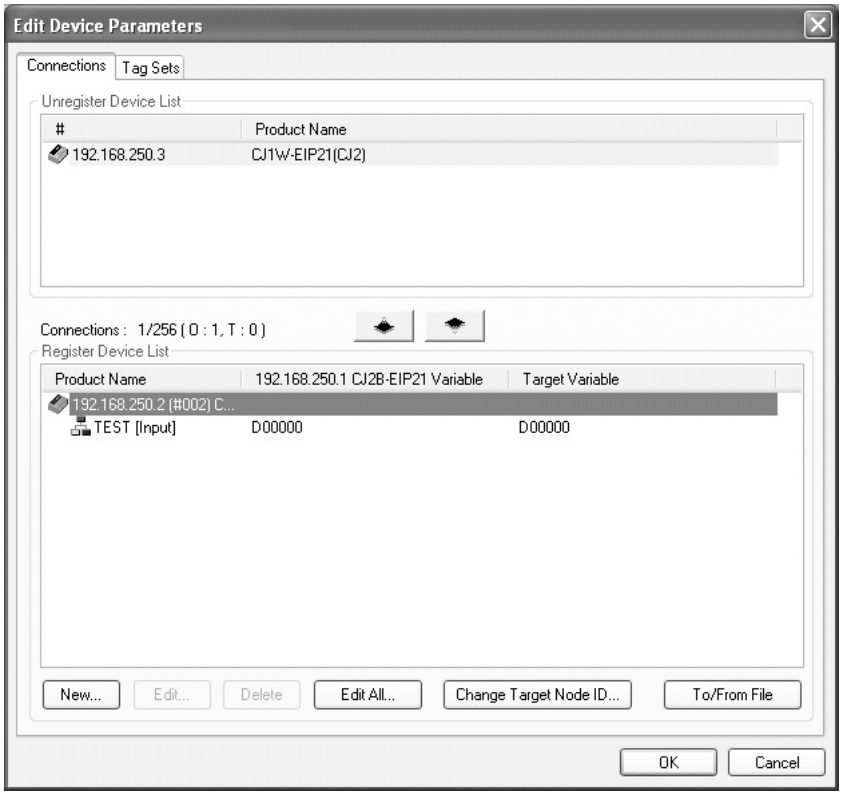
The following table describes the various settings in the dialog box.

Setting	Function
Target Device	Selects the target device.
Connection Name	Any name can be given to the connection (up to 32 characters). If this field is left blank, a default name will be assigned. This Connection Name can be used for comments.
Connection I/O Type	When making tag data links in a CS1W-EIP21/EIP21S, CJ3M-CPU3□, CJ1W-EIP21/EIP21S, CJ2B-EIP21, or CJ2M-EIP21, select ***Input Only (Tag type)***. When making tag data links in other devices, select the connection I/O type specified in that device's EDS file. Use the ***Input Only (ID type)*** setting when another company's node is the originator and does not support connection settings with the *Tag type* setting.
In/Out	The connections I/O is automatically displayed based on the selected connection. • Input Only: Just *In* is displayed.
Target Variable	Selects and allocates the target node's tag set. • In: Selects the target's output (produce) tag set. • Out: Selects the target's input (consume) tag set.
Originator Variable	Selects and allocates the originator node's tag set. • In: Selects the originator's output (produce) tag set. • Out: Selects the originator's input (consume) tag set.
Connection Type	Selects whether the data is sent in a multicast or unicast. The default setting is multicast. • Multicast connection: Select when the same data is shared by multiple nodes. This setting is usually selected. • Point-to-Point connection: Select when the same data is not being shared by multiple nodes. In a unicast transmission, other nodes are not burdened with an unnecessary load. **Note** Refer to *6-1-2 Overview of Operation* for details on using multicast and unicast transmissions, and counting the number of connections.
RPI	Sets the packet interval (RPI) of each connection between the originator and target. The interval can be set between 1 and 10,000 ms for the CJ2M-EIP21 and 0.5 and 10,000 ms for other CPU Units in 0.5-ms units. The default setting is 50 ms (data refreshed once every 50 ms).
Timeout Value	Sets the time until a connection timeout is detected. The time out value is set as a multiple of the packet interval (RPI) and can be set to a 4, 8, 16, 32, 64, 128, 256, or 512 multiple. The default setting is 4× the packet interval (RPI).

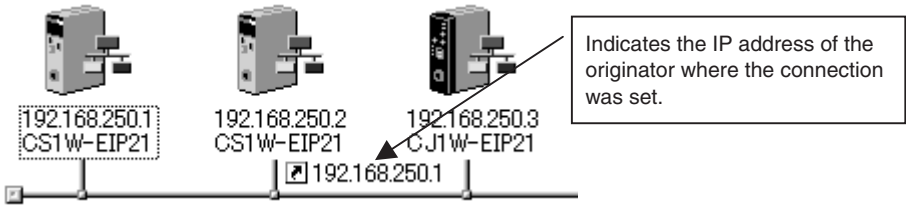
2. When the settings are completed, click the **OK** Button.

Confirming the Connections Settings

1,2,3... 1. An overview of the connections set in the Register Device List is displayed in the Connections Tab Page.



2. Click the **OK** Button. The following kind of diagram will be displayed.



3. Repeat the Connections setting procedure until all of the connections have been set.

Note After completing the settings, always click the **OK** Button before closing the Edit Device Parameters Dialog Box and performing another operation. If the **Cancel** Button is clicked and the dialog box is closed, the new settings will be discarded.

4. If the tag set's size is changed in either the originator or target after the connection was set, the size will not match the other node and a parameter data mismatch will occur. In this case, if the connection settings have been changed, be sure to check the connections. (*Refer to 6-2-17 Checking Connections.*)

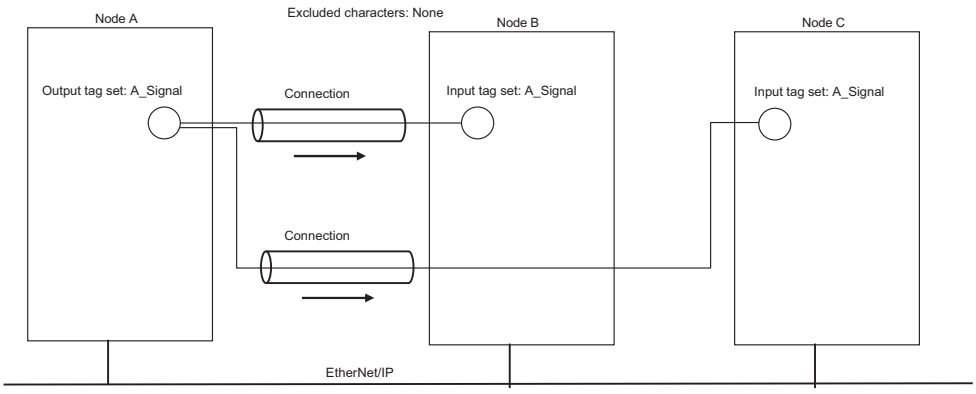
Automatically Setting Connections

Tag set names set for devices can be automatically detected to automatically set connections between input and output tag sets with the same name (or the same names excluding specified ellipses). Connections are automatically set under the following conditions.

Output tag set names	Except for specified ellipses, the output tag set name must be the same as the input tag set name. Ellipses can be set for the beginning or end of tag set names.
Input tag set names	Except for specified ellipses, the input tag set name must be the same as the output tag set name. Ellipses can be set for the beginning or end of tag set names.
Connection types	The connection type must be *Input Only*. Multicast and single cast connection types can be specified when executing a connection.
RPI	The default setting is used.
Timeouts	The default setting is used.

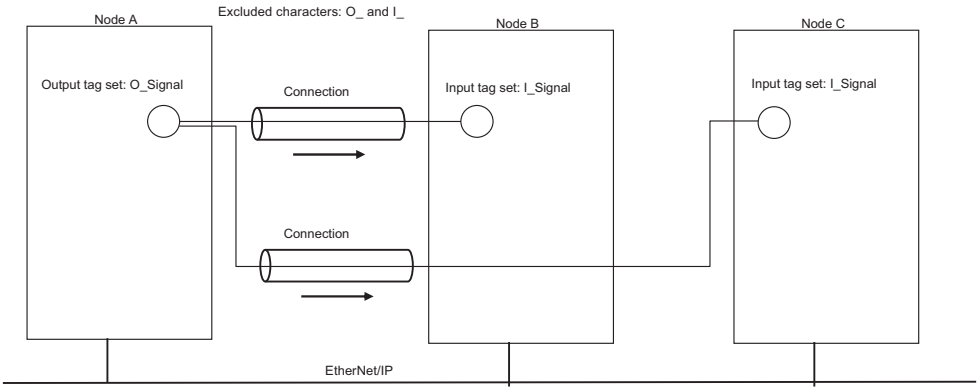
Example 1: Automatic Connections with the Same Tag Set Names

The following connections would automatically be set if there is an output tag set named A_Signal at node A and input tag sets named A_Signal at nodes B and C.



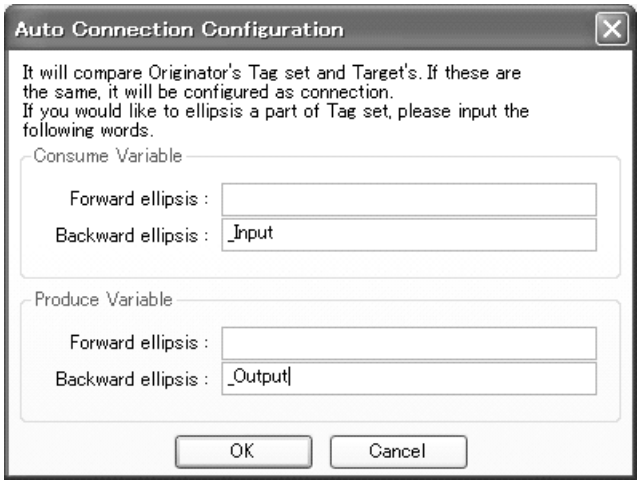
Example 2: Automatic Connections with the Ellipses

The following connections would automatically be set if there is an output tag set named O_Signal at node A and input tag sets named I_Signal at nodes B and C, and “O_” and “I_” were set as ellipses.



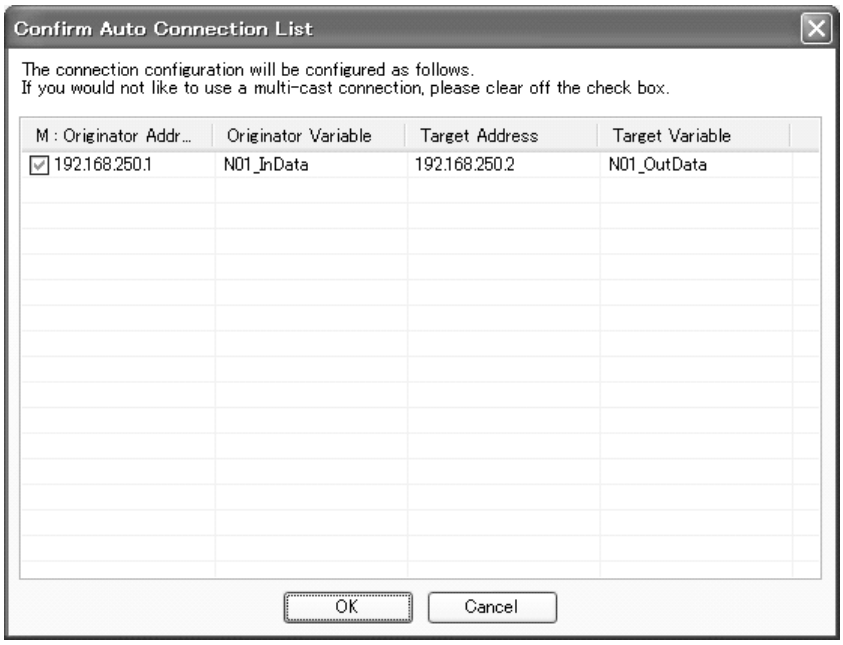
1,2,3... 1. Set the same tag set names for the output and input tag sets for the connection. The tag set names can also include forward and backward ellipses.

2. Select ***Auto Connection*** from the Network Menu. The connections will be set automatically.
   A dialog box will appear to set forward and backward ellipses for both output (product) and input (consume) tag sets as soon as automatic connection setting processing has begun.



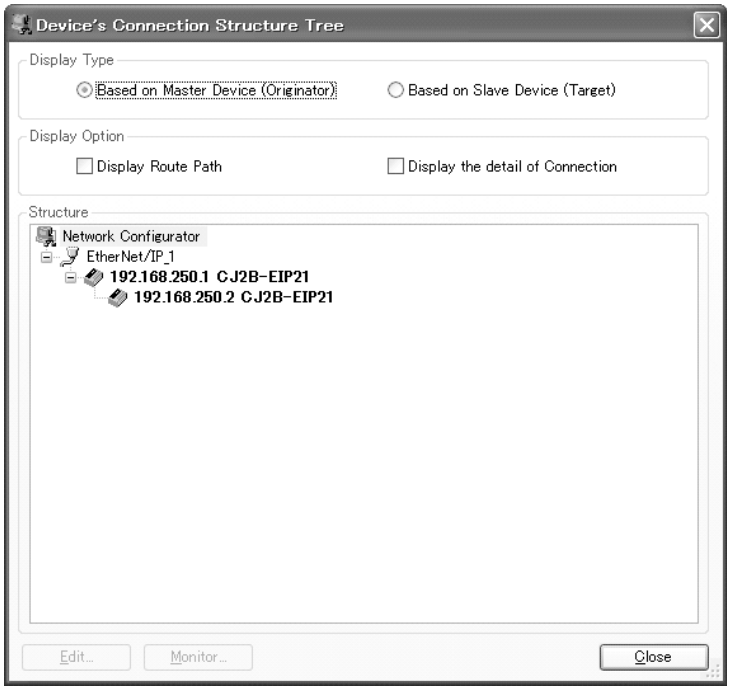
   Input the ellipses and click the **OK** Button. Automatic setting will be processed.

3. If there are tag sets that meet the conditions for automatic connection setting, they will be displayed.



Click the **OK** Button to start processing.

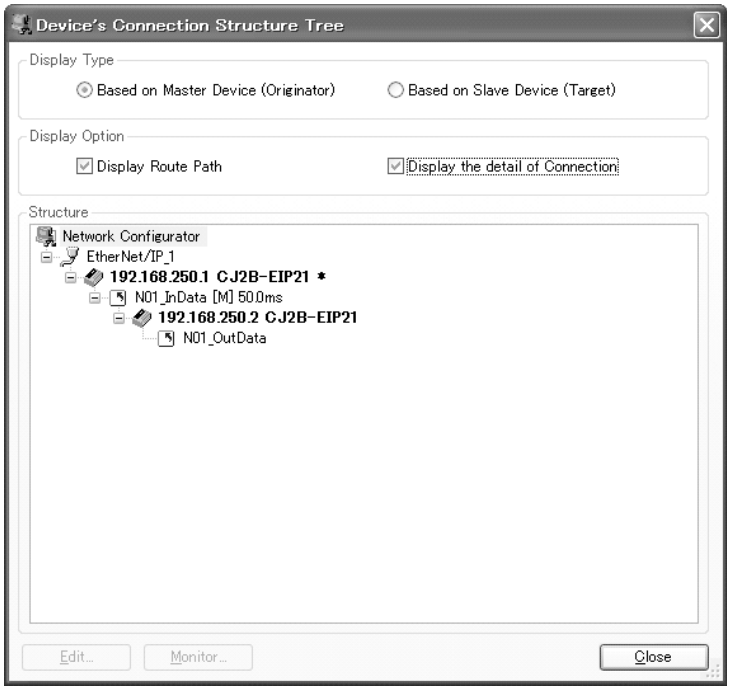
4. A device connection structure tree will be displayed when processing has been completed.



5. Use the device connection structure tree as required to change the RPI and timeout settings.

Device Connection Structure Tree

Connection settings can be displayed on the network configuration. Select ***View Device's Connection Structure Tree*** from the Network Menu.



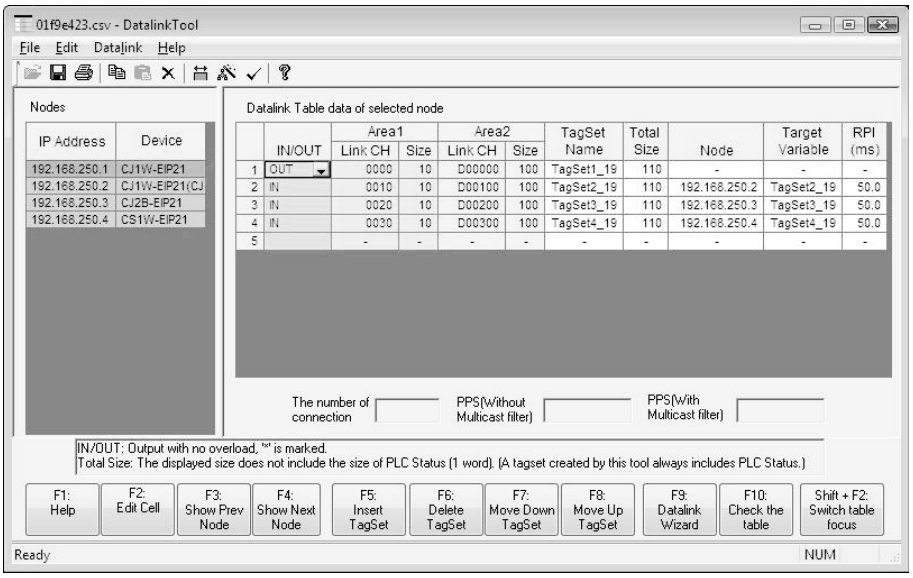
- The *Display the detail of Connection* Check Box can be used to switch between device-level and connection-level displays of tag data link communications.
- An asterisk will be displayed after the device name of the originator set for the connection.
- The Edit Device Parameters Dialog Box can be displayed by selecting a connection and clicking the **Edit** Button. The connections can be edited in this dialog box.

6-2-6 Setting Tags Using Data Link Tool

Using the EtherNet/IP Datalink Tool enables easily setting data links similar to those for the Controller Link by using only I/O memory addresses. This method has the following restrictions.

- Settings can be made only for tag data links between OMRON EtherNet/IP Units and built-in EtherNet/IP ports.
- Tags must be set using I/O memory addresses.
- A maximum of two tags (area 1 and area 2) can be set in one tag set.

Select ***Network - EtherNet/IP Datalink Tool*** from the menus in the Network Configurator after you have registered all the devices to start the EtherNet/IP Datalink Tool.



Node List

The following items will be displayed in the Node Area on the left side of the window.

- IP Address: The IP address of the node.
- Device: The name (model number) of the device at the node.

Note The node list will display the node registered in the Network Configurator. Nodes cannot be added or deleted from this window.

Data Link Table Information

The data link table of the node selected on the left will be displayed on the right. Each row specifies word that are allocated for data links for that node. Each row specifies the node settings for the words (area) where a data link has been created. You can set only area 1 or both area 1 and area 2.

- IN/OUT: Specifies whether the link inputs data to the node or outputs data from the node. *OUT* can be selected only once. Once *OUT* has been selected for one row, *IN* will automatically be selected for other rows. A asterisk will be displayed if the Over Load function is disabled. (See note.)

  Note The Over Load function is used to clear output data when all outputs are turned OFF from the CPU Unit of the PLC. This setting is not necessary for inputs.

  (a) Over Load function enabled: Output data will be cleared to all zeros when all outputs from the PLC are turned OFF from the CPU Unit.

  (b) Over Load function disabled: Output data will be maintained even when all outputs from the PLC are turned OFF from the CPU Unit.
- Area 1, Link CH: The I/O memory address of the first word in link area 1
- Area 1, Size: The number of words in link area 1. (See note.)
- Area 2, Link CH: The I/O memory address of the first word in link area 2
- Area 2, Size: The number of words in link area 2. (See note.)

  Note With the Network Configurator, the PLC status will be shown at the beginning of each area. The PLC status includes the CPU Unit operating status (operating information and error information).

- Tag Set Name: If the Wizard is used, the names will be automatically assigned using consecutive IP addresses in the following form for both input and output tags: TagSet1_192168.250.1. There is no reason to be concerned with these names. If the Wizard is not used, then names will not be automatically assigned and they must be entered directly into the data link table.
- Total Size: The total number of words in areas 1 and 2.
  If PLC status is included, the displayed value will be incremented by 1 word (Network Configurator 1.21 or higher). This value is automatically displayed after the sizes of areas 1 and 2 are entered.
- Node: For an input tag, this is the IP address of the node that provides the output. For an output tag, "-" will be entered automatically.
- Target Variable: The target tag set name. For an input tag, this is the name of the target set that provides the output. For an output tag, "-" will be entered automatically.
- RPI (ms): The requested packet interval for an input tag. For an output tag, "-" will be entered automatically.

Setting Procedure

The setting procedure is described here along with setting examples.

■ Setting Example A

Area 1 memory area = Work Area (W)

Area 1 start address = 0

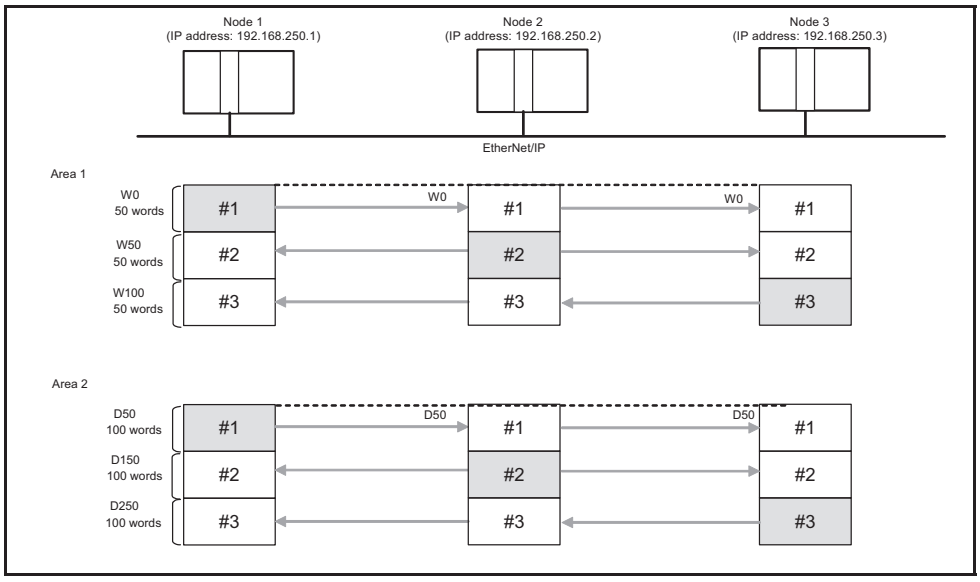
Area 1 size = 50 words

Area 2 memory area = DM Area (D)

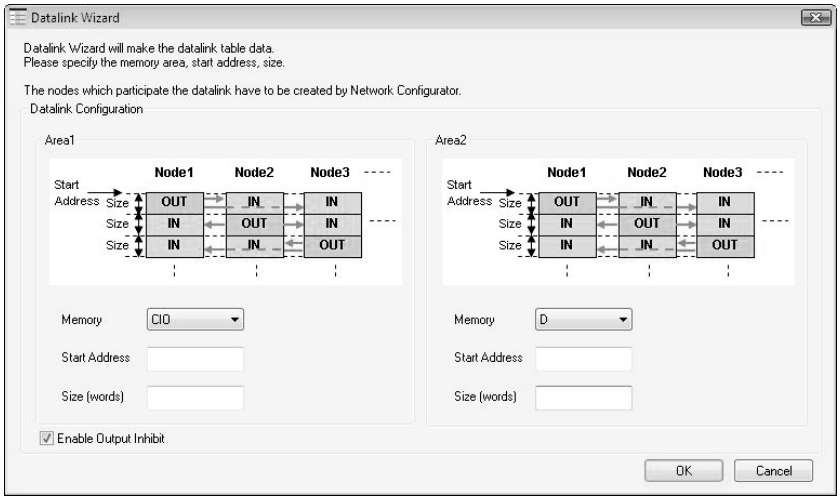
Area 2 start address = 50

Area 2 size = 100 words

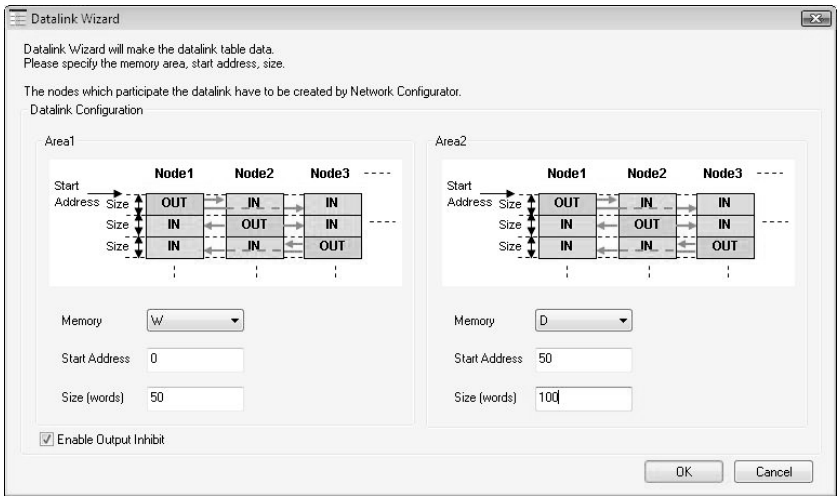
■ Allocations



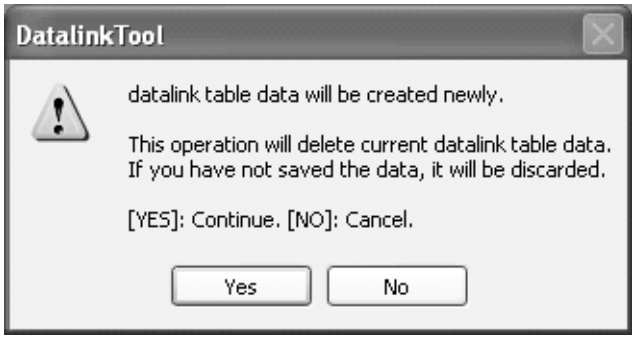
1,2,3... 1. Select ***Wizard*** from the Data Link Menu. The Datalink Wizard Dialog Box will be displayed.



2. Select the memory area (here, W) in the *Memory* Field and enter the starting address (here, 0) and number of words (here, 50) in the *Start Address* and *Size* Fields for Area 1.
3. Select the memory area (here, D) in the *Memory* Field and enter the starting address (here, 50) and number of words (here, 100) in the *Start Address* and *Size* Fields for Area 2.
4. Select the Enable Over Load Check Box if the Over Load function is necessary.

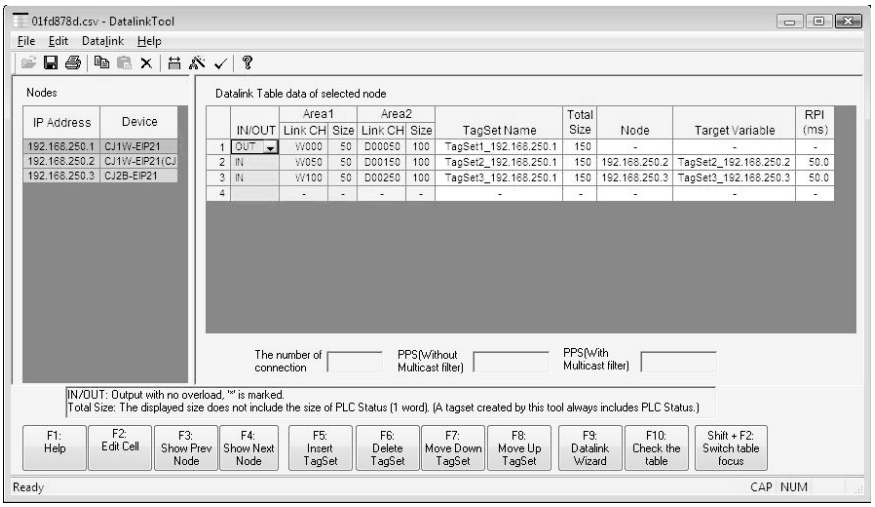


5. Click the **OK** Button. The following dialog box will be displayed.
Click the **Yes** Button to continue creating the data link table, or click the **No** Button to cancel the operation.

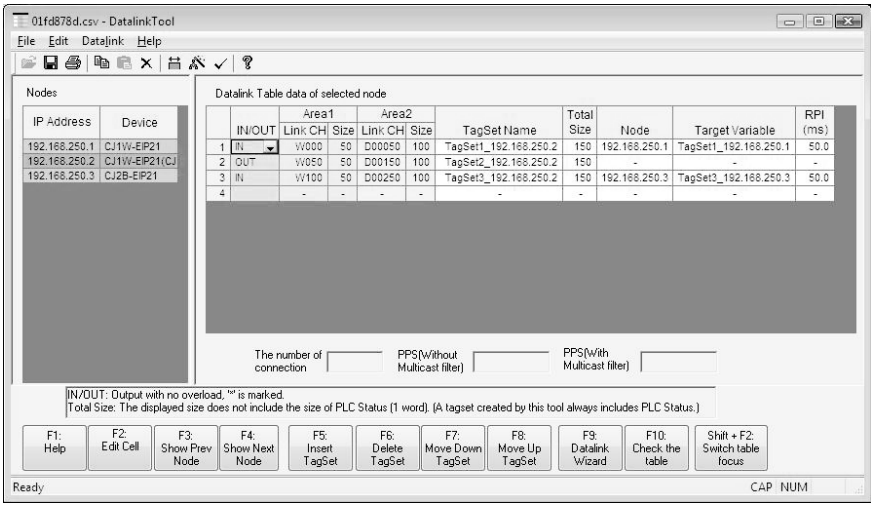


If the creating the data link table is continued, the data link table will be created with the same size of data link for all registered nodes. Examples are shown below.

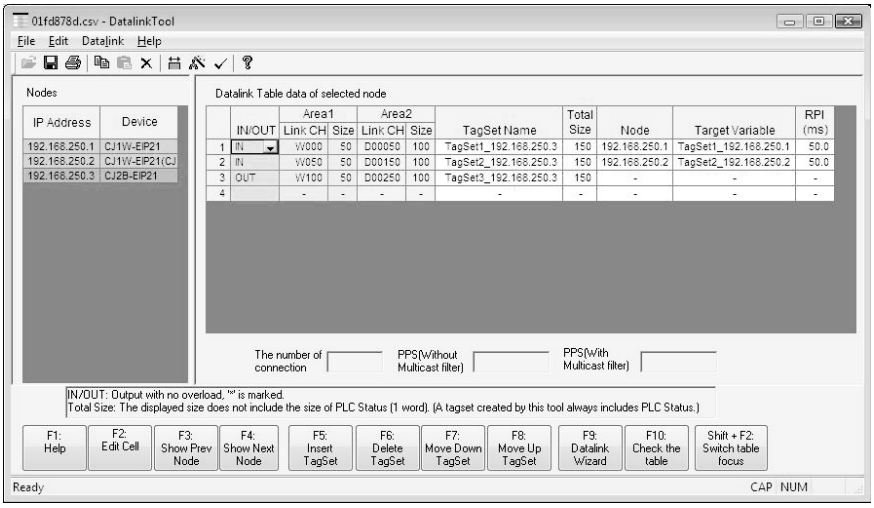
Automatic Allocation Results for Node 1 (IP Address: 192.168.250.1)



Automatic Allocation Results for Node 2 (IP Address: 192.168.250.2)



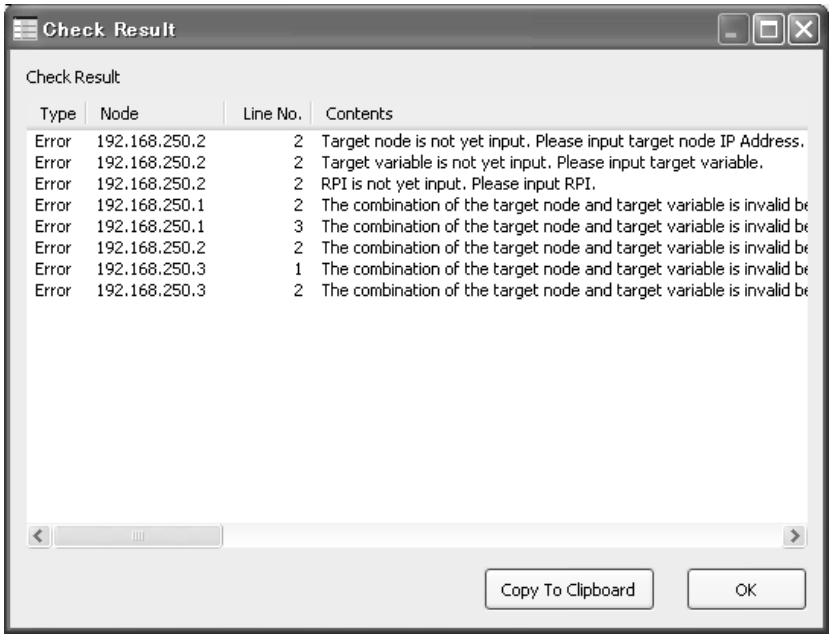
Automatic Allocation Results for Node 3 (IP Address: 192.168.250.3)



6. After entering all of the settings in the data link table, select ***Save*** from the File Menu. A consistency check will be performed on the table and the results will be displayed.

   a. Table Inconsistencies

   The following Check Result Dialog Box will be displayed. Correct the data link table according to the displayed information.



   To save the check results, click the **Copy To Clipboard** Button and paste the results to other file, such as the text pad.

   Click the **OK** Button. The following message will be displayed. Click the **OK** Button again to return to the EtherNet/IP Datalink Tool Window.



b. No Table Inconsistencies

The following message will be displayed. Click the **OK** Button.



7. Select ***Exit*** from the File Menu. The EtherNet/IP Datalink Tool will be exited and you'll return to the Network Configurator.
8. Returning to the Network Configurator
   Click the icon for each device and check the settings made with the EtherNet/IP Datalink Tool in the Edit Device Parameters Dialog Box.

6-2-7 Creating Connections Using the Wizard

You can use the Network Configurator's Wizard to easily create connections between OMRON PLCs following the instructions provided by the Wizard. Network Configurator version 3.10 or higher is required to use the Wizard.

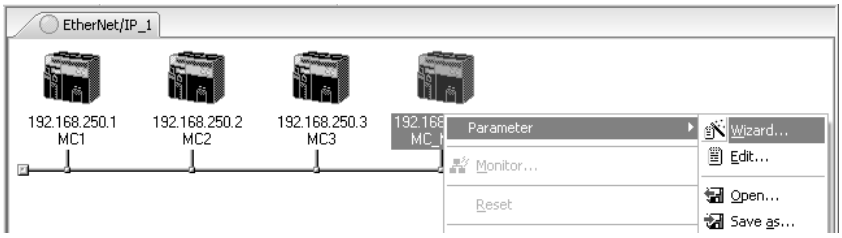
Note The Wizard can be used only with the following OMRON EtherNet/IP devices.

Device name	Remarks
CJ1W-EIP21	CJ1W-EIP21 mounted to CJ1 CPU Unit
CJ1W-EIP21(CJ2)	CJ1W-EIP21 mounted to CJ2/CJ3 CPU Unit
CJ2B-EIP21	Built-in EtherNet/IP port in CJ2H CPU Unit
CJ2M-EIP21	Built-in EtherNet/IP port in CJ2M-CPU3☐ CPU Unit
CS1W-EIP21	CJ1W-EIP21 mounted to CS1 CPU Unit
CJ1W-EIP21S	CJ1W-EIP21S mounted to CJ1 CPU Unit
CJ1W-EIP21S(CJ2)	CJ1W-EIP21S mounted to CJ2/CJ3 CPU Unit
CS1W-EIP21S	CS1W-EIP21S mounted to CS1 CPU Unit
CJ3M-CPU3☐	Built-in EtherNet/IP port in CJ3M-CPU3☐ CPU Unit

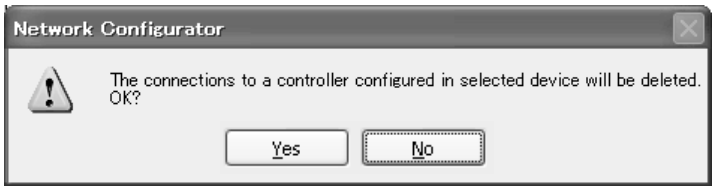
Use the following procedure to create connections (i.e., data links) with the Wizard.

1,2,3...

1. Set tags and tag sets for all devices before starting the Wizard. Refer to *6-2-4 Creating Tags and Tag Sets* for the setting procedure.
2. For tag data links between OMRON PLCs, a connection is created in the PLC (i.e., the originator device) that receives data as input data.
   First, select the registered device for which you want to create a connection in the Network Configuration Window of the Network Configurator, and then select ***Device - Parameters - Wizard*** from the menus.

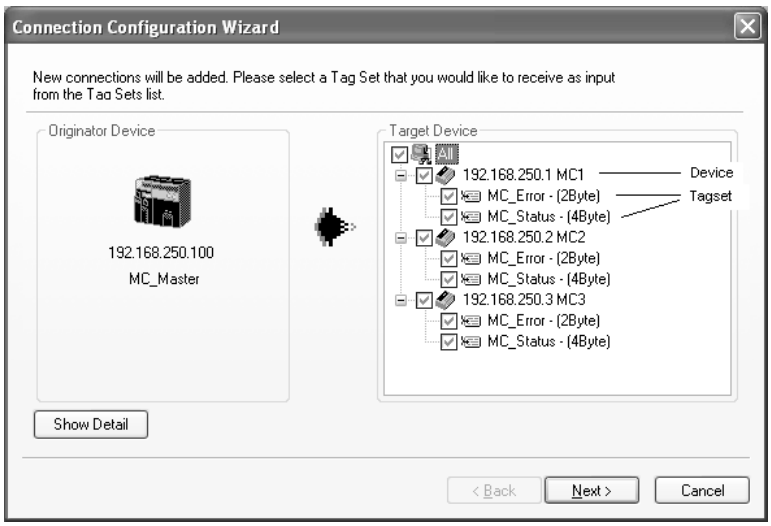


The following dialog box will be displayed before the Wizard starts.



Click the **Yes** Button to delete the connections that have been set with OMRON PLCs before starting the Wizard.

3. Create the connection following the instructions that are given by the Wizard after the Wizard starts. (See the following figure.)

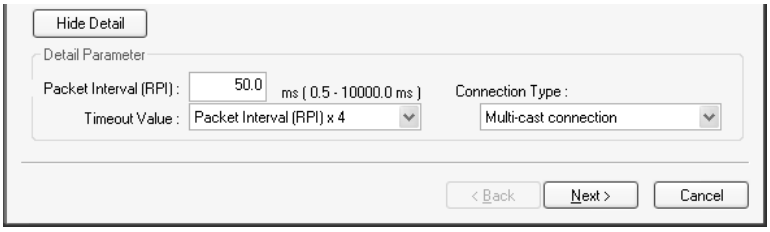


4. A list of tag sets is displayed on the right side of the Wizard Dialog Box with target devices that support receiving input data.
   Select the tag sets that you want to receive at the originator device.
   The following tables describes the meanings of the icons and check marks displayed in the tag set list.

Icon	Display position	Status
☑	All	All output tag sets for all devices are selected.
	Device	All output tag sets for the applicable device are selected.
	Tag set	The applicable output tag sets are selected. These are the tag sets that will be set in the connection.
☑	All	All or some output tag sets for some devices are selected.
	Device	Some output tag sets for applicable devices are selected.
☐	All	All output tag sets for all devices are not selected.
	Device	All output tag sets for applicable devices are not selected.
	Tag set	The applicable output tag sets are not selected. The connections for this tag set will be deleted.
☐	Device	No applicable tag sets.

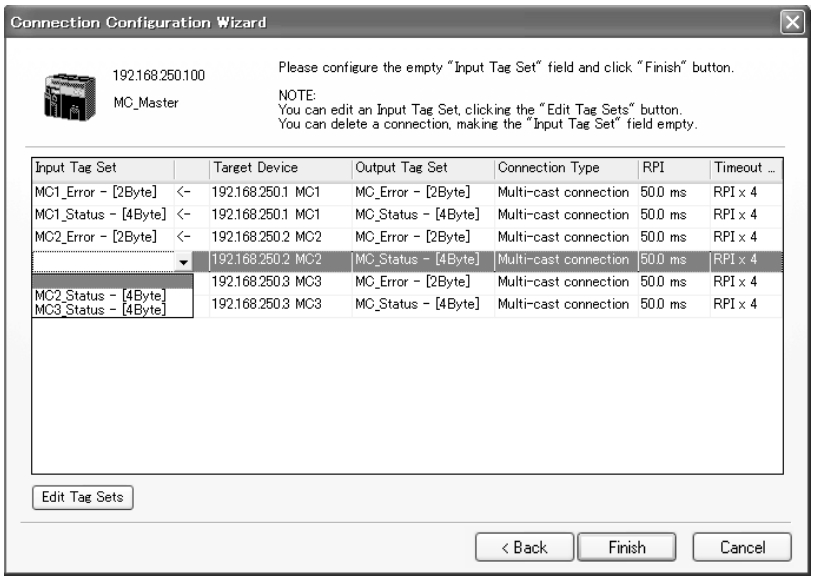
Note Tag sets that are used in connections that are already set are not displayed.

The following display will appear when you click the **Show Detail** Button.



The specified values for detailed parameters will be displayed. Change the values as required. The connection name cannot be set. They are automatically created using the following rule.
default_N (where N is a 3-digit number (001, 002, etc.) starting from 1)

5. Click the **Next** Button to switch to the table in the following Wizard Dialog Box. Follow the instructions to select and input from the list box the input tag set of the originator device that receives the output tag set of the target device.



- The blank area in the Input Tag Set Column is the connection that you are creating.
- The rows in which there are input tag sets are connections that are already set.
- To prevent duplicate settings, input tag sets that have been used are not displayed in the list box for input tag sets.
- If there is no applicable input tag set, you can edit a tag set or create a new one by using the **Edit Tag Sets** Button and **Edit Tag** Button.

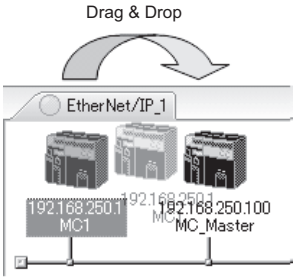
6. Once the input tag set settings have been completed, click the **Finish** Button. You can check the set connection by selecting ***Network - View Devices Connection Structure Tree*** from the menus.

- The Wizard can be ended even if the input tag set includes a blank row. In that case, a connection is not created for the blank row.
- You can delete a connection by deleting the input tag sets that were previously set.

6-2-8 Creating Connections by Device Dragging and Dropping

You can create a connection to the originator by dragging a target device and dropping it at the originator device. Network Configurator version 3.10 or higher is required to drag and drop devices to make connections.

Example:Drag the target device at 192.168.250.1 and drop it at the originator device at 192.168.250.100.



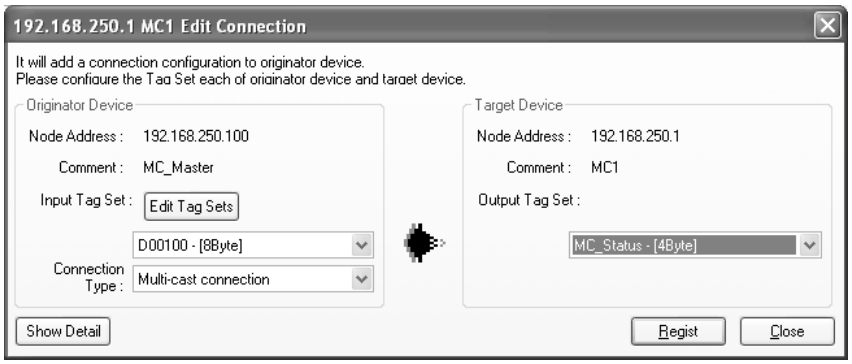
Note The EtherNet/IP originator device (i.e., a device in which connections can be set) must be one of the following OMRON EtherNet/IP devices.

Device name	Remarks
CJ1W-EIP21	CJ1W-EIP21 mounted to CJ1 CPU Unit
CJ1W-EIP21(CJ2)	CJ1W-EIP21 mounted to CJ2/CJ3 CPU Unit
CJ2B-EIP21	Built-in EtherNet/IP port in CJ2H CPU Unit
CJ2M-EIP21	Built-in EtherNet/IP port in CJ2M-CPU3☐ CPU Unit
CS1W-EIP21	CJ1W-EIP21 mounted to CS1 CPU Unit
CJ1W-EIP21S	CJ1W-EIP21S mounted to CJ1 CPU Unit
CJ1W-EIP21S(CJ2)	CJ1W-EIP21S mounted to CJ2/CJ3 CPU Unit
CS1W-EIP21S	CS1W-EIP21S mounted to CS1 CPU Unit
CJ3M-CPU3☐	Built-in EtherNet/IP port in CJ3M-CPU3☐ CPU Unit

Use the following procedure to create connections (i.e., data links) by dragging and dropping devices.

1,2,3... 1. Set the tags and tag sets for the target device that will be dragged.
   a. Refer to *6-2-4 Creating Tags and Tag Sets* for information on creating the settings if the target is one of the OMRON EtherNet/IP devices given above.
   b. If the target is another EtherNet/IP device, refer to the manual of that device and perform settings as required.
2. A dialog box as in the following figure for connection allocation will be displayed when you drag the target device and drop it at the OMRON EtherNet/IP device.

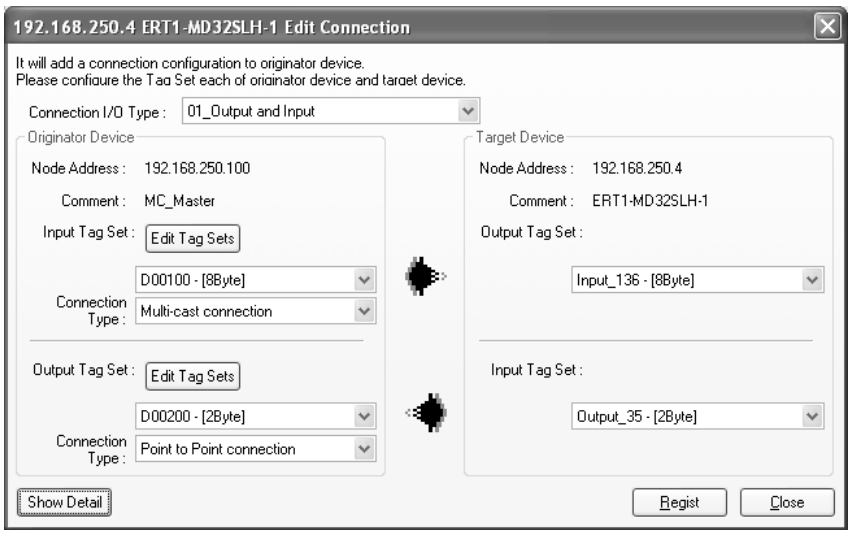
a. Using One of the Above OMRON EtherNet/IP Devices As Target



Select the output tag set from *Target Device* Area on the right side of the Edit Connection Dialog Box, and then select the input tag set to receive the output tag set in the *Originator Device* Area on the left.

- If there is no applicable input tag set at the originator, you can create a new one by using the **Edit Tag Sets** Button and **Edit Tag** Button.

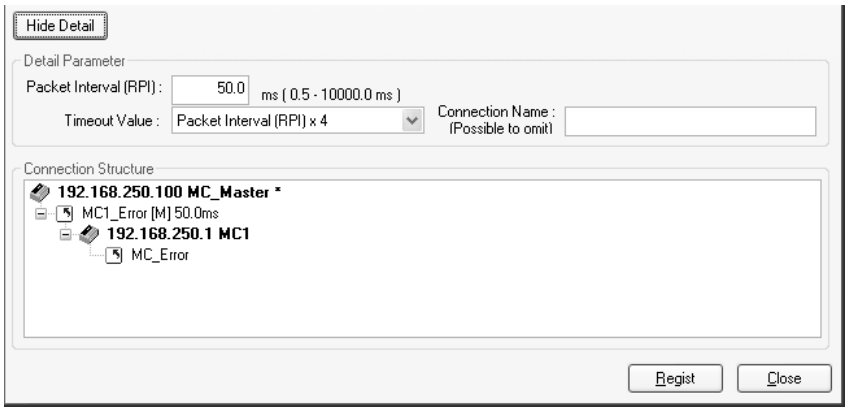
b. Using Other EtherNet/IP Devices as Target



The connection I/O type list box in the upper part of the Connection Settings Dialog Box displays the connection I/O types that can be selected. Select the connection I/O type according to your application.

- The connection I/O types that can be selected depend on the target device.
- Items that can be selected will depend on the connection I/O type that is selected.
- Select the output, input, or both output and input tag sets at the target and specify the corresponding input, output, or both input and output tag sets at the originator.
- If there is no applicable tag set at the originator, you can create a new one by using the **Edit Tag Sets** Button and **Edit Tag** Button.

The following display will appear when you click the **Show Detail** Button.



The specified values for detailed parameters will be displayed. Change the values as required. Connection names are automatically created using the following rule.

default_N (where N is a 3-digit number (001, 002, etc.) starting from 1)

Note The following dialog box will be displayed if a target device that does not have I/O data is dropped.



Before dropping again, refer to the manual of the applicable device and create the I/O data (i.e., output tag sets) required to create a connection.

3. After you have set all of the connection, click the **Regist** Button to create the connection. When creating the connection has been completed, the input tag set and output tag set will be blank. Next, you can continue to create connections by selecting the connection I/O type and setting a tag set.

6-2-9 Connecting the Network Configurator to the Network

This section explains how to connect the Network Configurator to the network.

Connecting through Ethernet

Note

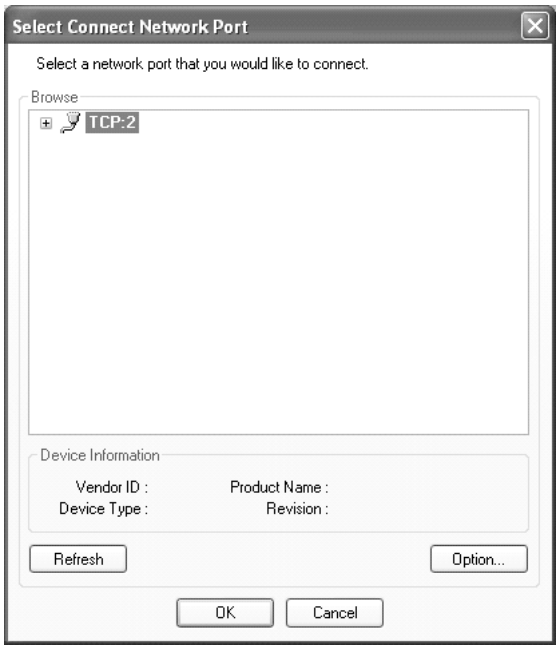
(1) If any of the following settings is made for a CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ on the connection path or in the destination, you may fail to connect it. If connection fails, check the settings. Refer to *CIP Message Server* in *13-4 Opening and Closing the Port* and *13-5 IP Packet Filtering.*
- The *Use CIP message server* Check Box is cleared.
- The *Use IP Packet Filter* Option is selected.

(2) The Windows firewall settings must be changed when making this connection for the first time in Windows XP or later Windows OS. For details on changing the firewall settings, refer to *Appendix G Precautions for Using Windows XP or Later Windows OS*.

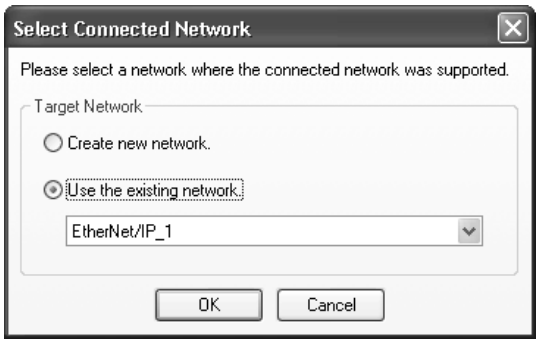
Connect to the EtherNet/IP Unit's Ethernet port via the Ethernet network.

1,2,3... 1. Select ***Option - Select Interface - Ethernet I/F***.

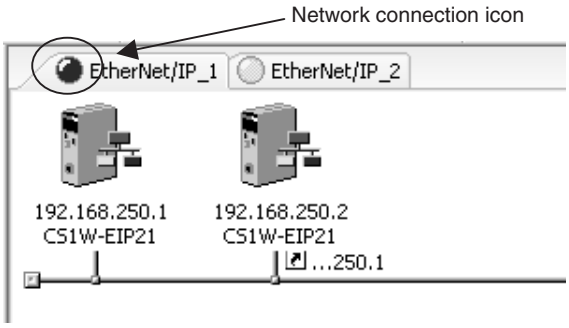
2. Select ***Network - Connect***.
   If there are multiple Ethernet interfaces on the computer, the Select Connect Network Port Dialog Box will be displayed. Select the interface that is to be connected, and press the **OK** Button.
   The following dialog box will be displayed.



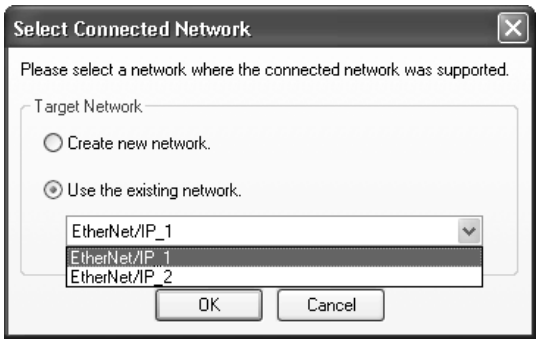
3. Click the **OK** Button. Select the network to be connected.



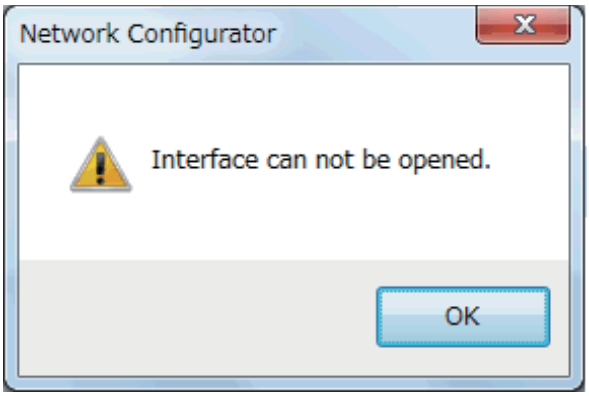
The Network Configurator will connect to the EtherNet/IP network. If the Network Configurator is connected online properly, *On-line* will be displayed in the status bar at the bottom of the window. The network connection icon will be displayed in blue in the Network Tab Page in which the Network Configurator is connected.



The connecting network can be switched by selecting ***Network - Change Connect Network***.



Note If the following dialog box is displayed on the Network Configurator when you connect the CPU Unit, use the table below to check the possible cause and take corrective action.



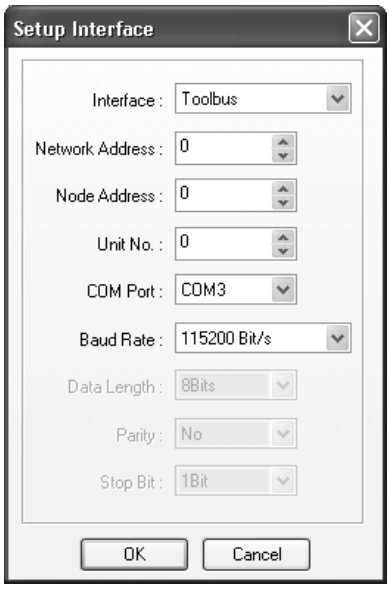
Probable cause	Corrective action
The cable is not connected correctly.	Check that the cable is not damaged or loose.
The connection to the CPU Unit is blocked by the firewall settings.	If the connection to the CPU Unit is blocked by the firewall settings, remove the cause of the blockage. Refer to *Appendix G Precautions for Using Windows XP or Later Windows OS* for information on the firewall settings.
The communications with the Network Configurator are blocked by the IP packet filtering of the CS1W/CJ1W-EIP21S or CJ3M-CPU3☐.	Allow the EtherNet/IP Unit to communicate with the Network Configurator. Refer to *13-5 IP Packet Filtering* for information on the IP packet filtering settings for the CS1W/CJ1W-EIP21S or CJ3M-CPU3☐.

Connecting through the CPU Unit's Peripheral or RS-232C Port

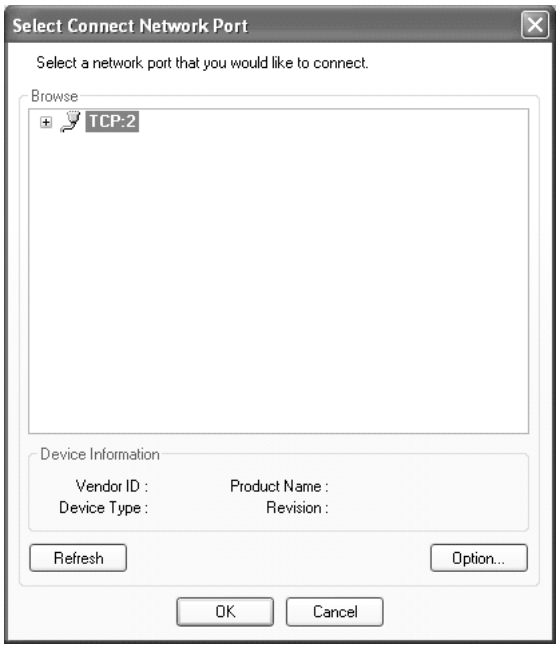
Connect to the EtherNet/IP Unit's Ethernet port via the CPU Unit's peripheral port or RS-232C port.

1,2,3...

1. Select ***Option - Select Interface - CS/CJ1 Serial Port → EIP Unit I/F***.
2. Select ***Network - Connect***. The following dialog box will be displayed.

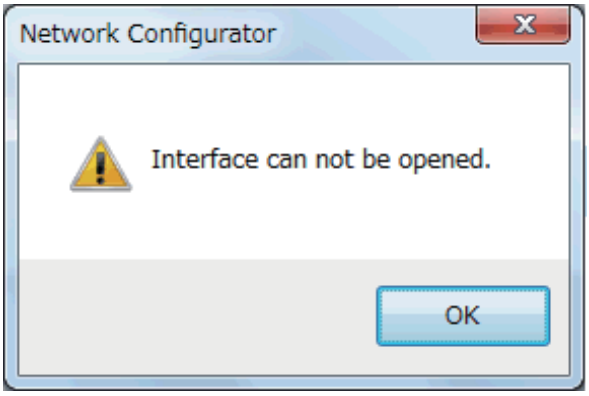


3. Input the EtherNet/IP Unit's unit number in the *Unit No.* Field, select the connecting COM port number, and click the **OK** Button.
   Usually, the *Baud Rate* is left at this setting.
   The following dialog box will be displayed.



4. After clicking **TCP:2**, click the **OK** Button. The Network Configurator will be connected to the EtherNet/IP network. If the Network Configurator is connected online properly, *On-line* will be displayed in the status bar at the bottom of the window.

Note If the following dialog box is displayed on the Network Configurator when you connect the CPU Unit, use the table below to check the possible cause and take corrective action.



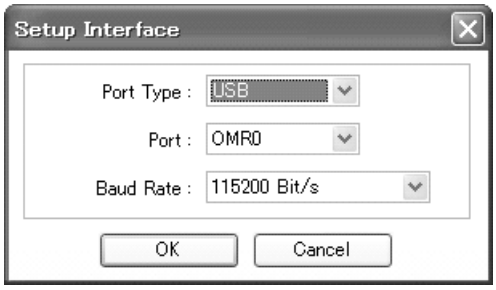
Probable cause	Corrective action
The cable is not connected correctly.	Check that the cable is not damaged or loose.
The connection to the CPU Unit is blocked by the firewall settings.	If the connection to the CPU Unit is blocked by the firewall settings, remove the cause of the blockage. Refer to *Appendix G Precautions for Using Windows XP or Later Windows OS* for information on the firewall settings.

Connecting through the CPU Unit's USB or RS-232C Port (CJ2 CPU Units Only)

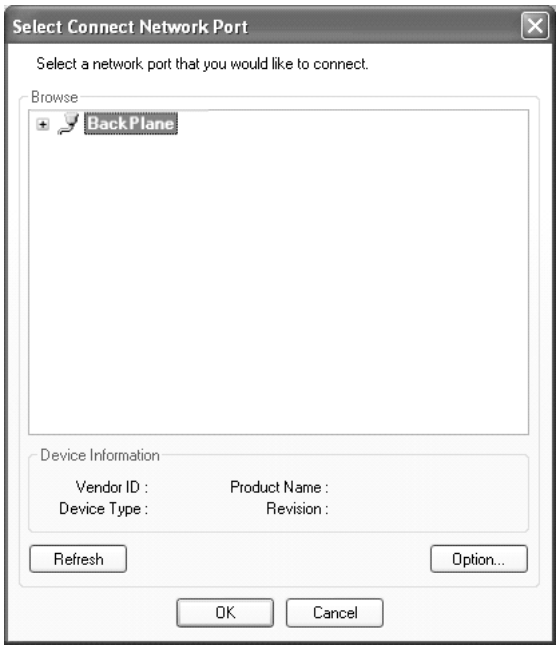
Connect to the EtherNet/IP Unit's Ethernet port via the CPU Unit's USB port or RS-232C port.

1,2,3...

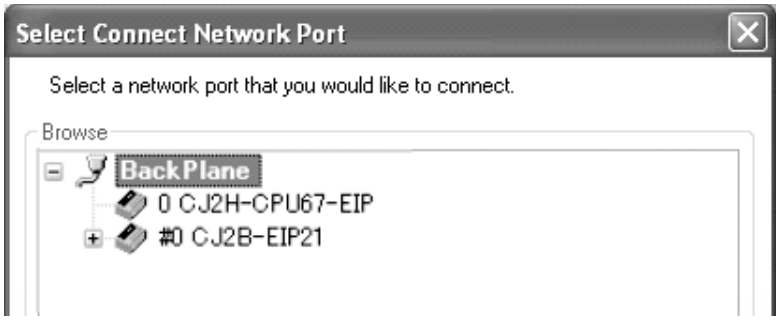
1. Select ***Option - Select Interface - CJ2 USB/Serial Port*** to set the communications interface.
2. Select ***Network - Connect***. The Setup Interface Dialog Box will be displayed.



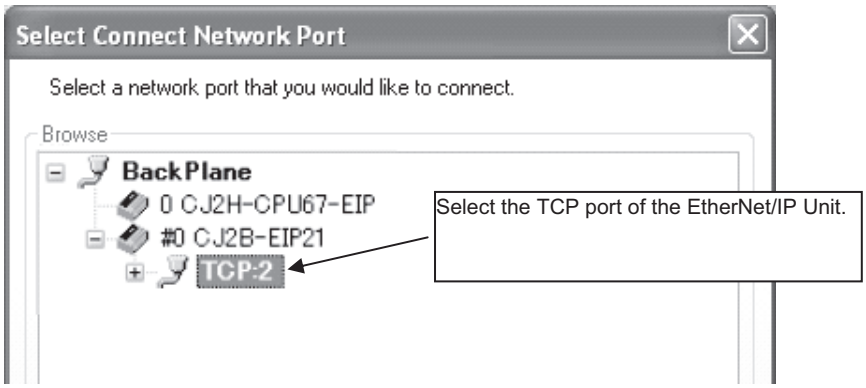
3. Set the port type to either USB or serial.
4. Set the port to use and then click the **OK** Button. (Leave the baud rate at the default setting.)
   The following dialog box will be displayed.



5. Select the *Backplane* Icon and click the **Refresh** Button.
The CPU Unit, CPU Bus Units, and Special I/O Units connected in the PLC will be displayed as shown below.

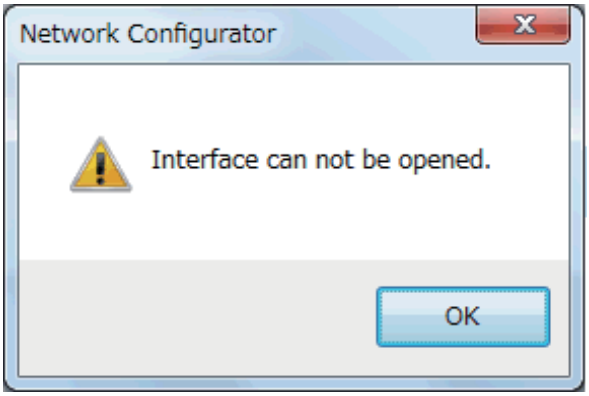


6. Click the + icon to the left of the EtherNet/IP Unit or built-in EtherNet/IP port (CJ1W-EIP21(CJ2)/CJ1W-EIP21S(CJ2) or CJ2B-EIP21/CJ2M-EIP21/ CJ3M-CPU3□). The TCP ports on the EtherNet/IP Unit will be displayed as shown below.



7. Select the port for the EtherNet/IP Unit and then click the **OK** Button. The Network Configurator will be connected to the EtherNet/IP network. If the Network Configurator goes online normally, “On-line” will be displayed in the status bar at the bottom of the window.

Note If the following dialog box is displayed on the Network Configurator when you connect the CPU Unit, use the table below to check the possible cause and take corrective action.



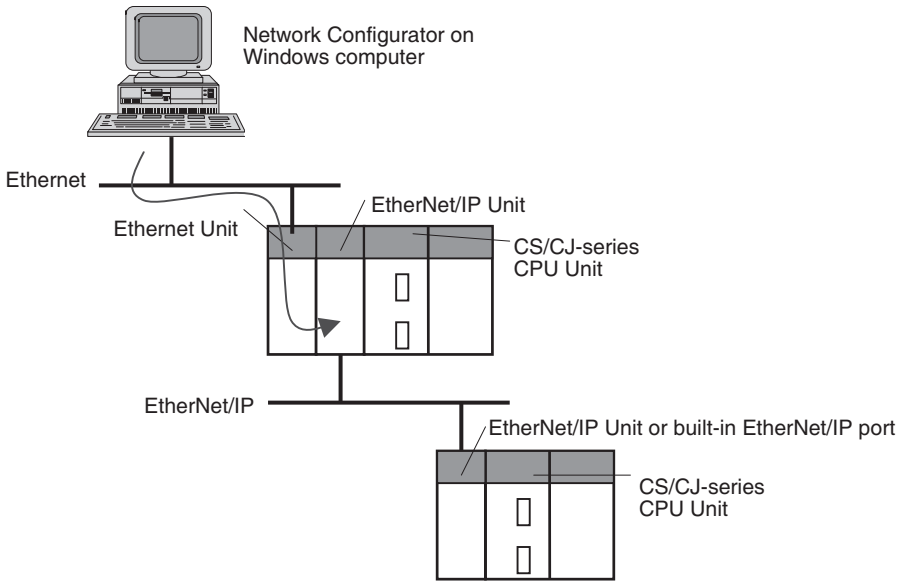
Probable cause	Corrective action
The cable is not connected correctly.	Check that the cable is not damaged or loose.
The connection to the CPU Unit is blocked by the firewall settings.	If the connection to the CPU Unit is blocked by the firewall settings, remove the cause of the blockage. Refer to *Appendix G Precautions for Using Windows XP or Later Windows OS* for information on the firewall settings.
The USB driver is not installed correctly.	Install the USB driver correctly. Refer to the *CJ-series CJ2 CPU Unit Hardware User's Manual* (Cat. No. W472) for information on installing the USB driver.

Connecting to an EtherNet/IP Network via an Ethernet Unit

Note

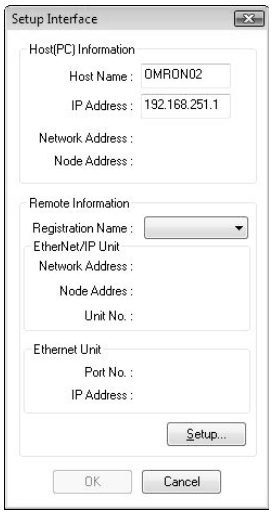
(1) The Windows firewall settings must be changed when making this connection for the first time in Windows XP or later Windows OS. Refer to *Appendix G Precautions for Using Windows XP or Later Windows OS* for information on how to make the changes.

(2) Use the CX-Integrator to correctly set the FINS routing tables for the CS/CJ-series CPU Unit that will be the relay node.

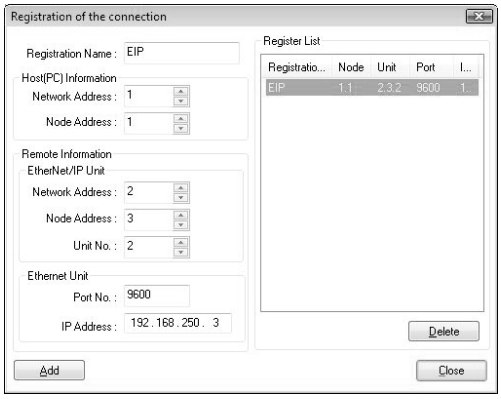


1,2,3... 1. Select ***Option - Select Interface - Ethernet → CS/CJ1 ETN-EIP Unit I/F***.

2. Select ***Network - Connect***.
The following Setup Interface Dialog Box will be displayed.



3. Click the **Setup** Button in the Setup Interface Dialog Box. The *Registration of the connection* Dialog Box will be displayed. Enter the network information for the connection destination, and then click the **Add** Button to register the settings.



The registration information details are as follows:

a. Registration name
Enter any name.

b. Host (PC) information
Enter information for the computer that has the Network Configurator installed.

•Network address
Same number as the network address of the Ethernet Unit of the PLC that will be the relay node.

•Node address
Last value in the computer's IP address (e.g., 1 for 192.168.250.1)

c. Remote Information - EtherNet/IP Unit
Enter the information for the EtherNet/IP Unit of the PLC that will be the relay node.

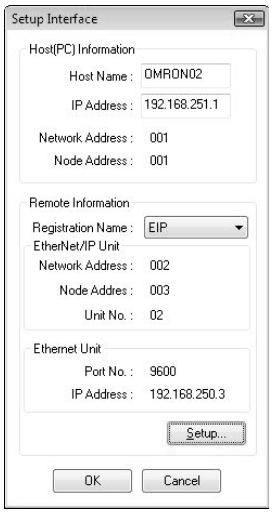
•Network address
Network address set in the routing tables

•Node address
Last value in the IP address of the Unit above (e.g., 3 for 192.168.251.3)

•Unit number of CPU Bus Unit
Unit number of the Unit above

d. Remote Information - Ethernet Unit
Enter the information for the Ethernet Unit of the PLC that will be the relay node.

4. Once the settings have been registered, the Setup Interface Dialog Box will be displayed again. Check the registered information that has been entered, and then click the **OK** Button.

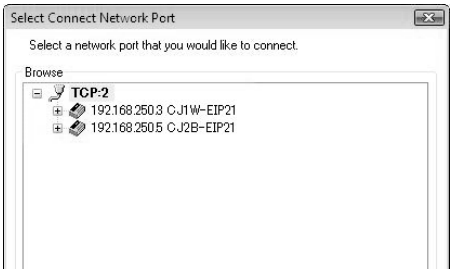


5. The following dialog box will be displayed. Select *TCP:2*, which represents the EtherNet/IP port, and then click the **OK** Button.

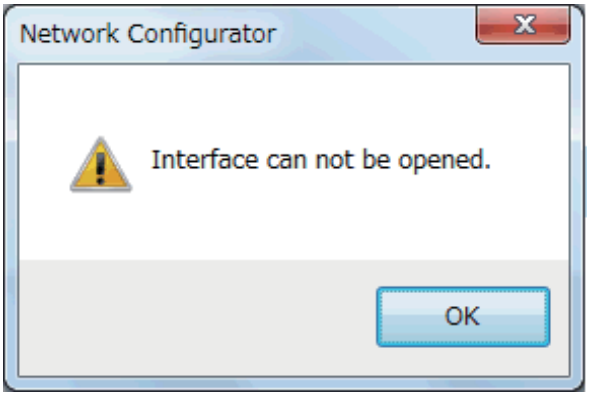


The Network Configurator will connect to the EtherNet/IP network, and "On-line" will be displayed in the status bar at the bottom of the window when connection has been properly made online.

Note A list of nodes on the EtherNet/IP network you are attempting to connect to will be displayed when the **Refresh** Button or the icon (⊞) at the left of *TCP:2* is clicked in the dialog box above. (Refer to the following figure.)



Note If the following dialog box is displayed on the Network Configurator when you connect the CPU Unit, use the table below to check the possible cause and take corrective action.



Probable cause	Corrective action
The cable is not connected correctly.	Check that the cable is not damaged or loose.
The connection to the CPU Unit is blocked by the firewall settings.	If the connection to the CPU Unit is blocked by the firewall settings, remove the cause of the blockage. Refer to *Appendix G Precautions for Using Windows XP or Later Windows OS* for information on the firewall settings.
The communications with the Network Configurator are blocked by the IP packet filtering of the CS1W/CJ1W-EIP21S or CJ3M-CPU3□.	Allow the EtherNet/IP Unit to communicate with the Network Configurator. Refer to *13-5 IP Packet Filtering* for information on the IP packet filtering settings for the CS1W/CJ1W-EIP21S or CJ3M-CPU3□.

6-2-10 Downloading Tag Data Link Parameters

To make tag data links, you must download tag data link parameters, such as tag set settings and connection settings, to all devices in the EtherNet/IP network. When the download operation is executed, the tag data link parameters will be transferred to the EtherNet/IP Units that require the settings.

The following procedure shows how to download the tag data link parameters. Refer to *6-2-9 Connecting the Network Configurator to the Network* for information on how to connect the Network Configurator to the network.

Note

- If the target node IP address is not set correctly, invalid device parameters may be set in the wrong PLC. Check the connected PLC before downloading parameters.
- If incorrect tag data link parameters are set, it may cause equipment to operate unpredictably. Even when the correct tag data link parameters are set, make sure that there will be no effect on equipment before transferring the data.
- When network symbols are used in tag settings, a connection error will result if the symbols are not also set in the CPU Unit. Before downloading the tag data link parameters, check to confirm that the network symbols have been set in the CPU Unit. On the Connection and Tag Status Tab Pages described in *18-1-1 The Network Configurator's Device Monitor Function*, check whether the network symbol, tag, and connection settings are correct.

- When a communications error occurs, the output status depends on the specifications of the Unit being used. When a communications error occurs for a Unit that is used along with output devices, check the operating specifications and implement safety countermeasures.
- The EtherNet/IP Unit is automatically restarted after the parameters have been downloaded. This restart is required to enable the tag set and connection information that have been set. Before downloading the parameters, check to confirm that restarting will not cause any problems with the equipment.
- Do not disconnect the Ethernet cable or reset or turn OFF the power to the EtherNet/IP Unit while the parameters are being downloaded
- The CPU Unit can download tag data link parameters in either RUN mode or MONITOR mode. (They can also be downloaded in PROGRAM mode.) While the download is in progress, tag data links (data exchange) between related nodes are stopped. If you download the parameters in RUN mode or MONITOR mode, confirm that there is no impact on the equipment before executing the transfer.
  In addition, in ladder programs that use tag data links, include a circuit to interlock data processing while the tag data links are stopped or in an error state.
- However, for CS1W/CJ1W-EIP21 or CJ2H-CPU6□-EIP with revision 1 (Unit version Ver.1.0) excluding CS1W/CJ1W-EIP21S, tag data link parameters can be downloaded only when the CPU Unit is in PROGRAM mode. All CPU Units must be in PROGRAM mode to download the parameters if any Units 1 are included in the network.

1,2,3... 1. Connect the Network Configurator online.

2. There are two ways to download the parameters.

- Downloading to All Devices in the Network

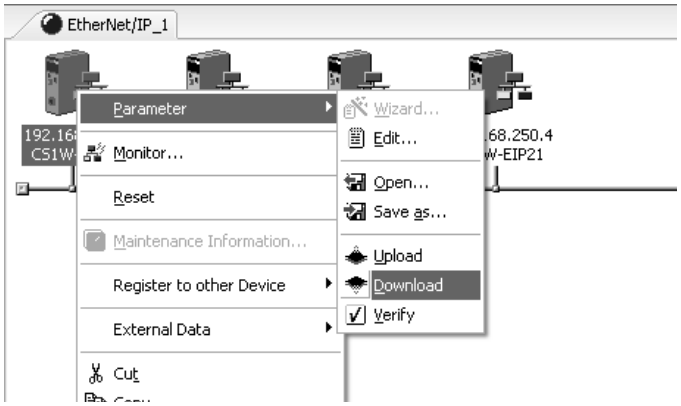
  Select ***Network - Download***. The following dialog box will be displayed.



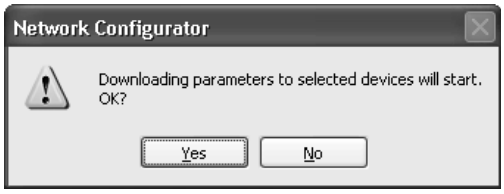
- Downloading Individually to Particular Devices

  Select the icon of the EtherNet/IP built-in Unit to which you want to download. To select multiple nodes, press and hold the Shift Key while selecting additional icons. (In the following example, 2 nodes are selected: 192.168.250.1 and 192.168.250.2.)

  After selecting the icons, click the right mouse button over the icon to display the pop-up menu, and select ***Parameter - Download***.



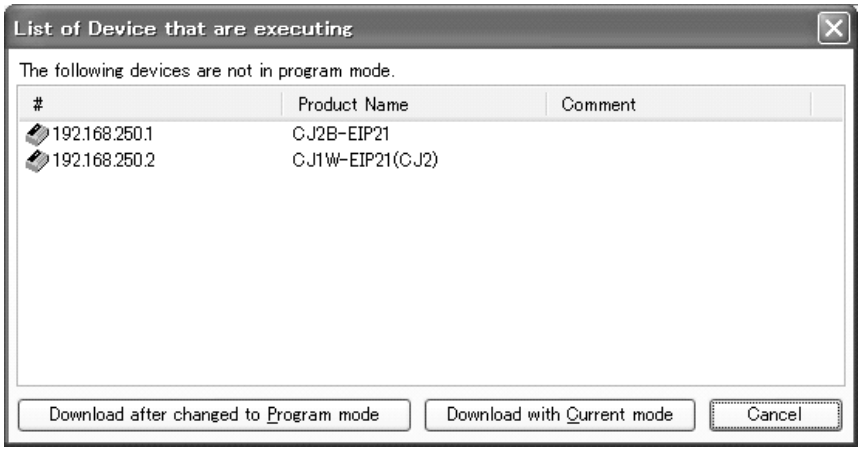
The following dialog box will be displayed.



3. Click the **Yes** Button to download the tag data link parameters to the built-in EtherNet/IP Unit.

   The following dialog box will be displayed if any of the CPU Units is not in PROGRAM mode.

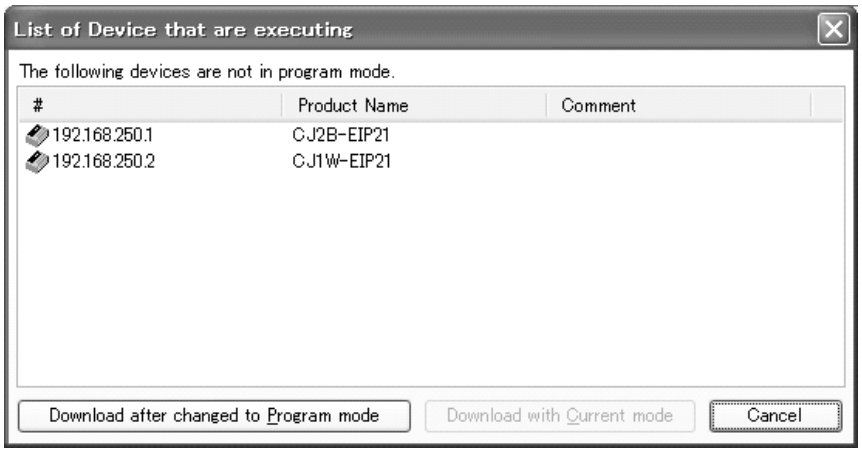
- Display When All EtherNet/IP Units and Built-in EtherNet/IP Ports are Revision 2 or Higher



If the **Download after changed to Program mode** Button is clicked, all CPU Units will be changed to PROGRAM mode and the parameters will be downloaded. Confirm safety for all controlled equipment if the CPU Units are changed to PROGRAM mode. The operating mode can be returned to the previous setting after the parameters have been downloaded.

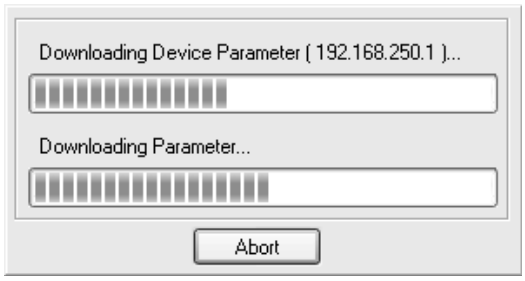
The **Download with Current mode** Button can be clicked to download load the parameters even when one or more CPU Units is in RUN or MONITOR mode.

- Display When Even One EtherNet/IP Unit Is Revision 1

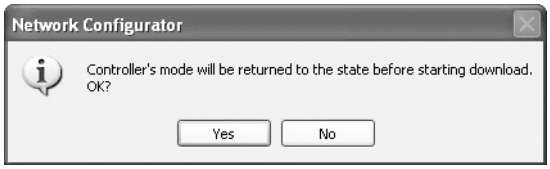


When the **Download after changed to Program mode** Button is clicked, all CPU Units will be changed to PROGRAM mode and the parameters will be downloaded. Confirm safety for all controlled equipment if the CPU Units are changed to PROGRAM mode. The operating mode can be returned to the previous setting after the parameters have been downloaded.

During the download, the following progress monitor will be displayed to show the progress of the download.



If the operating mode of one or more CPU Units was changed to download the parameters, the CPU Units can be returned to the previous operating mode. If the **No** Button is clicked, the CPU Units will remain in PROGRAM mode.



4. The following dialog box will be displayed, indicating that the download was completed.



6-2-11 Uploading Tag Data Link Parameters

Tag data link parameters (such as the tag set settings and connection settings) can be uploaded from EtherNet/IP Units in the built-in EtherNet/IP network. The following procedure shows how to upload the parameters. For details on connecting to the network from the Network Configurator, refer to *6-2-9 Connecting the Network Configurator to the Network*.

1,2,3... 1. Connect the Network Configurator to the network.

2. There are two ways to upload the parameters.

- Uploading from All Devices in the Network

  Select ***Network - Upload***. The following dialog box will be displayed.



- Clicking the **Yes** Button:

  Parameters will be uploaded only from the devices registered in the Network Configuration Window. Parameters will not be uploaded from devices that are not registered in the Network Configuration Window.

- Clicking the **No** Button:
  - If parameters are being uploaded from all devices in the network, the parameters will be newly uploaded from all devices. The current network configuration information will be lost.
  - If parameters are being uploaded from specified devices only, the upload operation will be cancelled and the upload will not be performed.

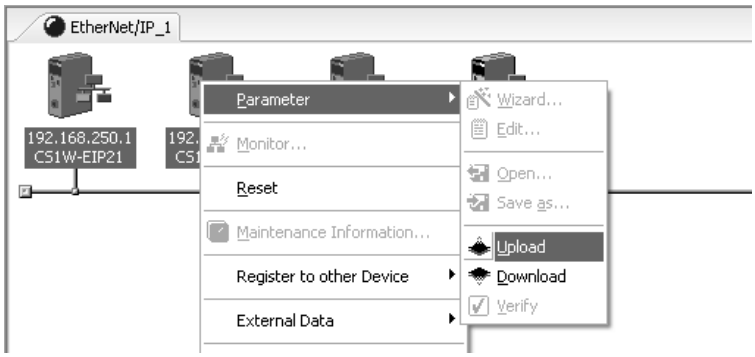
- Clicking the **Cancel** Button:

  The upload operation will be cancelled and the upload will not be performed.

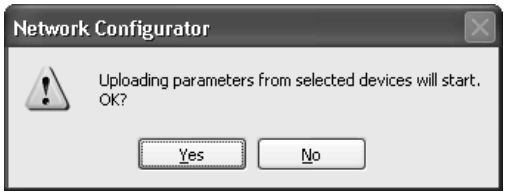
- Uploading Individually from Particular Devices

  Select the icon of the built-in EtherNet/IP Unit from which you want to upload. To select multiple nodes, press and hold the Shift Key while selecting additional icons. (In the following example, 2 nodes are selected: 192.168.250.1 and 192.168.250.2.)

  After selecting the icons, click the right mouse button over the icon to display the pop-up menu, and select ***Parameter - Upload***.

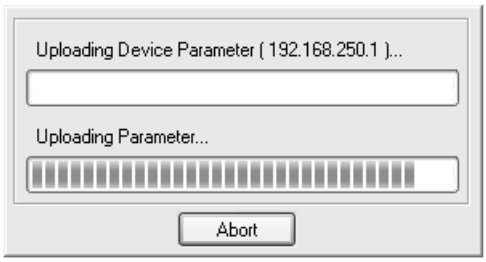


The following confirmation dialog box will be displayed.



Click the **Yes** Button or **No** Button.

During the upload, the following progress monitor will be displayed to show the progress of the upload.



3. The following dialog box will be displayed, indicating that the upload was completed.



6-2-12 Verifying the Tag Data Links

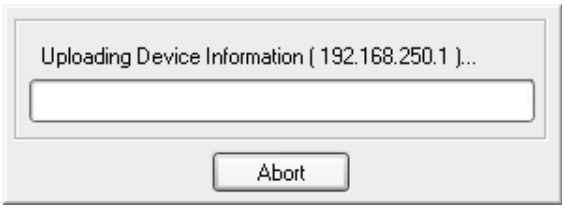
Tag data link parameters (such as the tag set settings and connection settings) can be compared with the built-in EtherNet/IP Units in the EtherNet/IP network. The following procedure shows how to compare the parameters. For details on connecting to the network from the Network Configurator, refer to *6-2-9 Connecting the Network Configurator to the Network*.

Verifying the Network Configuration

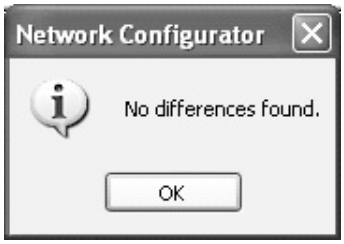
Compare the list of registered devices in the Network Configuration Window with the devices connected on the EtherNet/IP network, and check the IP addresses and device types. This function cannot be used to verify device parameters.

1,2,3...

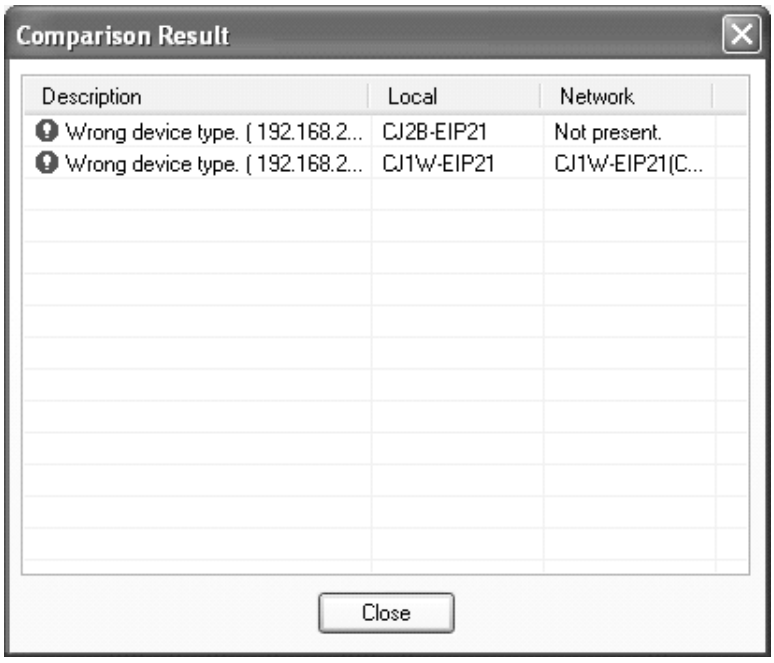
1. Connect the Network Configurator to the network.
2. The following progress monitor will be displayed to show the progress as data is read from the network and compared.



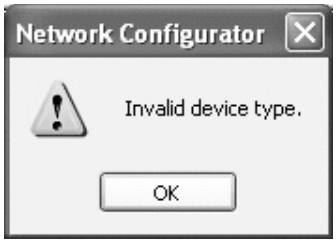
3. The results of the comparison between the network configuration file and data from the network are displayed as follows.
   - Differences Not Found in the Comparison



- Differences Found in the Comparison



- Differences Found in the Device Type.



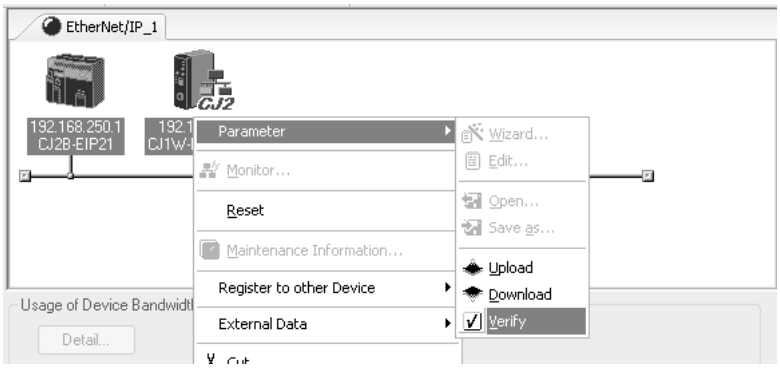
Click the **OK** Button or the Close Button.

Verifying the Device Parameters

Use the following procedure to compare the device parameters for the devices selected in the Network Configuration Window with those of the devices connected on the EtherNet/IP network. The IP addresses, device types, and device parameters are compared.

1,2,3...

1. Connect the Network Configurator to the network.
2. Click the icon of the built-in EtherNet/IP Unit that is to be verified. To select multiple nodes, hold down the Shift Key while clicking the icons. (In the following example, the 192.168.250.1 and 192.168.250.2 nodes are selected.)
   With the icons selected, right-click and select ***Parameter - Verify*** from the pop-up menu.

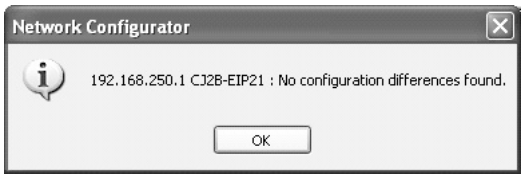


3. The following dialog box will be displayed.

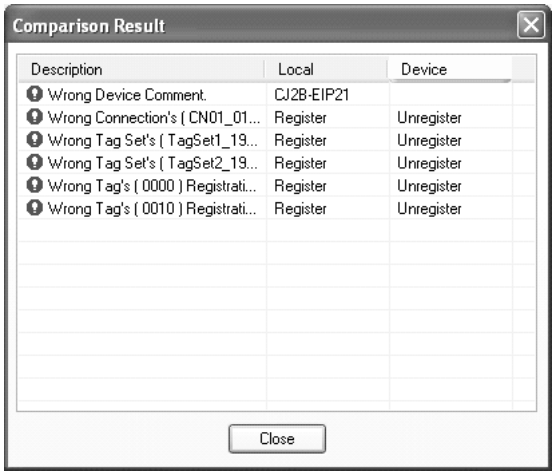


Click the **Yes** Button or the **No** Button.

4. One of the following dialog boxes will be displayed.
   - Differences Not Found in the Comparison



   - Differences Found in the Comparison

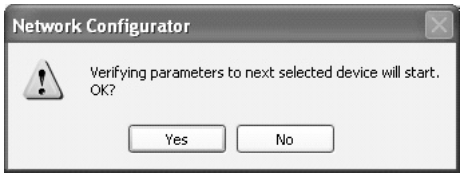


   - Differences Found in the Device Type



Click the OK Button or the Close Button.

5. If multiple nodes have been selected, the following message will be displayed. Click the **Yes** Button.



The comparison results will be displayed in order of the selected nodes.

6-2-13 Starting and Stopping Tag Data Links

Automatically Starting Tag Data Links

Tag data links will start operating automatically immediately after the tag data link parameters are downloaded from the Network Configurator. (They will also start automatically when the power to the PLC is turned ON or the CPU Unit is restarted.)

Starting and Stopping All Tag Data Links on the Network

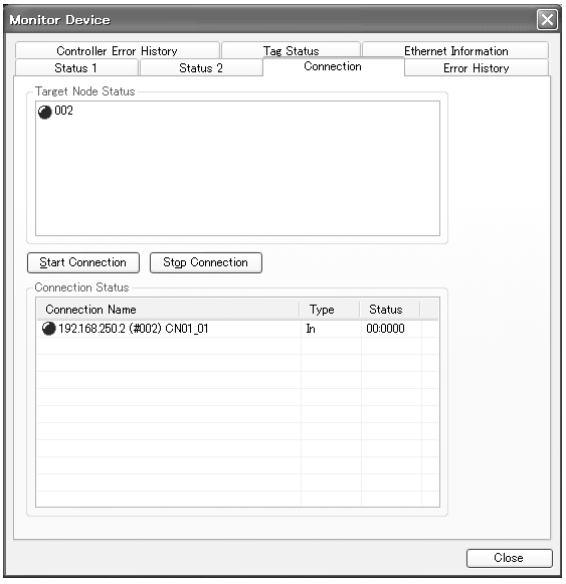
Using the Network Configurator

All tag data links on the network can be started and stopped by selecting ***I/O Connection - Start/Stop*** from the Network Menu.

Starting and Stopping Tag Data Links for Individual Devices

Using the Network Configurator

You can start and stop tag data links for individual devices using the following buttons in the Monitor Device Dialog Box. This applies only to tag data links for which the device is the originator. Access the Monitor Device Dialog Box by selecting ***Monitor*** from the Device Menu.



Start Connection Button:

Starts all connections for which the device is the originator.

Stop Connection Button:

Stops all connections for which the device is the originator.

Note Connections will be cut off if any of the following errors occurs in the CPU Unit that is the originator while tag data links are active.

- Fatal CPU Unit error
- I/O refresh error

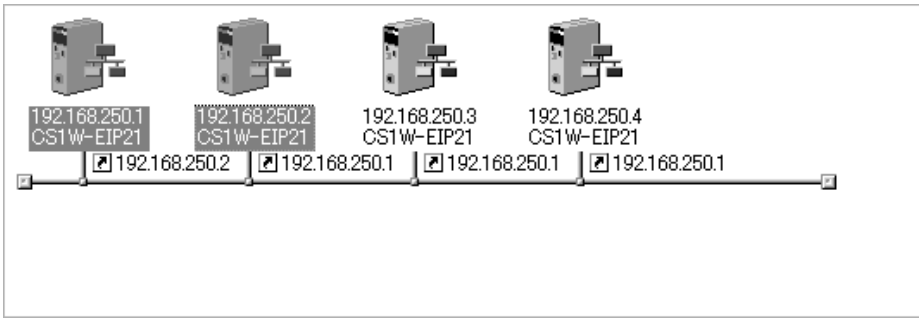
- CPU Unit WDT error
- I/O bus error

6-2-14 Clearing the Device Parameters

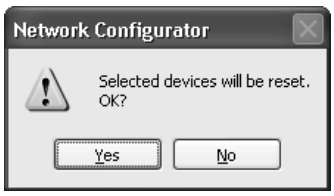
The device parameters saved in the built-in EtherNet/IP Units in the EtherNet/IP network can be cleared (returned to their default settings). The following procedure shows how to clear the device parameters. For details on connecting to the network from the Network Configurator, refer to *6-2-9 Connecting the Network Configurator to the Network*.

1,2,3...

1. Connect the Network Configurator to the network.
2. Select the icon of the built-in EtherNet/IP Unit in which you want to clear the device parameters. In the following example, 2 nodes are selected: 192.168.250.1 and 192.168.250.2. To select multiple nodes, press and hold the Shift Key while selecting additional icons.



3. Select **Device - Reset**. The following dialog box will be displayed.



- Clicking the **Yes** Button:

  The following dialog box will be displayed.



  Select one of the following options and click the **OK** Button.

  - *Emulate cycling power*
    Restarts the Unit.
  - *Return to the out-of-box configuration, and then emulate cycling power*
    Returns the Unit to its factory default settings, and restarts the Unit.

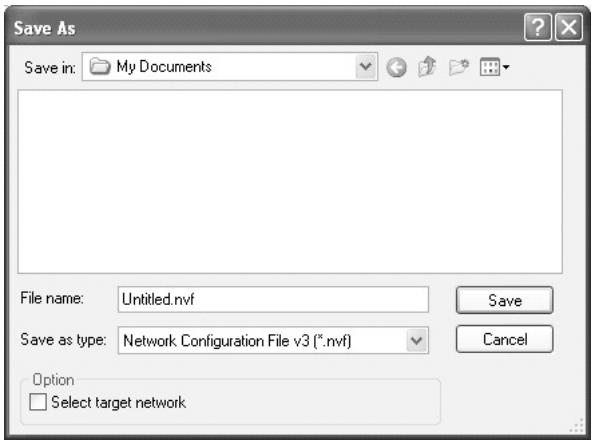
- Clicking the **No** Button:

  The device parameters are not cleared or reset.

6-2-15 Saving the Network Configuration File

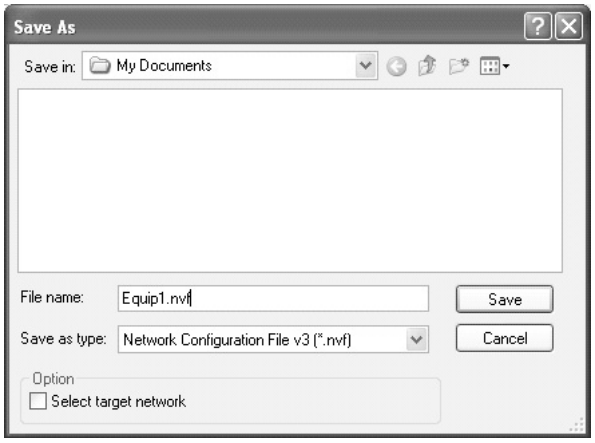
Device parameters set in the Network Configurator, or device parameters uploaded from the network can be saved as a network configuration file.

1,2,3... 1. Select ***File - Save As***. The following dialog box will be displayed.



The *File name* Field will contain *Untitled.nvf* as the default file name.

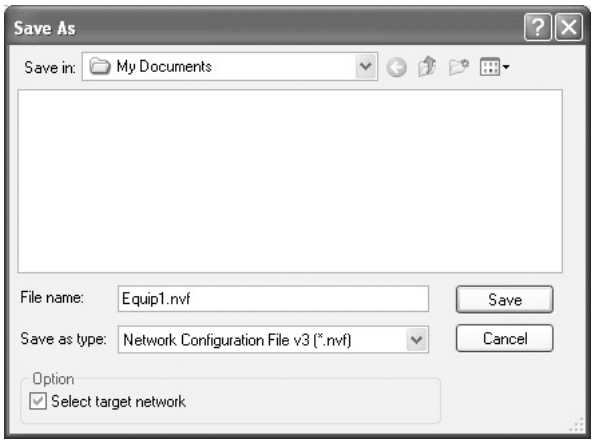
2. Input the file name, and click the **Save** Button.



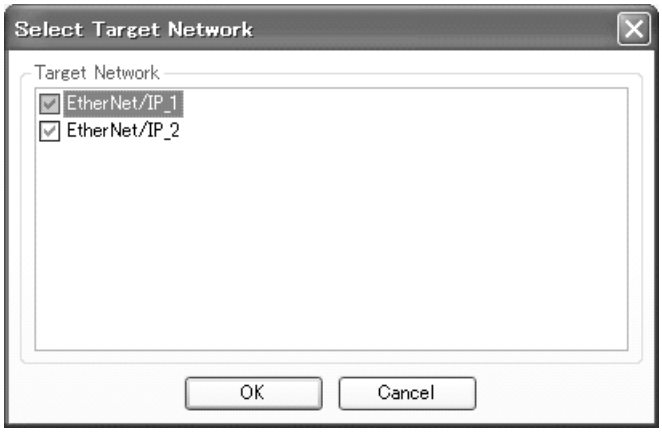
The network configuration file save operation is complete.

3. When the network configuration is changed later, the existing network configuration file can be overwritten by selecting ***File - Save*** or clicking the Button.

4. You can select the *Select target network* Check Box in the *Option* Area to save a network configuration file with only the required networks.



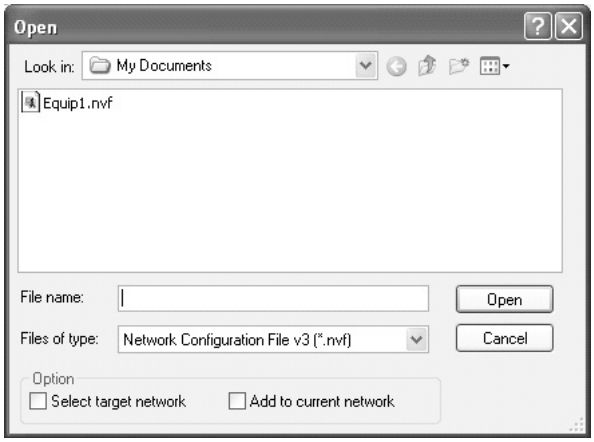
Select the check boxes of the networks to save and click the **OK** Button.



6-2-16 Reading a Network Configuration File

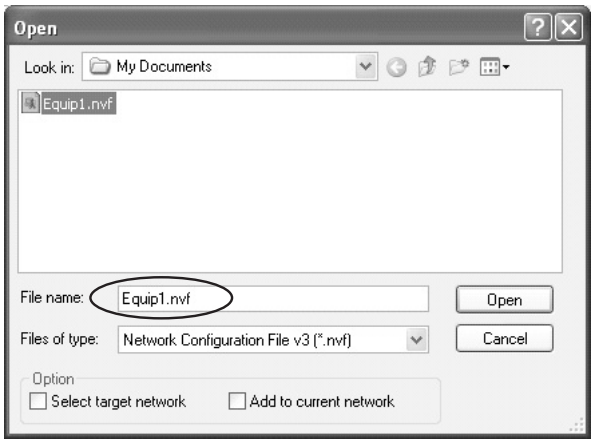
A previously saved network configuration file can be read into the Network Configurator.

1,2,3... 1. Select ***File - Open*** or click the Button. The following dialog box will be displayed.

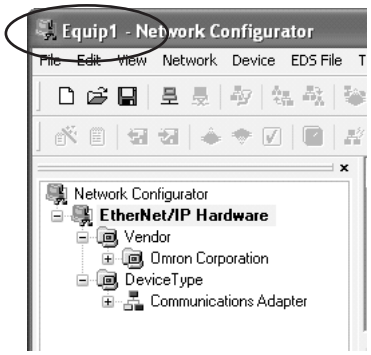


If the network configuration file that you want to read is not displayed, change to (*Look in*) another folder.

2. When you click and select the network configuration file that you want to read, that file name will be displayed in the *File name* Field.



3. Click the **Open** Button to read the network configuration file.
4. The Network Configurator's Title Bar will display the name of the file that was read.



5. Select any of the options as necessary. The options are listed below.

Option	Function
Select target network	Allows you to select specific networks from the network configuration and open them.
Add to current document	Allows you to add the networks from the network configuration file being opened to the current configuration file.

Note The save format will vary depending on the Network Configurator version. Configuration files (*.ncf) created using the Network Configurator for EtherNet/IP (version 2 or higher) can be imported (opened) by selecting ***External Data - Import*** from the File Menu.

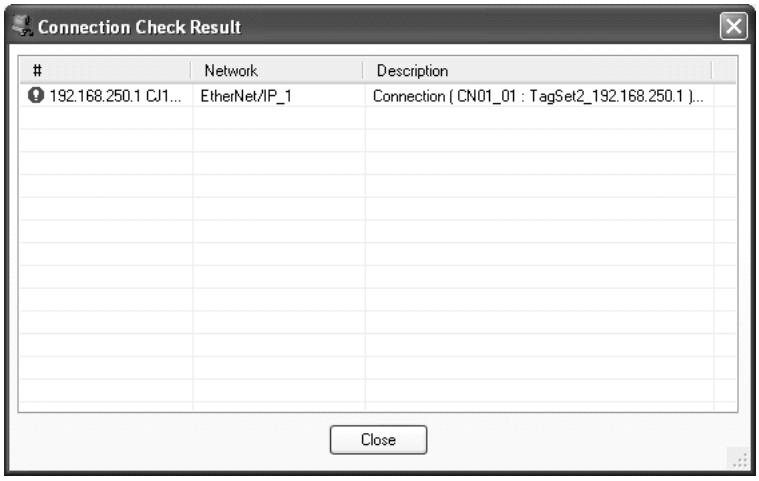
6-2-17 Checking Connections

Check the consistency of connection parameters for network configuration files with device parameters set using the Network Configurator and device parameters uploaded from the network.

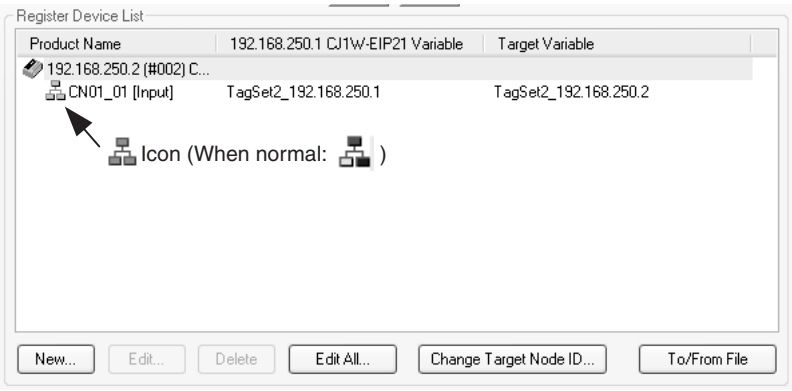
1. Select *Check Connections* in the Network Menu. The following dialog box will be displayed if parameters are normal.



The following dialog box will be displayed if there are parameter errors. Check the displayed details and review the settings.



If an inconsistency occurs, open the originator's Edit Device Parameter Dialog Box and click the **Connection** Tab. The inconsistent connection will be displayed with a  icon (instead of the normal  icon). To change the connection setting and select a different target variable, select the connection as shown below and click the **Edit** Button.



6-2-18 Changing Devices

Devices that are registered in a network configuration with the Network Configurator can be changed. Select ***Change Device*** from the Device Menu to display a list of the devices that can be changed to. Select the desired device.

A device can be changed only when there is complete or upward compatibility with the device being changed to.

Device Changes

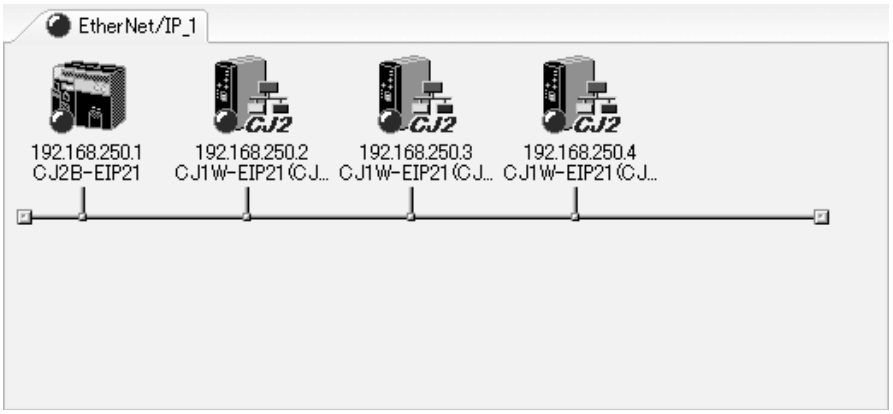
Device after change		CJ1W-EIP21	CS1W-EIP21	CJ1W-EIP21	CS1W-EIP21	CJ1W-EIP (CJ2)	CJ2B-EIP21	CJ2M-EIP21	CJ1W-EIP21	CS1W-EIP21	CJ1W-EIP (CJ2)	CJ2B-EIP21	CS1W-EIP21S	CJ1W-EIP21S	CJ3M-CPU3☐
Device before change		Rev. 1	Rev. 1	Rev. 2	Rev. 2	Rev. 2	Rev. 2	Rev. 2	Rev. 3	Rev. 3	Rev. 3	Rev. 3	Rev. 4	Rev. 4	Rev. 4
CJ1W-EIP21	Rev. 1	---	OK	OK	OK	OK	OK	(See note 2.)	OK	OK	OK	OK	OK	OK	OK
CS1W-EIP21	Rev. 1	OK	---	OK	OK	OK	OK	(See note 2.)	OK	OK	OK	OK	OK	OK	OK
CJ1W-EIP21	Rev. 2	No	No	---	OK	OK	OK	(See note 2.)	OK	OK	OK	OK	OK	OK	OK
CS1W-EIP21	Rev. 2	No	No	OK	---	OK	OK	(See note 2.)	OK	OK	OK	OK	OK	OK	OK
CJ1W-EIP (CJ2)	Rev. 2	No	No	(See note 1.)	(See note 1.)	---	OK	(See note 2.)	(See note 1.)	(See note 1.)	OK	OK	(See note 1.)	(See note 1.)	OK
CJ2B-EIP21	Rev. 2	No	No	(See note 1.)	(See note 1.)	OK	---	(See note 2.)	(See note 1.)	(See note 1.)	OK	OK	(See note 1.)	(See note 1.)	OK
CJ2M-EIP21	Rev. 2	No	No	(See note 1.)	(See note 1.)	OK	OK	---	(See note 1.)	(See note 1.)	OK	OK	(See note 1.)	(See note 1.)	OK
CJ1W-EIP21	Rev. 3	No	No	OK	OK	OK	OK	(See note 2.)	---	OK	OK	OK	OK	OK	OK
CS1W-EIP21	Rev. 3	No	No	OK	OK	OK	OK	(See note 2.)	OK	---	OK	OK	OK	OK	OK
CJ1W-EIP (CJ2)	Rev. 3	No	No	(See note 1.)	(See note 1.)	OK	OK	(See note 2.)	(See note 1.)	(See note 1.)	---	OK	(See note 1.)	(See note 1.)	OK
CJ2B-EIP21	Rev. 3	No	No	(See note 1.)	(See note 1.)	OK	OK	(See note 2.)	(See note 1.)	(See note 1.)	OK	---	(See note 1.)	(See note 1.)	OK
CS1W-EIP21S	Rev. 4	No	No	OK	OK	OK	OK	(See note 2.)	OK	OK	OK	OK	---	OK	OK
CJ1W-EIP21S	Rev. 4	No	No	OK	OK	OK	OK	(See note 2.)	OK	OK	OK	OK	OK	---	OK
CJ3M-CPU3☐	Rev. 4	No	No	(See note 1.)	(See note 1.)	OK	OK	(See note 2.)	(See note 1.)	(See note 1.)	OK	OK	(See note 1.)	(See note 1.)	---

Note (1) Cannnot be changed if a variable is specified as a tag.

(2) Cannot be changed if the following items exceed the permissible settings of the device after the change: Number of I/O connections, number of tags, number of tag sets, and size of one tag set.

6-2-19 Displaying Device Status

Device status is displayed using the following icons in Maintenance Mode. To enter maintenance mode, select ***Large Icons - Maintenance Mode*** from the View Menu.



Icon	Status
(gray)	Offline
(turquoise edge)	Default (no configuration)
(green)	Idle (CPU Unit of PLC is in PROGRAM mode.)
(blue)	Communications normal (CPU Unit of PLC is in RUN or MONITOR mode.)
(yellow)	Warning (A non-fatal error has occurred in the CPU Unit of the PLC.)
(red)	Alarm (A fatal error has occurred in the CPU Unit of the PLC.)

6-3 Ladder Programming with Tag Data Links

6-3-1 Ladder Programming Related to Tag Data Links

If data in the ladder program is linked by tag data links, add conditions 1 to 4 in the ladder program for that data. If you want to use target node PLC flags as input conditions, add conditions 5 and 6.

For details on the various flags, refer to *4-2 CIO Area Allocations*.

Conditions showing the built-in EtherNet/IP Unit's Tag Data Links are enabled:

1. The Unit Error Occurred Flag (n+10, bit 00) is OFF,
2. and the Online Flag (n+11, bit 00) is ON,
3. and the Tag Data Link Operating Flag (n+11, bit 01) is ON.

Conditions showing that connections are established with the target device, and tag data links are operating:

4. The corresponding Normal Target Node Flag (in words n+20 to n+23) is ON.

   The location of the Normal Target Node Flags depends on the layout setting. For details on the layout settings, refer to *4-2-2 Details of the Allocated CIO Area Words*.

Condition showing that the Target Node PLC is operating (OMRON PLCs only):

5. The corresponding Target Node PLC Operating Flag (in words n+2 to n+5) is ON.

Condition showing the Target Node PLC's fatal or non-fatal error status (OMRON PLCs only):

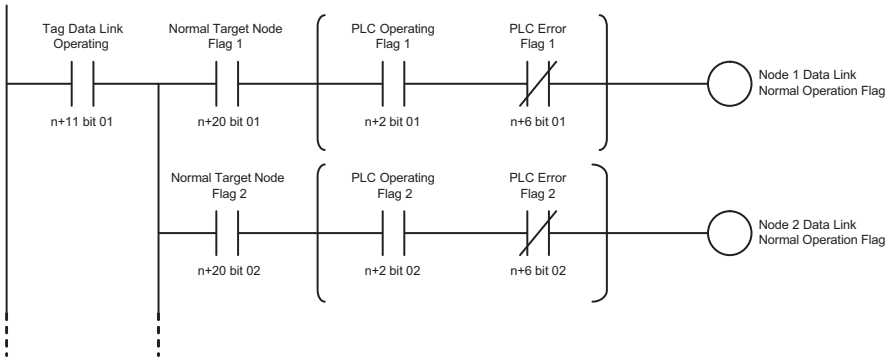
6. The corresponding Target Node PLC Error Flag (in words n+6 to n+9) is OFF.

   When you want to use the Target Node PLC Error Flag, the PLC status must be included in the tag sets for both the originator and target. Include the PLC status by using the Network Configurator to select the *Include* Options in the Edit Tag Set Dialog Boxes. For details, refer to *6-3-2 Status Flags Related to Tag Data Links*.

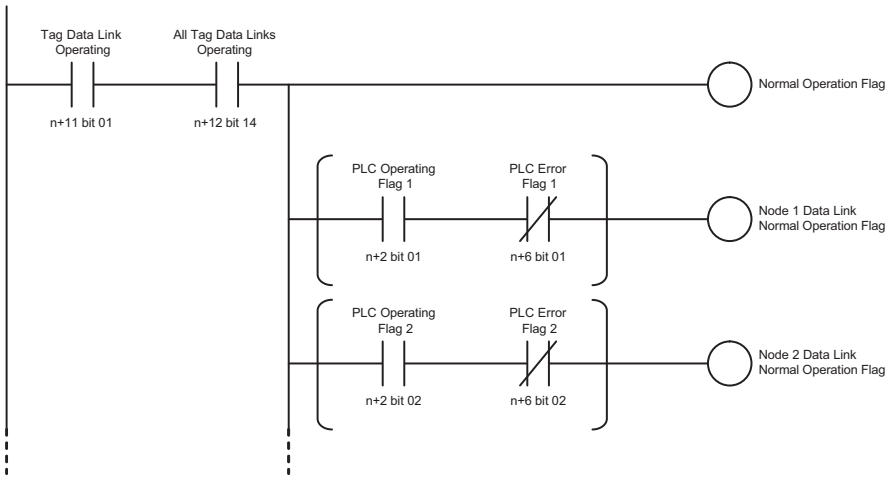
Example of Programming to Detect Normal Status

The following programming can be used to confirm that normal communications are being performed for each target node. If the PLC status is included in the tag data, the status of the PLC can also be detected.

Programming for EtherNet/IP Units or Built-in EtherNet/IP Ports with Revision 2 or Higher



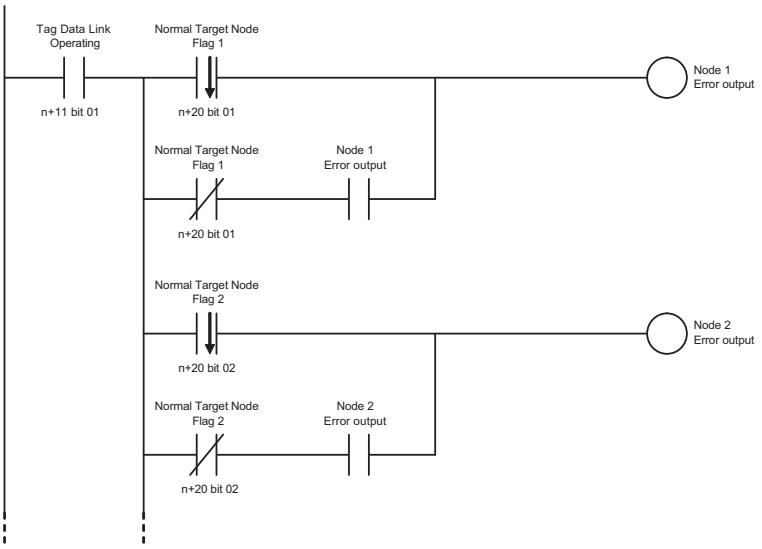
Programming for All Revisions



Programming to Detect Errors: Example 1

The following programming can be used to check for errors for each target node. This programming is used to detect errors only after the data links for all nodes have started normally.

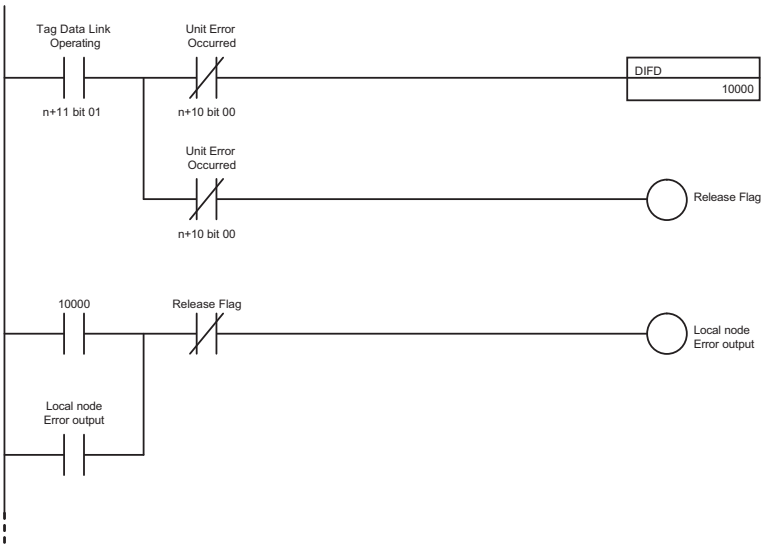
Programming for EtherNet/IP Units or Built-in EtherNet/IP Ports with Revision 2 or Higher



Programming to Detect Errors: Example 2

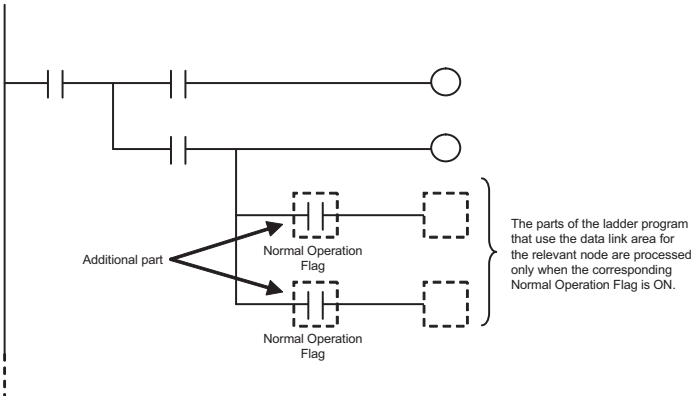
The following programming can be used to detect tag data link errors at the local node.

Programming for All Revisions

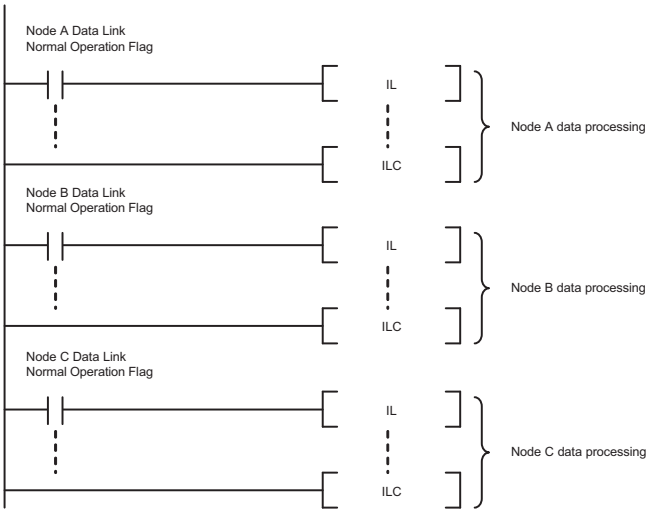


Example of Programming to Process Data

The following type of programming can be used to process data only when the data links are operating normally.



Interlocks (IL and ILC instructions) and jumps (JMP and JME instructions) can also be used to process data only when the data links are operating normally as shown below.



Note Even if an error occurs in communications with a target device, the input data from the target device will remain stored in words allocated in memory to the local node. To prevent malfunctions, write the ladder program so that input data processing will not be performed when the Unit Error Occurred Flag (word n+10 bit 00) is ON.

6-3-2 Status Flags Related to Tag Data Links

The status of the tag data links is reflected in the following words.

Name (allocated area)	Contents
Target Node PLC Operating Flag Information Layout set to default settings: Words n+2 to n+5 Layout set to user settings: Words n+32 to n+47 **Note** Corresponds to the PLC status's PLC Operating Flag.	Each flag indicates the operating status of the corresponding target node PLC of connections in which the EtherNet/IP Unit is the originator. The flag corresponding to the target node's target ID will be ON when the PLC Operating Flags for all connections with that target node indicate that the PLC is operating. Each node address's flag location (i.e., target ID) can be changed from the Network Configurator. The PLC status flags are enabled when the PLC status is included in the communications data for both the originator and target. The data in this table is refreshed when necessary.
Target Node PLC Error Flag Information Layout set to default settings: Words n+6 to n+9 Layout set to user settings: Words n+48 to n+63 **Note** Corresponds to the PLC status's PLC Error Flag.	Each flag indicates the error status (logical OR of non-fatal and fatal errors) of the corresponding target node PLC of connections in which the EtherNet/IP Unit is the originator. The flag corresponding to the target node's target ID will be ON if even one error is indicated in any of the connections with that target node. Each node address's flag location (i.e., target ID) can be changed from the Network Configurator. The PLC status flags are enabled when the PLC status is included in the communications data for both the originator and target. The data in this table is refreshed when necessary.
Normal Target Node Flag Table Layout set to default settings: Words n+20 to n+23 Layout set to user settings: Words n+16 to n+31 **Note** Does not correspond to the PLC status.	Each flag indicates the connection status of the corresponding target node PLC of connections in which the EtherNet/IP Unit is the originator. The flag corresponding to the target node's target ID will be ON when connections are established for all connections with that target node indicate that the PLC is operating. Each node address's flag location (i.e., target ID) can be changed from the Network Configurator. The data in this table is refreshed when necessary.

6-4 QuickConnect

QuickConnect is used for robots, tool changers, and similar application devices to support requests for rapid devices changes, such as for tools, during network operation. When the EtherNet/IP Unit is used as the originator, it supports QuickConnect.

By using the EtherNet/IP Unit as the originator, connections can be opened and closed for individual target nodes. This is achieved by executing services of the Connection Configuration object of the EtherNet/IP Unit. Refer to *9-2-2 Connection Configuration Object* for object specifications.

Note QuickConnect can be used for CS1W/CJ1W-EIP21S and CJ3M-CPU3□.

SECTION 7
Message Communications Functions

This section describes message communications using FINS messages and explicit messages.

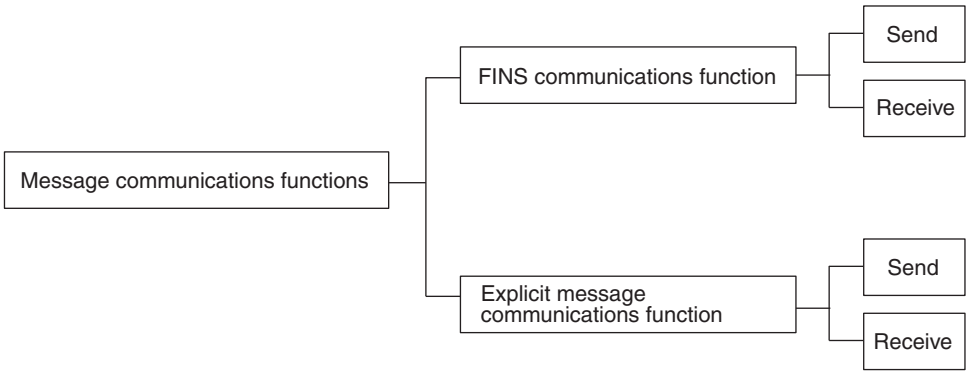
7-1 Overview 228
7-2 FINS Message Communications 230
7-3 Explicit Message Communications 232
7-4 Message Communications Specifications 233
7-5 Message Communications Error Indications 234
7-6 Message Communications Errors 235

7-1 Overview

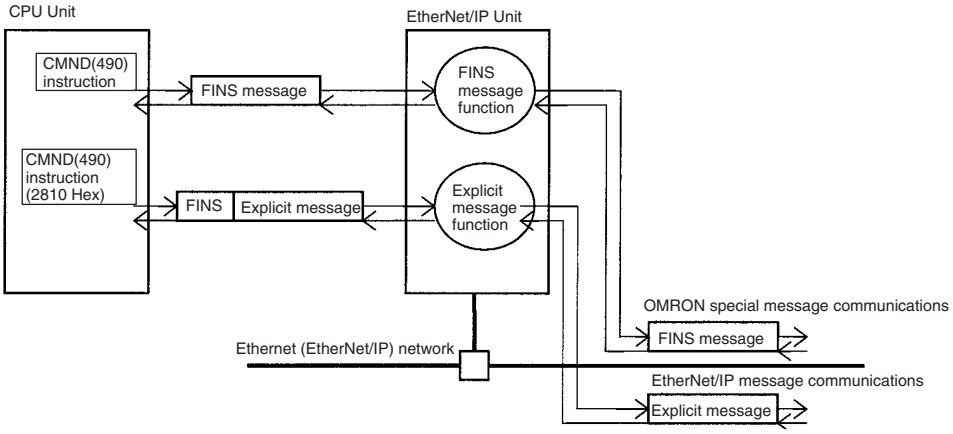
The message communications functions send command/response messages between nodes on the Ethernet network. The messages can be sent between a computer and PLC, between two PLCs, between an OMRON PLC and a master made by another company, or between slaves. The messages can be used to send/receive data; read time data, error logs, and other data; or control operation, e.g., by force-setting/resetting bits.

There are two types of messages: FINS messages and explicit messages.

Item	FINS messages	Explicit messages
Outline	Message communications for OMRON products that use the FINS protocol.	Standard ODVA message communications using the CIP protocol.
Remote device	• Computer with an Ethernet interface • OMRON PLCs (with a CS/CJ-series EtherNet/IP Unit, built-in EtherNet/IP port, or Ethernet Unit)	• Computer with an Ethernet interface • Another company's masters or slaves. • OMRON PLCs (with a CS/CJ-series EtherNet/IP Unit or built-in EtherNet/IP port)
Features	• Send and receive the various FINS commands to provide an even greater range of services than the CIP UCMM messages. • Provide transparency in message communications with other OMRON networks, such as Controller Link, SYSMAC LINK, and Ethernet. (CS1/CJ1 CPU Units with unit version 2.0 or later or CJ2/CJ3 CPU Units: Up to 8 levels, CPU Units with unit version earlier than 2.0: Up to 3 levels)	• Supports message communications with other companies' EtherNet/IP devices. CS/CJ Series • CS1W-EIP21/EIP21S • CJ1W-EIP21/EIP21S • CJ2H-CPU□□-EIP • CJ2M-CPU3□ • CJ3M-CPU3□



Overall Structure

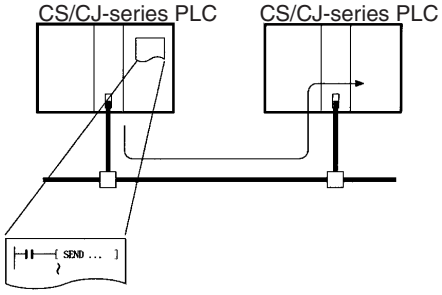
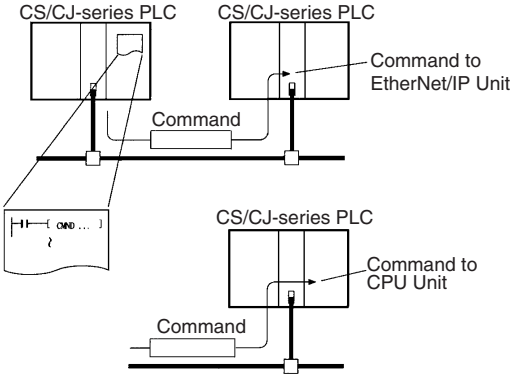


Note With the EtherNet/IP Unit or built-in EtherNet/IP port, message communications are possible even if the I/O link function is disabled.

7-2 FINS Message Communications

Messages containing FINS commands can be exchanged over the Ethernet network between nodes that support FINS messages.

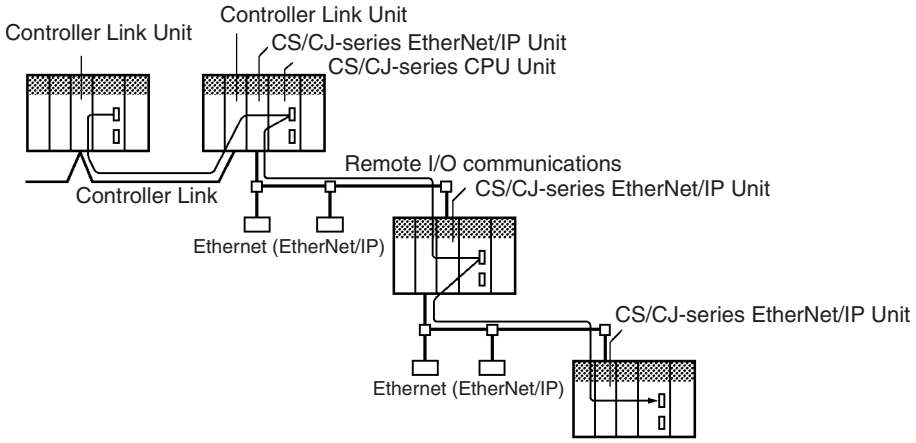
Note FINS message communications can be executed without any particular restrictions over the Ethernet network with OMRON Ethernet Units, computers (CX-One or Fins Gateway applications), and NS-series Programmable Terminals.

Type of FINS message	Data send/receive commands	Any kind of FINS command
Network communications instructions	**SEND/SEND2/RECV/RECV2 instructions**	**CMND/CMND2 instructions**
PLC to PLC (both must be CS/CJ-series PLCs with a CS/CJ-series EtherNet/IP Unit, built-in EtherNet/IP port, or Ethernet Units) (See note 1.) **Note** Inter-network communications are possible with Ethernet networks or other networks, such as Controller Link. (See note 2.)		
Data length (excluding command code)	SEND/SEND2 instruction: 990 words, RECV/RECV2 instruction: 990 words.	CMND/CMND2 instruction: 1,990 bytes max.

Note

1. When two or more Communications Units (including the EtherNet/IP Units and built-in EtherNet/IP ports) are mounted to a CS/CJ-series PLC and FINS messages are being used, the EtherNet/IP Units and built-in EtherNet/IP ports must be registered in the CS/CJ-series PLC's local network routing table. The commands will not be sent if the Unit is not registered in the routing tables.
2. When a CS/CJ-series EtherNet/IP Unit or built-in EtherNet/IP port is connected to an Ethernet network, message communications can be conducted between networks, including other Ethernet networks as well as other networks such as Controller Link and SYSMAC LINK. Up to eight levels of networks can be crossed, provided that routing tables (containing local network tables and relay network tables) have been registered in the CPU Units of each PLC on the network.
3. A Programming Device connected to the CPU Unit of a PLC connected to the network can be used to program and monitor another PLC that is on the network. Up to eight levels of networks can be crossed for CS1/CJ1-series CPU Units with unit version 2.0 or later, CJ2/CJ3 CPU Units, and CX-Programmer version 4.0 or higher.

Up to 8 network levels, including the EtherNet/IP network, can be crossed.



Note FINS commands sent and received by the CS/CJ-series EtherNet/IP Unit include commands addressed to the CS/CJ-series CPU Unit and commands addressed to the CS/CJ-series EtherNet/IP Unit.

7-3 Explicit Message Communications

Explicit messages defined in EtherNet/IP can be used to send service requests to other companies' EtherNet/IP masters/slaves and OMRON PLCs with CS/CJ-series EtherNet/IP Units and built-in EtherNet/IP ports.

Note Specific FINS commands (commands 2810 and 2801) are used to send explicit messages.

Explicit message	Sending	Receiving
Network communications instruction	CIP UCMM messages can be sent to an EtherNet/IP Unit or built-in EtherNet/IP port by a CMND/CMND2(490) instruction containing FINS command code 2810 Hex.	Automatically responds to explicit messages from other devices.
Functions supported in remote devices	• Masters/slaves made by other manufacturers: Supported services determine supported functions. • PLC with a CS/CJ-series EtherNet/IP Unit or built-in EtherNet/IP port: Supports the reading/writing of a remote CPU Unit's status information and I/O memory data.	• Masters made by other manufacturers • PLC with a CS/CJ-series EtherNet/IP Unit or built-in EtherNet/IP port: Supports the reading/writing of the local CPU Unit's status information and I/O memory data.

Note The CS/CJ-series EtherNet/IP Units and built-in EtherNet/IP ports contain a PLC Object, so that other devices can read/write the I/O memory of the CPU Unit with the built-in EtherNet/IP port or the CPU Unit to which the EtherNet/IP Unit is mounted.

7-4 Message Communications Specifications

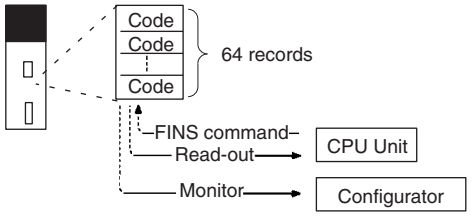
CPU Unit function		CS/CJ Series
Unit model number		CS1W-EIP21, CS1W-EIP21S, CJ1W-EIP21, CJ1W-EIP21S, CJ2H-CPU□□-EIP, or CJ2M-CPU3□, CJ3M-CPU3□
Communications instructions	**Sending/ receiving data**	SEND/SEND2 and RECV/RECV2 instructions
	FINS commands	CMND/CMND2 instruction
		There are two kinds of FINS commands: commands addressed to the CPU Unit, and commands addressed to the CS/CJ-series EtherNet/IP Unit or built-in EtherNet/IP port.
	Sending EtherNet/IP CIP UCMM messages	CMND/CMND2 instruction
		Sends CIP UCMM messages to other companies' masters/slaves, or PLCs with a CS/CJ-series EtherNet/IP Unit or built-in EtherNet/IP port mounted.
Number of destination nodes	**FINS message communications**	1:N communications
	Explicit message communications	1:N communications Send functions: CIP unconnected (UCMM) communications only Receive functions: CIP unconnected (UCMM) and CIP connected (Class 3) communications
Transmission data length (not including the command code)	**FINS message communications**	• SEND/SEND2: 990 words (1,980 bytes) max. normally, or 727 words (1,454 bytes) max. when broadcasting • RECV/RECV2: 990 words (1,980 bytes) max. • CMND/CMND2: 1,990 bytes max. normally, or 1,462 bytes max. when broadcasting (data after the FINS command code)
	Explicit message communications	CMND/CMND2: 492 bytes max.
No. of simultaneous instructions		One each for 8 ports (ports 0 to 7) Refer to *Network Instructions* in the *CS/CJ Series Programmable Controllers Instructions Reference Manual* (W474) for information on ports (logical ports).
Response monitoring time		Default setting: 2 s User setting: 0.1 to 6553.5 s
Retries		0 to 15
Internetwork connections	**Same network type**	Supports internetwork communications between Ethernet networks connected to CS/CJ-series EtherNet/IP Units and built-in EtherNet/IP ports (up to 3 levels).
	Different network type	Supports internetwork communications between the EtherNet/IP network connected to a CS/CJ-series EtherNet/IP Unit or built-in EtherNet/IP port and other networks such as Controller Link or SYSMAC LINK (up to 3 levels).

7-5 Message Communications Error Indications

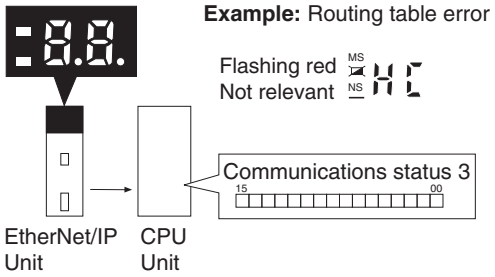
There are two ways to obtain information on communications errors that occur in message communications: checking the EtherNet/IP Unit's error log or checking its indicators.

1,2,3... 1. Each time a communications error occurs, an error code is placed in an error record in the error log stored in RAM in the EtherNet/IP Unit or CPU Unit with the built-in EtherNet/IP Port. Up to 64 records can be stored in the error log. The time and date that the error occurred are also recorded together.

The error log can be read or cleared from the CPU Unit by sending an FINS command to the EtherNet/IP Unit (Error Log Read/Clear). The contents of the error log can also be monitored from the Configurator.



2. When a communications error has occurred, details on the error are indicated by the MS and NS indicators and the 7-segment display on the front panel of the EtherNet/IP Unit or CPU Unit with the built-in EtherNet/IP port. This information can be used for troubleshooting.



7-6 Message Communications Errors

The following table shows the main errors that may occur when messages are sent or received. Refer to *SECTION 16 Modbus Client Function* for corrective measures and details on errors that are recorded in error log but not indicated by the LED indicators.

Error	Indicators			Error code (Hex)
	MS	NS	7-segment display (See note.)	
Routing table error	Flashing red	No change	HC	021A
IP address duplication error	No change	Lit red	F0	0211
CPU Unit service monitoring error	Flashing red	No change	HE	0002
Other CPU error		Not lit	H7	0006
Too many retries, cannot send	No change	No change	No change	0103
Node address setting error, cannot send				0105
Remote node not part of network, cannot send				0107
No Unit with specified unit address, cannot send				0108
CPU Unit error occurred, cannot send				010B
Destination address not set in routing tables, cannot send				010D
Routing tables not registered, cannot send				010E
Routing tables error occurred, cannot send				010F
Too many relay connections, cannot send				0110
Maximum command length exceeded, cannot send				0111
Header error; cannot send				0112
Reception buffer full, packet discarded				0117
Invalid packet discarded				0118
Local node busy, cannot send				0119
Unexpected routing error				0120
Service not supported in present mode, packet discarded				0122
Transmission buffer full, packet discarded				0123
Maximum frame length exceeded, routing impossible				0124
Packet discarded due to response time-out				0125

Note The 7-segment display alternately displays the error and the node address of the node where the error occurred.

SECTION 8
FINS Communications

This section provides information on communicating on EtherNet/IP Systems and interconnected networks using FINS commands. The information provided in the section deals only with FINS communications in reference to EtherNet/IP Units or built-in EtherNet/IP ports.

FINS commands issued from a PLC are sent via the SEND(090), RECV(098), and CMND(490) instructions programmed into the user ladder-diagram program. Although an outline of these instructions is provided in this section, refer to the *CS/CJ Series Programmable Controllers Instructions Reference Manual* (W474) for further details on programming these instructions.

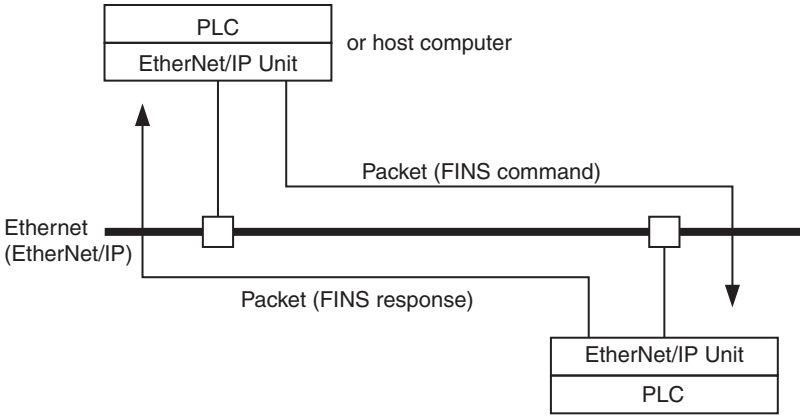
8-1 Overview of FINS Communications 238
8-1-1 Communications On an Ethernet Network 238
8-1-2 Using the FINS/UDP and FINS/TCP Methods 239
8-1-3 FINS Communications Service Specifications 239
8-2 FINS/UDP Method 240
8-2-1 Overview 240
8-3 FINS/TCP Method 242
8-3-1 Overview 242
8-4 Routing Tables 247
8-4-1 Routing Table Overview 247
8-4-2 Connecting and Using a Peripheral Device for the PLC 248
8-4-3 Routing Table Setting Examples 249
8-5 Using FINS Applications. 251
8-5-1 CX-Programmer (CX-Server) 251
8-5-2 FinsGateway 255
8-6 Communicating between OMRON PLCs 260
8-6-1 Communications Specifications 260
8-6-2 PLC Communications Data Areas. 261
8-6-3 Using SEND, RECV, and CMND. 262
8-6-4 Writing Programs 266
8-6-5 Program Example 270
8-7 Precautions on High Traffic in FINS Communications 272

8-1 Overview of FINS Communications

8-1-1 Communications On an Ethernet Network

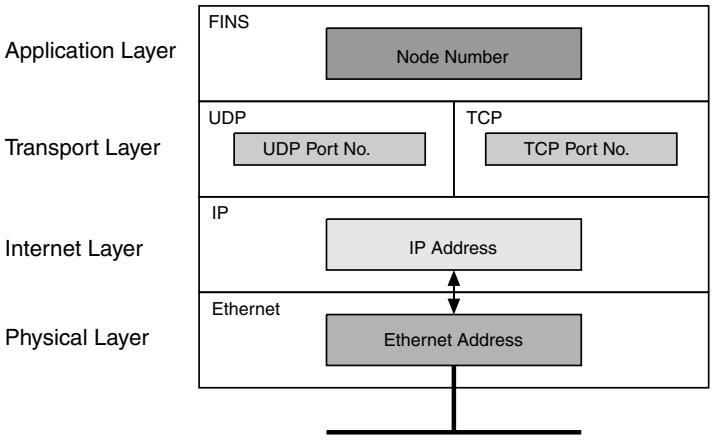
The EtherNet/IP Units and built-in EtherNet/IP ports support the FINS communications service, which can be used simultaneously with the CIP communications service.

FINS communications data is sent and received as UDP/IP packets or TCP/IP packets.



In the FINS communications service, both an IP address for IP (the Internet layer) and a FINS node address for FINS (the application layer) are used for the remote device. Also, 9600 is used as the default setting for the local UDP or TCP port number (i.e., the transport layer) for identifying the application layer, i.e., the FINS communications service. (Another number can be set for the FINS/UDP port from the Setup Tab Page in the Unit Setup.)

For details on pairing FINS node addresses with IP addresses and UDP/TCP port numbers, refer to *5-2 IP Addresses in FINS Communications*.



The FINS communications service is a communications method based on UDP/IP, and it is supported by most OMRON Ethernet-related products. (In this manual it is called the FINS/UDP method.) In addition to supporting the FINS/UDP method, support FINS communications using TCP/IP. (In this manual, this is called the FINS/TCP method.)

8-1-2 Using the FINS/UDP and FINS/TCP Methods

It is recommended that FINS/UDP and FINS/TCP be used as follows:

- When remote devices do not support the FINS/TCP method: Use the FINS/UDP method for FINS communications with those devices.
- When FINS nodes are connected on the same Ethernet segment: Use the FINS/UDP method between those nodes.

  Note FINS/UDP offers a slight advantage in performance.
- When FINS nodes are connected over multiple IP network layers: Use the FINS/TCP method between those nodes.

  Note FINS/TCP offers superior communications quality.
- When the quality of connections is unreliable, as with wireless LAN: Use the FINS/TCP method between those nodes.

  Note FINS/TCP offers superior communications quality.

8-1-3 FINS Communications Service Specifications

Item	Specifications	
Number of nodes	254	
Message length	2,012 bytes max.	
Number of buffers	192	
Protocol name	FINS/UDP method	FINS/TCP method
Protocol used	UDP/IP	TCP/IP
Number of connections	---	16
Port number	9600 (default) Can be changed.	9600 (default) Can be changed.
Protection	No	Yes (Specification of client IP addresses when Unit is used as a server)
Keep-alive time **(See note 1.)**	No	Common items for all connections The setting range is 0 to 65,535 minutes. (The default is 0, meaning that the checking time is 5 minutes.)
Other	Items set for each UDP port • Broadcast • IP Address Conversion	Items set for each connection • Server/client specification • Remote IP address specification When client: Specify the IP address of the remote Unit (server). When server: Specify IP addresses of clients permitted to connect. • Automatic FINS node address allocation: Specify automatic allocation of client FINS node addresses. • Keep-alive: Specify whether remote node keep-alive is to be used.
Internal table	This a table of correspondences for remote FINS node addresses, remote IP addresses, TCP/UDP, and remote port numbers. It is created automatically when power is turned ON to the PLC or when the Ethernet Unit is restarted, and it is automatically changed when a connection is established by means of the FINS/TCP method or when a FINS command received. The following functions are enabled by using this table. • IP address conversion using the FINS/UDP method • Automatic FINS node address conversion after a connection is established using the FINS/TCP method • Automatic client FINS node address allocation using the FINS/TCP method • Simultaneous connection of multiple FINS applications	

Note (1) This setting is provided for CS1W/CJ1W-EIP21S or CJ3M-CPU3□ only. CS1W/CJ1W-EIP21, CJ2H-CPU6□-EIP or CJ2M-CPU3□, the keep-alive time is fixed to 5 minutes.

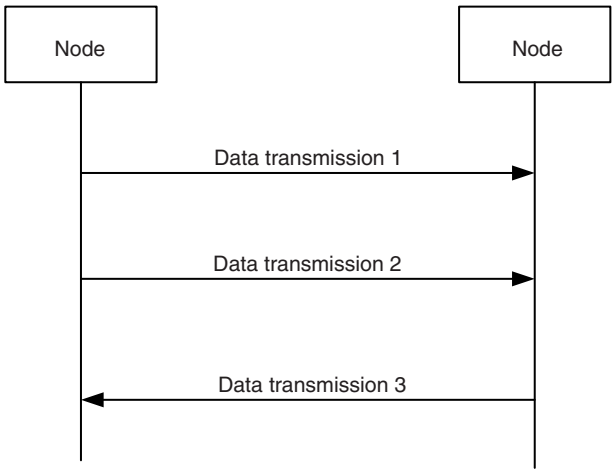
8-2 FINS/UDP Method

8-2-1 Overview

FINS/UDP Features

The FINS/UDP method is a FINS communications method that uses the UDP/IP protocol. UDP/IP is a connectionless communications protocol. When a message is sent from one node to another, the two nodes have an equal relationship and there is no clear connection. If using TCP is like making a telephone call, then UDP is more like delivering a memo by hand. Although the UDP protocol is fast, data communications are less reliable than with TCP.

In particular, when sending large amounts of data involving significant routing, the user must program measures, such as retries, into applications in order to improve reliability.



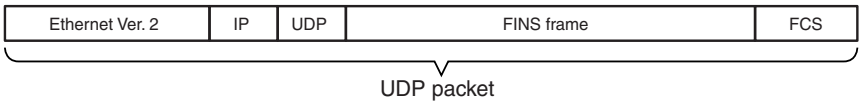
Data is sent in one direction, with no confirmation of whether the data was received. Because there are few procedures involved, data can be sent at high speed but with less reliability than with TCP.

The FINS/UDP method has the following features:

- Because FINS/UDP is a connectionless protocol, there is no limit to the number of corrections.
- FINS/UDP can be used for broadcasting.
- When data is sent via an IP network with multiple layers (such as the Internet), communications reliability drops.

FINS/UDP Frame Format

The following diagram shows the structure of a UDP packet used for sending and receiving data on an Ethernet network.



As the diagram shows, a nested structure is used with the FINS/UDP method, i.e., Ethernet Ver. 2, IP frame, UDP frame, and FINS frame. A UDP data section (FINS frame) that exceeds 1,472 bytes is split into packets for transmission. The split UDP data is then joined automatically at the UDP/IP protocol layer. There is normally no need to pay attention at the application layer to this split, but it may not be possible to send 1,472-byte UDP packets over an IP network with multiple layers. When using the FINS communications service in a system such as this, select the FINS/TCP method.

UDP Port Numbers for FINS/UDP

The UDP port number is the number for UDP to identify the application layer (i.e., the FINS communications service in this case). When communications are executed by UDP/IP, this port number must be allocated to the communications service.

The default setting for the UDP port number (i.e., the UDP port number of the EtherNet/IP Unit or built-in EtherNet/IP port) is 9600. To set another number, set the number on the FINS/UDP Tab Page of the CX-Programmers Edit Parameters Dialog Box.

At the EtherNet/IP Unit or built-in EtherNet/IP port, a UDP/IP frame received with a FINS/UDP port number is recognized as a FINS frame.

Procedure for Using FINS/UDP

1,2,3...

1. Make the basic settings.
   Refer to *Initial Settings* in *3-1-1 Procedures*.
2. Keep the CX-Programmer connected online, right-click the EtherNet/IP Unit or built-in EtherNet/IP port in the PLC IO Table Dialog Box, and select ***Edit - Unit Setup***. Set the following in the CPU Bus Unit Setup Area from the FINS/UDP Tab Page of the Edit Parameters Dialog Box.
   - Use of FINS/UDP (CS1W/CJ1W-EIP21S or CJ3M-CPU3□ only)
   - FINS/UDP Port No. (Default: 9600)
   - IP Address Conversion
   - IP Address Table
     When the IP address conversion method is set to the IP address table.
   - Dynamic Change of remote IP addresses
3. Select ***Transfer to PLC*** from the PLC Menu and click the **Yes** Button. The setting data will be transferred to the nonvolatile memory of the EtherNet/IP Unit or built-in EtherNet/IP port.
4. Make the routing table settings and transfer them to each PLC. (See note.)
   Set the routing tables with CX-Integrator, and transfer it to each PLC.
5. Create a ladder program that includes the SEND/SEND2, RECV/RECV2, and CMND/CMND2 instructions.

Note Routing tables are required in the following situations:

- When communicating with a PLC or computer on another network (e.g., remote programming or monitoring using FINS messages or a CX-Programmer).
- When multiple Communications Units are mounted to a single PLC (i.e., CPU Unit).
- When routing tables are used for one or more other nodes on the same network.

It is not necessary to set routing tables if one Communications Unit is mounted to the PLC and the nodes are connected as one network.

8-3 FINS/TCP Method

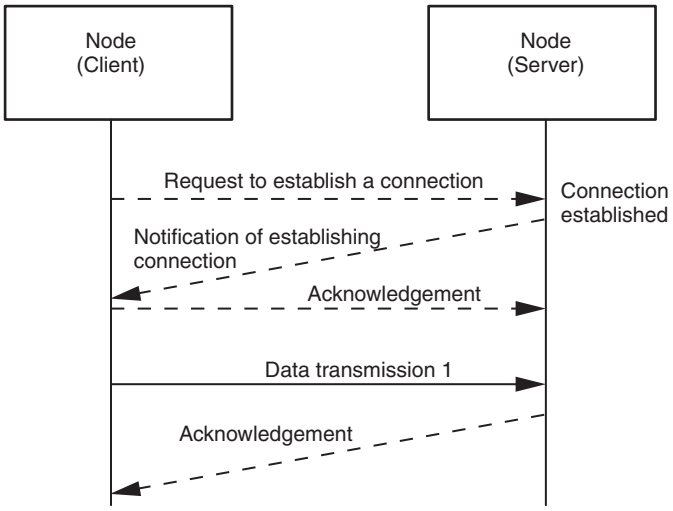
8-3-1 Overview

FINS/TCP Features

The FINS/TCP method is a FINS communications method that uses the TCP/IP protocol. TCP/IP is a connection-type communications protocol. Before a message is sent from one node to another, it is necessary to establish a virtual circuit, i.e., a connection. Once a connection has been established, communications are quite reliable. The arrival of data that is sent via the connection is confirmed by an acknowledgement (ACK) response, and retries are executed automatically as required.

When FINS/TCP is used, it must be determined which node is the server and which nodes are the clients.

For communications between a personal computer and a PLC, the computer should normally be set as the client and the PLC as the server. For communications between two PLCs, either one can be set as the client and the other as the server.



An acknowledgement is received whenever a connection is established or data is sent, so transmissions are more reliable but somewhat slower.

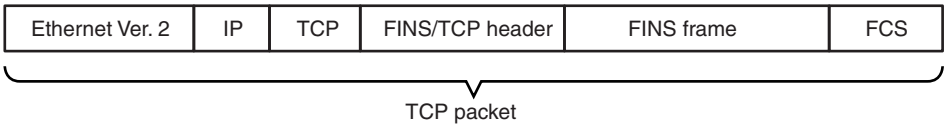
Compared to the FINS/UDP method, the FINS/TCP method has the following characteristics.

- Data transmission is more reliable, due to factors such as retry processing at the TCP/IP layer. The FINS/TCP method is thus better suited to dealing with communications errors in an IP network that spans several layers.
- Remote clients can be restricted by means of settings at the server (i.e., the server can be protected from access by non-specified IP addresses).
- Broadcasting cannot be used.
- TCP/IP has various retry procedures, and this tends to lower its performance in comparison with UDP/IP.
- There is a limit to the number of connections that can be made (i.e., 16 connections maximum), and any given node can communicate only with up to 16 other nodes at a time.

- After a FINS/TCP connection (connection number, remote IP address) has been set in the FINS/TCP Tab Page of the Network Configurator's Edit Parameters Dialog Box, it can be dynamically changed from the ladder program using a FINS command (i.e., FINS/TCP CONNECTION REMOTE NODE CHANGE REQUEST).

FINS/TCP Frame Format

The following diagram shows the structure of a TCP packet sent over an Ethernet network.



As the diagram shows, a nested structure is used with the FINS/TCP method, i.e., Ethernet Ver. 2, IP frame, TCP frame, FINS/TCP header frame, and FINS frame. A TCP data section (FINS/TCP header + FINS frame) that exceeds the segment size (default setting of 1,460 bytes, or 1,024 bytes in the EtherNet/IP Unit or built-in EtherNet/IP port on other than CS1W/CJ1W-EIP21S with automatic adjustment for optimum values between the nodes) is split into TCP packets for transmission. The split TCP data is then joined automatically at the remote node's TCP/IP protocol layer. The TCP/IP protocol layer, however, cannot determine where the data has been split, so the TCP data sections from multiple packets are all joined together. Therefore, when using the FINS/TCP method, FINS/TCP headers must be added at the beginning of FINS frames in order to serve as FINS frame delimiters. The length of the data in the following FINS frame is stored in the header, allowing the frame to be separated out by the remote node. With the EtherNet/IP Unit or built-in EtherNet/IP port and FinsGateway (Ver. 2003 or higher) the appropriate frames are separated out automatically, so there is normally no need to be pay attention to it at the application layer.

TCP Port Number for FINS/TCP

The TCP port number is the number for TCP to identify the application layer (i.e., the FINS communications service in this case). When communications are executed using TCP/IP, this port number must be allocated for the communications service.

The default setting for the TCP port number (i.e., the TCP port number of the EtherNet/IP Unit or built-in EtherNet/IP port) is 9600. To set another number, make the setting for the FINS/TCP port on the FINS/TCP Tab Page of the CX-Programmer's Edit Parameters Dialog Box.

The FINS/TCP port number set in the FINS Configuration Tab Page is used by the FINS/TCP server's TCP socket. The FINS/TCP client's TCP socket uses any TCP port number that can be used at that node. (With the EtherNet/IP Unit or built-in EtherNet/IP port and FinsGateway (Ver. 2003 or higher), an unused TCP port is automatically detected and utilized.)

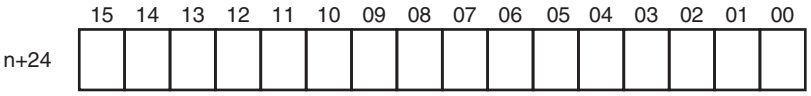
At the EtherNet/IP Unit or built-in EtherNet/IP port, a TCP/IP frame that is received is recognized as a FINS frame, according to the remote TCP port number in the frame.

FINS/TCP Connection Numbers

FINS/TCP allows up to 16 FINS/TCP connections to be established simultaneously, and these 16 connections are managed at the EtherNet/IP Unit or built-in EtherNet/IP port by connection numbers. When setting FINS/TCP connection settings in the FINS/TCP Tab Page of the Network Configurator's Edit Parameters Dialog Box, set them individually using these connection numbers.

FINS/TCP Connection Status (Word n+24)

While a connection with a remote node is established, the bit corresponding to the FINS/TCP connection status turns ON in the section of the CPU Bus Unit words allocated in the CIO Area. The bit turns OFF if the connection is terminated by a communications error or a FINS command (i.e., FINS/TCP CONNECTION REMOTE NODE CHANGE REQUEST).

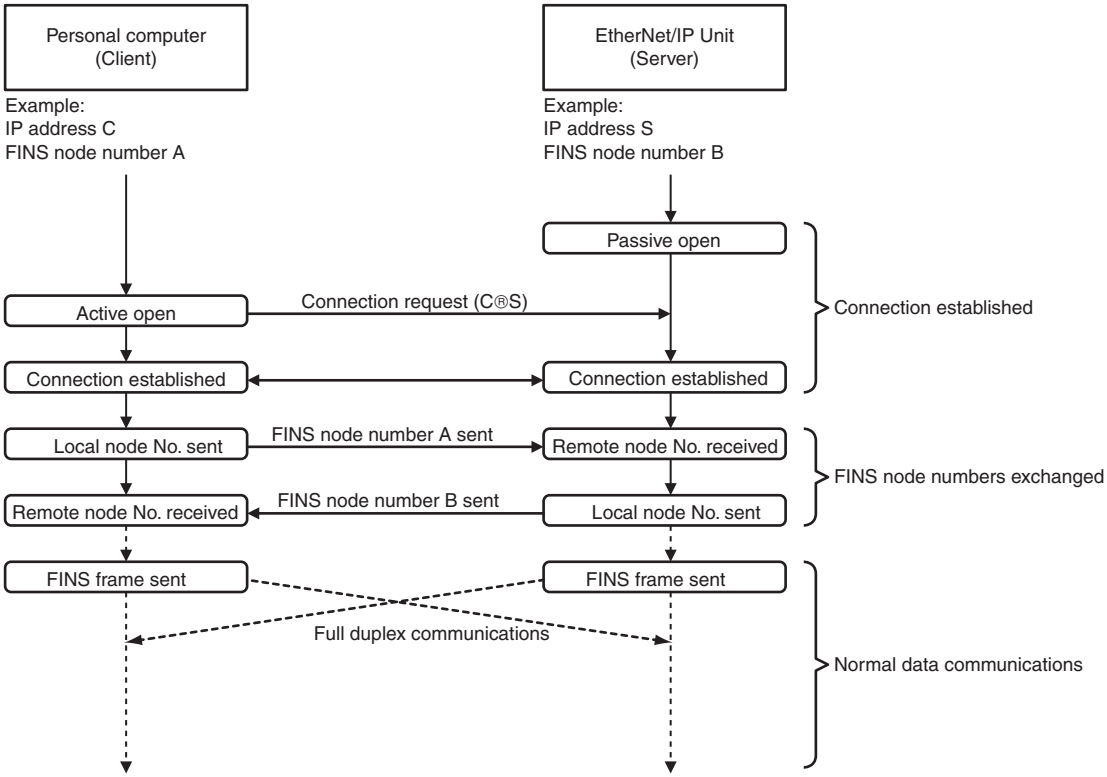


*: Bit 15 corresponds to connection No. 16, bit 00 to connection No. 1, etc.

Note The starting word of the FINS/TCP Connection Status Area is different in the CS1W-ETN21 and CJ1W-ETN21 Ethernet Units; it is n+23 in the Ethernet Units. If a ladder program using FINS/TCP communications was created for Ethernet Units, and is being reused for EtherNet/IP Units and built-in EtherNet/IP ports, change the word starting word address for this area from n+23 to n+24.

FINS/TCP Communications Procedure

With FINS/TCP, FINS node addresses are exchanged immediately after a connection is established. This makes it possible to determine the FINS node addresses to which the 16 connection numbers, and to manage them in an internal table.



After a connection has been established as a FINS/TCP server, it is terminated in the following ways.

- When the connection is closed by the client.
- When a FINS command to close the connection (FINS/TCP CONNECTION REMOTE NODE CHANGE REQUEST) is sent by the client.
- When there is no response from the client when the keep-alive function is in effect.

After a connection has been established as a FINS/TCP client, it can be terminated in the following ways.

- If the connection is closed by the server.
- If there is no response from the client when the keep-alive function is in effect.

Even if the connection is closed at the FINS/TCP client, requests continue to be made to the FINS/TCP server every few seconds to open a connection.

Note After the EtherNet/IP Unit or built-in EtherNet/IP port is powered up or restarted, the IP address for the connection used as the FINS/TCP client is the remote IP address that was set in the FINS/TCP Tab Page of the CX-Programmer's Edit Parameters Dialog Box. To dynamically change the remote IP address (i.e., during CPU Unit operation), execute the CMND(490) instruction in the ladder program and send a FINS command (FINS/TCP CONNECTION REMOTE NODE CHANGE REQUEST; command code: 27 30 hexadecimal) to the EtherNet/IP Unit or built-in EtherNet/IP port.

Procedure for Using FINS/TCP

1,2,3...

1. Make the basic settings.
   Refer to *Initial Settings* in *3-1-1 Procedures*.
2. Make the following settings on the FINS/TCP Tab Page of the CX-Programmer's Edit Parameters Dialog Box.
   - Use of FINS/TCP (CS1W/CJ1W-EIP21S or CJ3M-CPU3□ only)
   - FINS/TCP port (default: 9600)
   - FINS Connection Settings
     Server/Client: Specifies whether the connection will operate in FINS/TCP server mode.
   - Target IP address for client: Specifies the IP address of the target FINS/TCP server.
   - Target IP address for server: Specifies allowed client IP addresses when protection is enabled.
   - Automatically allocated FINS node address for server: Specifies the address to allocate when automatically allocating a FINS node address to the target FINS/TCP client.
   - Keep-alive: Specified whether to use the keep-alive function.

     Note Normally this function is used and the option is selected.
   - Protection Settings for server: Specifies the IP address of the connected client.

     Note Select this option only when protecting as the server.
3. Select ***Transfer to PLC*** from the PLC Menu and click the **Yes** Button. The setting data will be transferred to the nonvolatile memory of the EtherNet/IP Unit or built-in EtherNet/IP port.
4. Make the routing table settings and transfer them to each PLC. (See note 1.)
   Set the routing tables with CX-Integrator, and transfer it to each PLC.
5. Create a ladder program that includes the SEND/SEND2, RECV/RECV2, and CMND/CMND2 instructions.

Note (1) Routing tables are required in the following situations:

- When communicating with a PLC or computer on another network (e.g., remote programming or monitoring using FINS messages or a CX-Programmer)

- When multiple Communications Units are mounted to a single PLC (i.e., CPU Unit)
- When routing tables are used for one or more other nodes on the same network

It is not necessary to set routing tables if one Communications Unit is mounted to the PLC and the nodes are connected as one network.

(2) If EtherNet/IP is selected for CX-Programmer communications, FINS message communications and remote programming/monitoring from the CX-Programmer will be possible as long as CIP routing is possible for the entire communications path. Routing tables do not need to be set. If FINS messages are sent from a PLC, however, then routing tables must be set.

8-4 Routing Tables

When the FINS communications service is used, routing tables must be created in advance. Routing tables are required in the following circumstances.

- When communicating with a PLC or computer on another network (e.g., remote programming or monitoring using FINS messages or a CX-Programmer)
- When multiple Communications Units are mounted to a single PLC (i.e., CPU Unit).
- When routing tables are used for one or more other nodes on the same network.

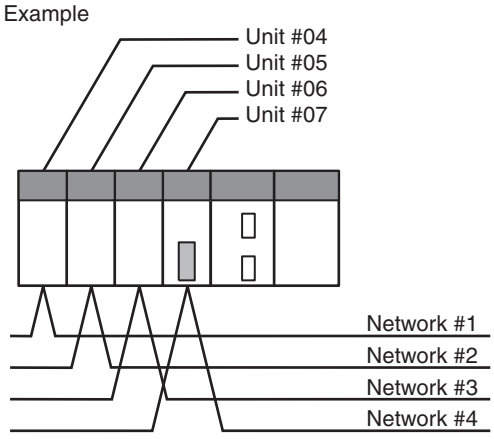
It is not necessary to set routing tables if one Communications Unit is mounted to the PLC and the nodes are connected as one network. The routing tables are required not only for nodes communicating via the FINS communications service but also for all relay nodes on the network.

8-4-1 Routing Table Overview

The routing tables describe the transmission path for FINS messages when the FINS communications are used. It consists of two tables: A local network table and a relay network table.

Local Network Table

The local network table is a table describing the correspondences among unit numbers of the Communications Units and Boards mounted to each node.



Local Network Table

Local network address	Unit number
1	04
2	05
3	06
4	07

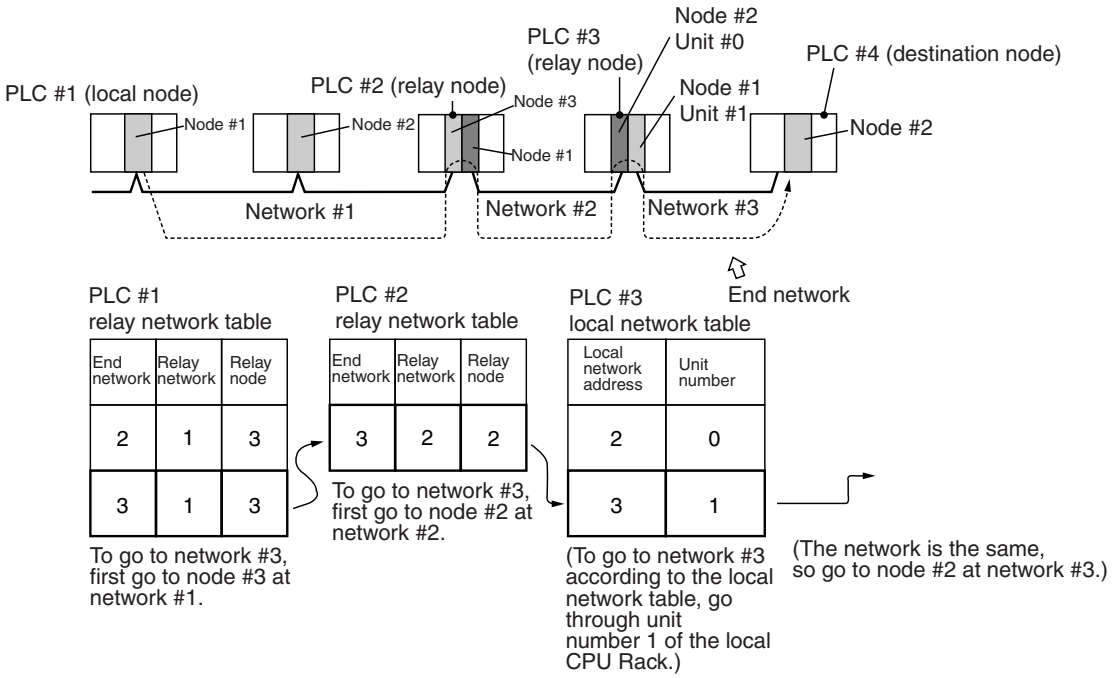
Note

1. The unit number is set (0 to F: 0 to 15) using the rotary switch on the front of the EtherNet/IP Unit.
2. The network address is the number of the network (1 to 127) to which the Communications Unit or Board is connected. It is set when the local network table is created.

Relay Network Table

A relay table is a table that shows the nodes to which data should be sent first in order to send data to a network that is not connected to the local node. It shows the correspondence between the address of the final destination network, and the network address and node address of the first relay point of the path to reach there. When internetwork communications are carried out, the end network can be reached by following the relay points.

The following example shows routing tables for sending data from PLC #1 (the local node: network address 1, node address 1) to PLC #4 (the destination node: network address 3, node address 2).



Note In the above example, the routing tables required for a message to reach PLC #4 from PLC #1 are shown. Additional settings would be required in the routing tables for a message to reach PLC #1 from PLC #4. Refer to *8-4-3 Routing Table Setting Examples* for routing table setting examples.

8-4-2 Connecting and Using a Peripheral Device for the PLC

Routing tables must be created by a CX-Integrator connected to the PLC. (They cannot be created using a Programming Console.) For details on how to connect and use the CX-Integrator, refer to the *CX-Integrator Operation Manual* (W445). (CX-Integrator is automatically installed when CX-One is installed.)

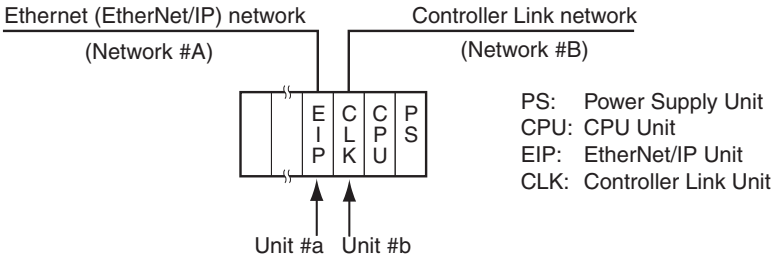
Note

1. When routing tables are transferred from the CX-Integrator to the PLC, all of the CPU Bus Unit are reset so that the routing tables that have been created can be read and enabled. Before transferring the routing tables, confirm that there will be no problems in the system when the CPU Bus Units are reset.
2. To transfer routing tables for multiple nodes to a PLC in one batch, connect the CX-Integrator to a PLC with only one Communications Unit mounted. Routing tables cannot be transferred to other nodes from a PLC with multiple Communications Units mounted.
3. Routing tables can only be transferred as a batch to multiple nodes within the same network as the PLC to which the CX-Integrator is connected.

8-4-3 Routing Table Setting Examples

■ Example 1: Local Network Table for a PLC With Multiple Units Mounted

This example shows the local network table settings for a PLC to which multiple CPU Bus Units are mounted.

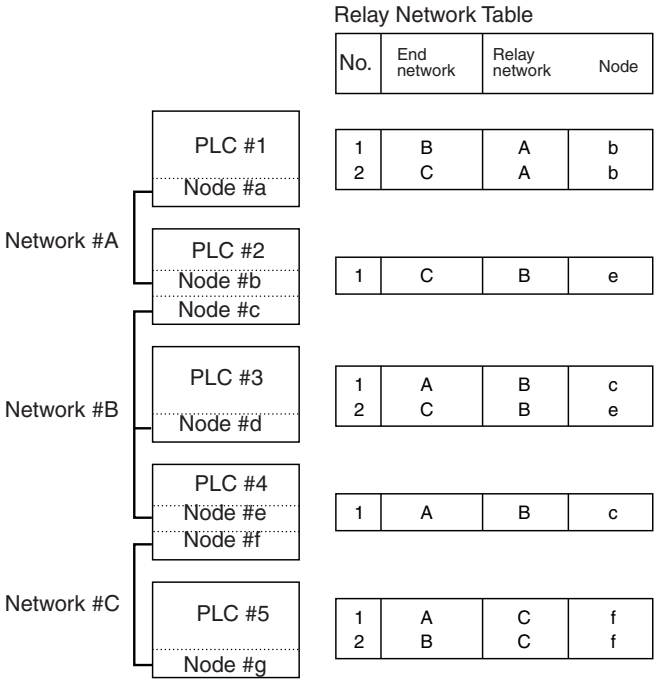


Local Network Table

No.	Local network	CPU Bus Unit
1	A	a
2	B	b

■ Example 2: Three Interconnected Networks

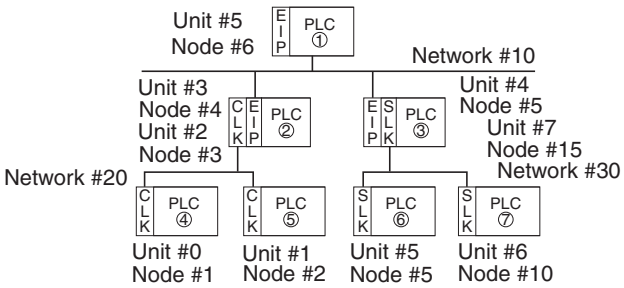
This example shows the relay network table settings for three different interconnected networks.



In the table for PLC #3, for example, if network #A is taken as the end network, then network #B becomes the relay network and node #c becomes the relay node. If network #C is taken as the end network, then network #B still becomes the relay network and node #e becomes the relay node.

■ **Example 3: All Nodes**

This example uses the following configuration to show the routing tables for all nodes.



PLC #1 Routing Table

(Local network table)

No.	Local network	CPU Bus Unit No.
1	010	05
2		
3		

(Relay network table)

No.	End network	Relay network	Relay node
1	020	010	004
2	030	010	005
3			

PLC #2 Routing Table

(Local network table)

No.	Local network	CPU Bus Unit No.
1	010	03
2	020	02
3		

(Relay network table)

No.	End network	Relay network	Relay node
1	030	010	005
2			
3			

PLC #3 Routing Table

(Local network table)

No.	Local network	CPU Bus Unit No.
1	010	04
2	030	07
3		

(Relay network table)

No.	End network	Relay network	Relay node
1	020	010	004
2			
3			

PLC #4 Routing Table

(Local network table)

No.	Local network	CPU Bus Unit No.
1	020	00
2		
3		

(Relay network table)

No.	End network	Relay network	Relay node
1	010	020	003
2	030	020	003
3			

PLC #5 Routing Table

(Local network table)

No.	Local network	CPU Bus Unit No.
1	020	01
2		
3		

(Relay network table)

No.	End network	Relay network	Relay node
1	010	020	003
2	030	020	003
3			

PLC #6 Routing Table

(Local network table)

No.	Local network	CPU Bus Unit No.
1	030	05
2		
3		

(Relay network table)

No.	End network	Relay network	Relay node
1	010	030	015
2	020	030	015
3			

PLC #7 Routing Table

(Local network table)

No.	Local network	CPU Bus Unit No.
1	030	06
2		
3		

(Relay network table)

No.	End network	Relay network	Relay node
1	010	030	015
2	020	030	015
3			

8-5 Using FINS Applications

8-5-1 CX-Programmer (CX-Server)

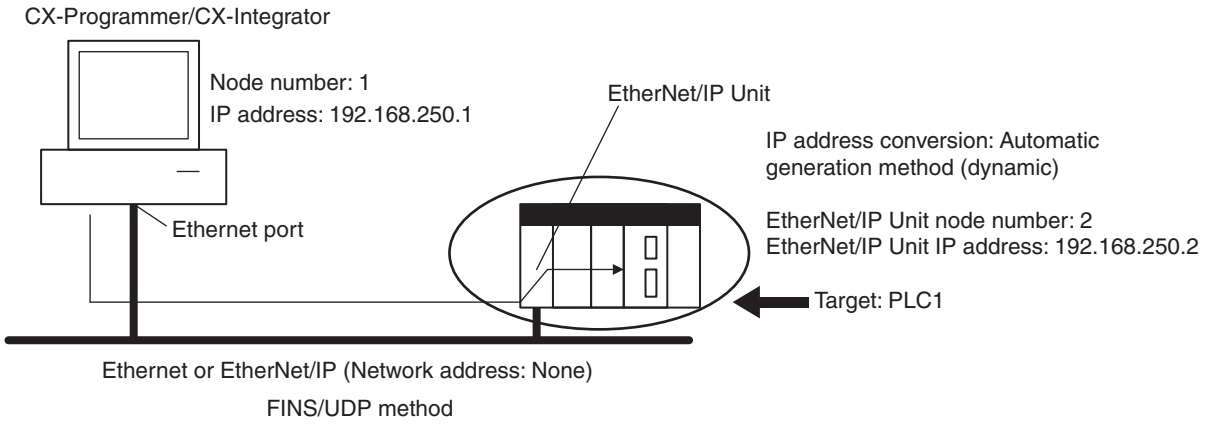
The following examples show how to connect online from a CX-Programmer on an Ethernet network to a PLC on the Ethernet network.

■ **System Configuration Example 1: No Routing**

In this example, an online connection is made by FINS/UDP to a PLC on an Ethernet network (PLC1 in the diagram below) from a CX-Programmer/CX-Integrator connected to the Ethernet network.

Conditions

- FINS/UDP method
- IP Address Conversion: Automatic (Dynamic) generation method



CX-Programmer's Change PLC Dialog Box

Settings for target PLC (PLC1)'s Change PLC Dialog Box			Setting
Device Name			PLC1
Network Type			Ethernet
Network Tab Page	FINS transmission source address		0
	FINS destination	Network number	0
		Node address	2
	Frame length		2,000 bytes
	Response monitor time		2 seconds
Driver Tab Page	Workstation node address		1
	Automatic generation method		Not selected
	IP address		192.168.250.2 (EtherNet/IP Unit or built-in EtherNet/IP port IP address)
	Port number		9600

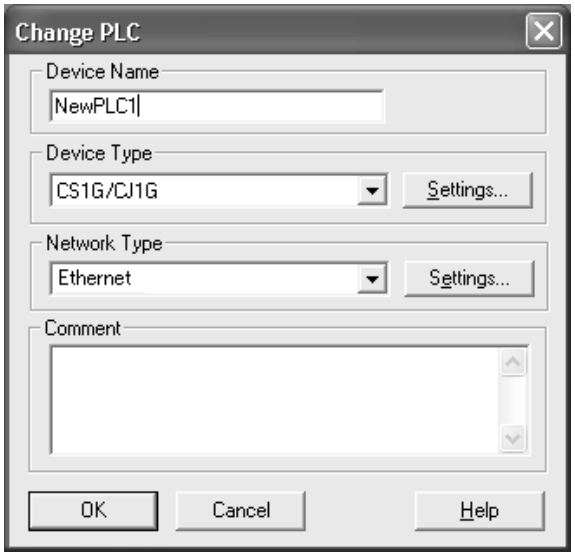
CX-Programmer's FINS/UDP Tab Page in Edit Parameters Dialog Box

Item	Setting
Use of FINS/UDP (See note 1.)	Use FINS/UDP service
FINS/UDP Port	Default (9600)
IP Address Conversion	Automatic (Dynamic) generation method
IP Router Table	None

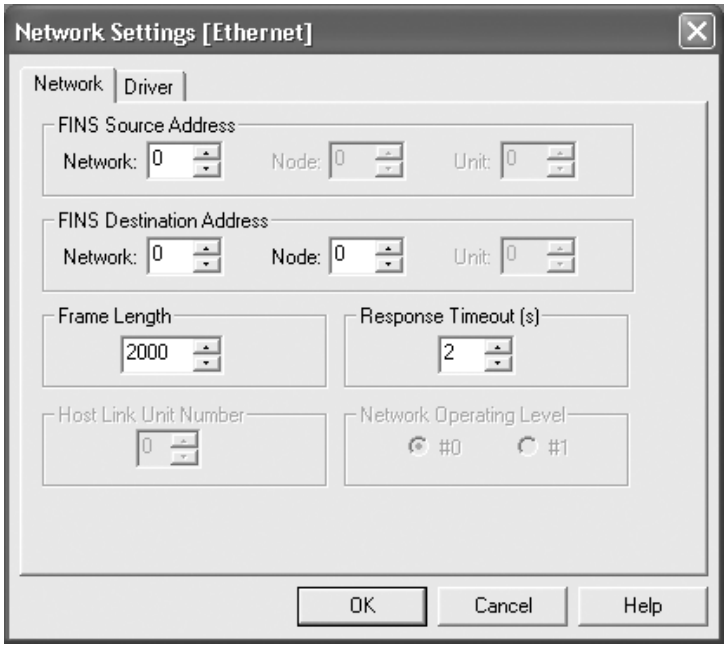
Note (1) This setting is provided for CS1W/CJ1W-EIP21S or CJ3M-CPU3□ only.

Example: Inputs to the CX-Programmer's Setup Window

Example: Change PLC Settings

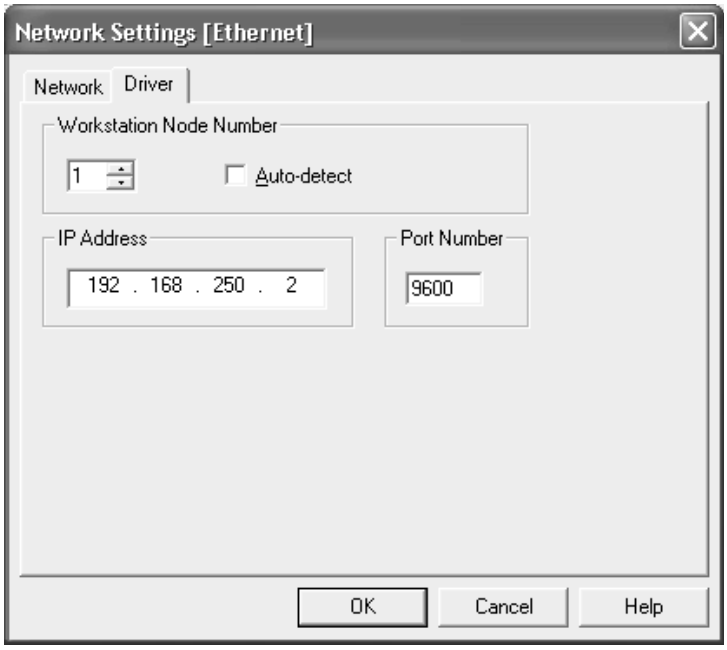


Example: Network Settings (Network Tab Page)



Note When FinsGateway is selected as the network type, make sure that the frame length is set to 2,000 bytes max.

Example: Network Settings (Driver Tab Page)

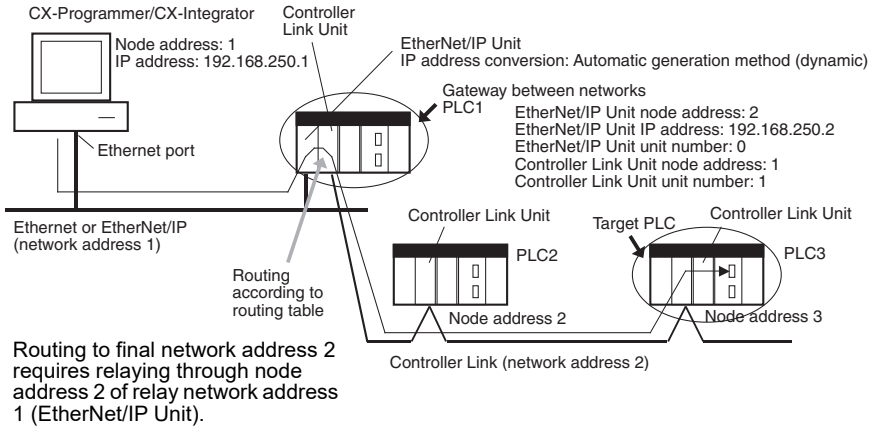


■ **System Configuration Example 2: Using Routing Tables**

In this example, an online connection is made via the Ethernet to a PLC on a Controller Link network (PLC 3 below) from a CX-Programmer/CX-Integrator connected to the Ethernet network.

Conditions

- FINS/UDP method
- IP address conversion: Automatic generation method (dynamic)



Routing to final network address 2 requires relaying through node address 2 of relay network address 1 (EtherNet/IP Unit).

CX-Programmer's Change PLC Dialog Box

Settings for target PLC (PLC3)'s Change PLC Dialog Box			Setting
Device Name			PLC3
Network Type			Ethernet
Network Tab Page	FINS destination	FINS transmission source address	1
		Network number	2
		Node address	3
	Frame length		2,000 bytes
	Response monitor time		2 seconds

Settings for target PLC (PLC3)'s Change PLC Dialog Box		Setting
Driver Tab Page	Workstation node address	1
	Automatic generation method	Not selected
	IP address	192.168.250.2 (EtherNet/IP Unit or built-in EtherNet/IP port IP address)
	Port number	9600

CX-Programmer's FINS/UDP Tab Page in Edit Parameters Dialog Box

Same as for *System Configuration Example 1*.

Routing Table Settings and Transfer to Each PLC

Set the routing tables with CX-Integrator, and transfer them.

1. Using CX-Integrator, connect online, and select ***Routing table*** – ***Settings***. Then create FINS local routing tables (a local network table and a relay network table).

   Example: PLC 1 Routing Table Settings

   • Local Network Table

Unit number	Local network number
0	1
1	2

   • Relay Network Table

   None

   Example: PLC 2 and PLC 3 Routing Table Settings

   • Local Network Table

Unit number	Local network number
0	2

   • Relay Network Table

   In order to relay from PLC2/3 to the final network number 1, it is necessary to relay via node address 1 (i.e., the Controller Link Unit) on relay network number 2.

Final network number	Relay network number	Relay node address
1	2	1

2. Save the routing table file (File - Save local routing table file).
3. Next, to connect online, select ***Communication Settings*** from the Network Menu. For each PLC, register a PLC with a direct serial connection (node address: 0), and select it.
4. With the CX-Integrator, select ***Work Online*** from the Network Menu.
5. Select ***Tools - Start Routing table***, read the saved file, and select ***Options - Transfer to PLC***. Click Yes to transfer the routing tables to the connected PLC.

8-5-2 FinsGateway

FinsGateway Ver. 2003 must be used to communicate using FINS/TCP between applications serving as communications drivers and built-in EtherNet/IP Units.

FinsGateway Ver. 3.☐ or lower versions can be used, however, when communicating by the FINS/UDP method only.

■ **Overview of Setup Methods**

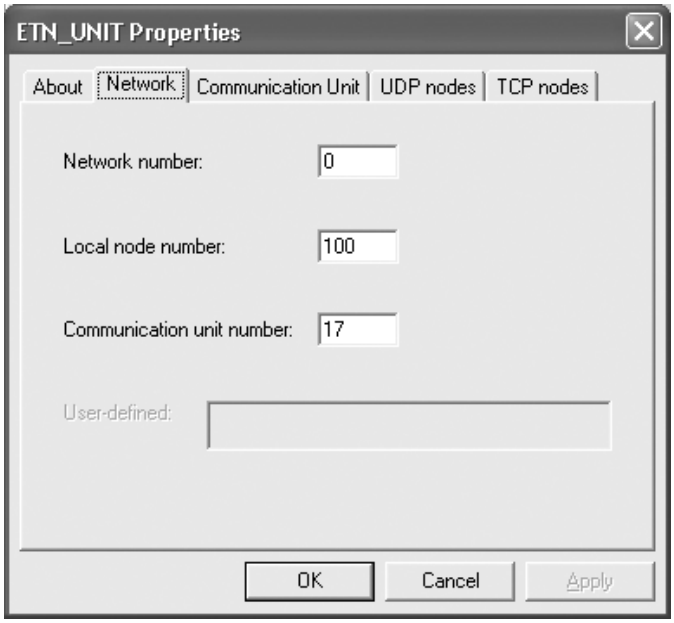
1. Starting FinsGateway Settings

Select ***FinsGateway*** – ***FinsGateway Setup*** to start the FinsGateway Setup.

2. ETN_UNIT Driver Setup

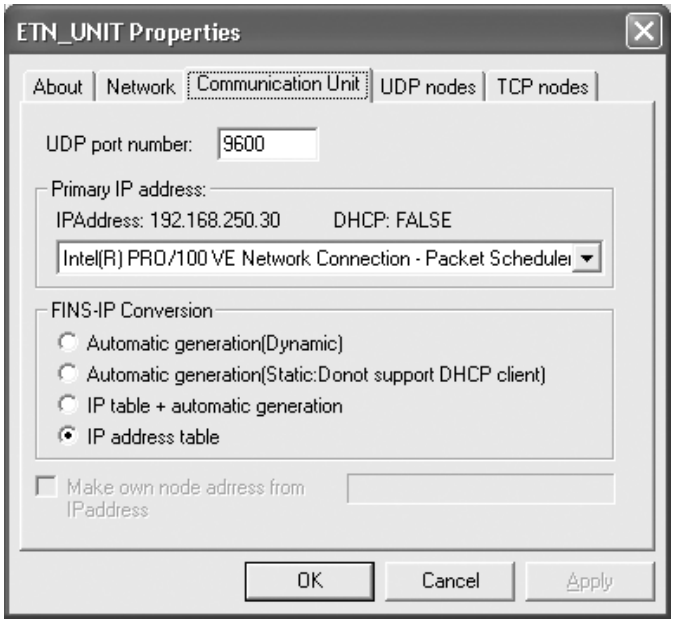
1. Double-click on **ETN_UNIT** in the settings for the network and Unit. The following ETN_UNIT Properties Window will be displayed.

• Network Tab Page



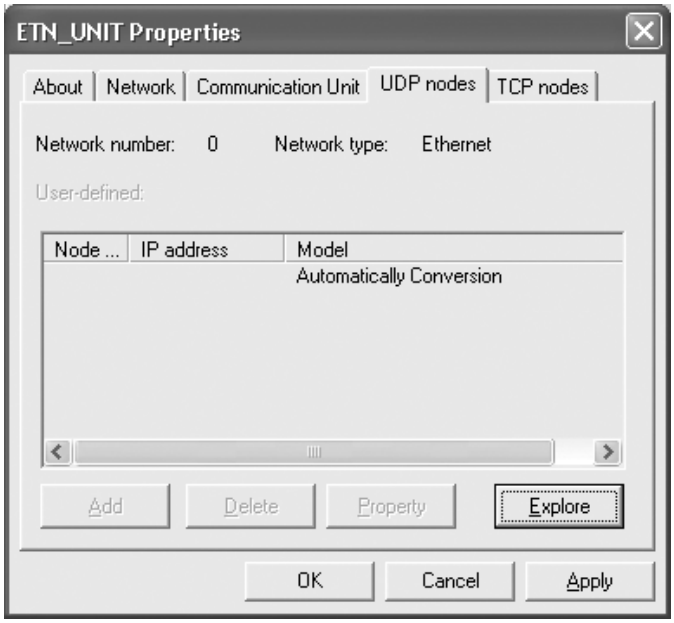
• Network number	Set the network number for the personal computer (Ethernet port).
• Local node address	Set the personal computer (Ethernet port) node address (1 to 254) on the Ethernet network.
• Communication unit number	Set the unit number in decimal (16 to 31) for the personal computer (Ethernet port).

• Communication Unit Tab Page

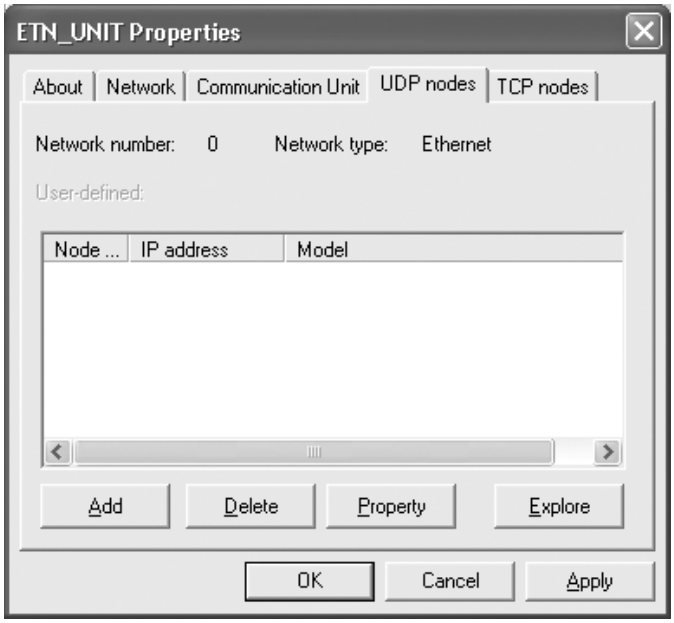


• UDP port number	Set the local UDP port number for the personal computer (Ethernet port). The default is 9600.
• Priority Network Card	If multiple Network Cards are mounted at the personal computer, select the Network Card that is to be given priority.
• FINS - IP address conversion	Set the IP address conversion method.

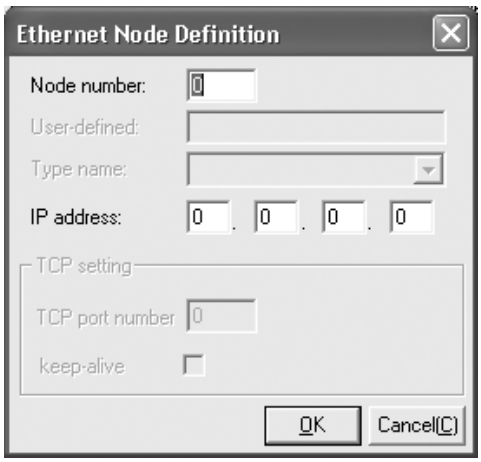
• UDP Nodes Tab Page: Automatic Generation Method (Dynamic or Passive)



• UDP Nodes Tab Page: IP Address Table Method or Combined Method

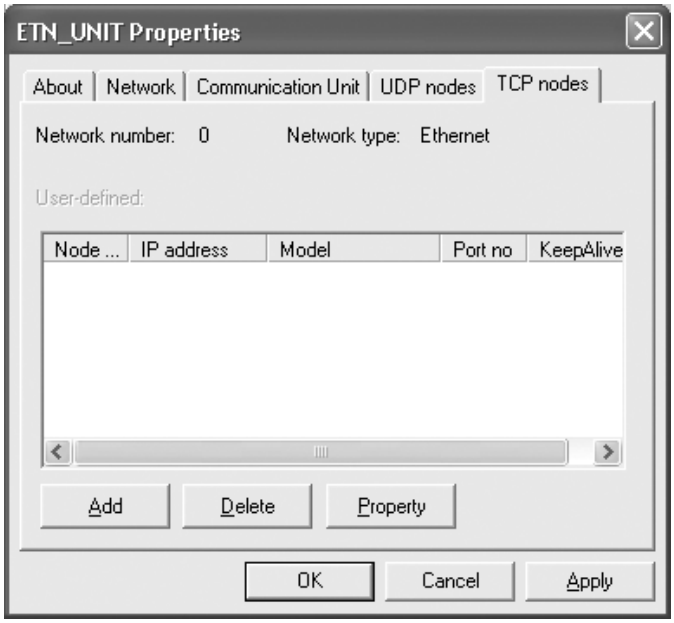


Click the **Add** Button, and then set the IP address table in the following Ethernet Node Definition Dialog Box.

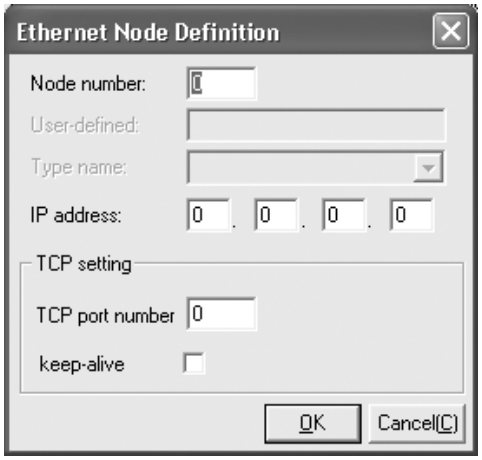


• Node address: Set the remote FINS node address.
• IP address: Set the remote IP address.

• TCP Nodes Tab Page



Click the **Add** Button, and then set the IP address table in the following Ethernet Node Definition Dialog Box.



• Node address:	Set the remote FINS node address.
• IP address:	Set the remote IP address.
• Destination port number:	Set the FINS/TCP port number for the remote node. Normally the PLC's default setting of 9600 should be specified.
• Keep-alive setting:	Sets the keep-alive function. Normally this should be selected.

3. Starting FinsGateway ETN_UNIT Service

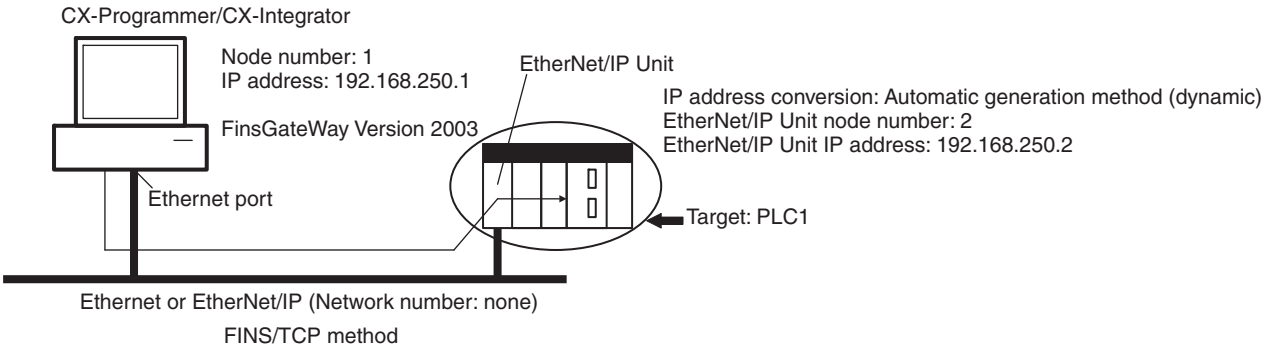
Select ETN_UNIT from Services under the Basic Tab in the FinsGateway Setup Window, and then click the **Start** Button.

■ System Configuration Example 3: Connecting the CX-Programmer Online Using the FINS/TCP Method

In this example, an online connection is made by FINS/TCP to a PLC on an Ethernet network (PLC1 in the diagram below) from a CX-Programmer/CX-Integrator connected to the Ethernet network.

Conditions

• FINS/TCP method



CX-Programmer's Change PLC Dialog Box

Settings for target PLC (PLC1)'s Change PLC Dialog Box			Setting
Device Name			PLC1
Network Type			FinsGateway
Network Tab Page	FINS destination	Network number	0
		Node address	2
	Frame length		2,000 bytes
	Response monitor time		2 seconds

CX-Programmer's FINS/TCP Tab Page in Edit Parameters Dialog Box

Item	Setting
Use of FINS/TCP (See note 1.)	Use FINS/TCP service
FINS/TCP Port	Default (9600)
IP Router Table	None

Note (1) This setting is provided for CS1W/CJ1W-EIP21S or CJ3M-CPU3□ only.

FinsGateway ETN_UNIT Setup

TCP Nodes Tab Page: Ethernet Node Definition Dialog Box

Item	Setting
Node address	2
IP address	192.168.250.2
Destination port number	9600
Keep-alive setting	Selected (yes)

8-6 Communicating between OMRON PLCs

FINS commands can be sent from the CPU Unit of a PLC by using the SEND/SEND/SEND2, RECV/RECV2, and CMND/CMND2 instructions.

SEND/SEND2: Writes I/O data from the local node to another node.
RECV/RECV2: Reads I/O data from another node to the local node.
CMND/CMND2: Issues FINS commands for controlling operations such as sending and receiving I/O memory data to and from other nodes, reading information regarding other nodes, and so on.

8-6-1 Communications Specifications

The following table shows the specifications for PLC communications using the SEND/SEND2, RECV/RECV2, and CMND/CMND2 instructions.

Item	Specifications
Destination	1:1 SEND/SEND2/RECV/RECV2/CMND/CMND2 instructions 1:N SEND/SEND2/RECV/RECV2/CMND/CMND2 instructions (broadcasting)
Data length	SEND/SEND2: 990 words (1,980 bytes) max.; broadcasting: 727 words (1,454 bytes) RECV/RECV2: 990 words (1,980 bytes) max. CMND/CMND2: 1,990 bytes max.; broadcasting: 1,462 bytes (after FINS command code)
Data contents	The following data is sent and received with the execution of each instruction. SEND/SEND2: Sends request for remote node to receive data, and receives response data. RECV/RECV2: Sends request for remote node to send data, and receives response data. CMND/CMND2: Sends any FINS command and receives response data.
Communications port number	Ports 0 to 7 SEND, RECV, or CMND instruction (Eight transmissions can occur simultaneously.)
Response monitor time	0000: 2 s (default) 0001 to FFFF: 0.1 to 6,553.5 s in 0.1-s increments (specified by user)
Number of retries	0 to 15 retries

Note

1. The maximum data length is limited to 512 bytes for data exchange between the PLC and SYSMAC LINK Systems or the PLC and SYSMAC BUS/2 Remote I/O Systems.
2. The SEND2, RECV2, or CMND2 instruction is supported by the CJ2/CJ3 CPU Units.
3. When broadcasting, do not require a response.
   Use the FINS/UDP method for broadcasting.

8-6-2 PLC Communications Data Areas

The following table shows the I/O data areas involved when SEND/SEND2 and RECV/RECV2 are used.

Area	Range
CIO Area	CIO 0000 to CIO 6143
Work Area	W000 to W511
Holding Area	H000 to H1535
Auxiliary Area	A000 to A959 (See note 1.)
Timer Area	TIM0000 to 4095
Counter Area	CNT0000 to 4095
DM Area	D00000 to D32767
EM Area	E00000 to E32767 (See note 2.)

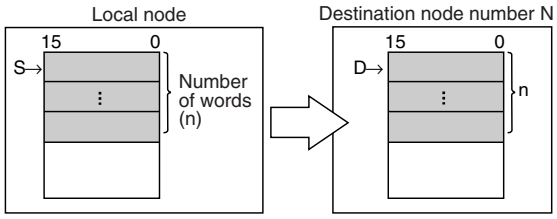
Note
1. Data cannot be written to words A000 to A447 in the Auxiliary Area.
2. Refer to the operation manual for your CPU Unit to confirm EM Area support.

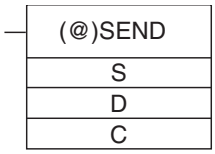
8-6-3 Using SEND, RECV, and CMND

Make the settings shown below when using the SEND, RECV, and CMND instructions in the user's ladder-diagram program in the PC.

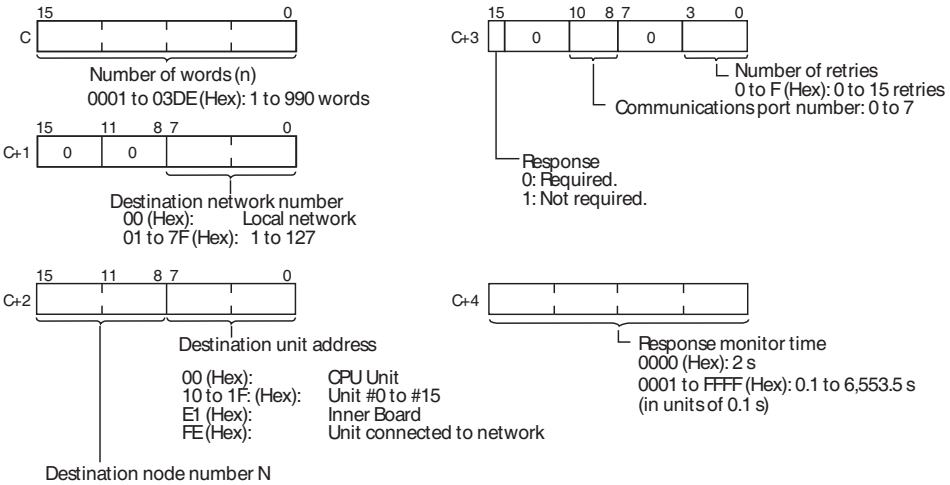
SEND

The SEND instruction sends the data in n number of words, starting from the beginning word S at the local node, to the words starting from the beginning word D at the remote destination node (node address N).





S: Local node beginning word
D: Destination beginning word
C: First word of control data (below)



The same data can be broadcast to all nodes on the network by setting the destination node number to FF (Hex).

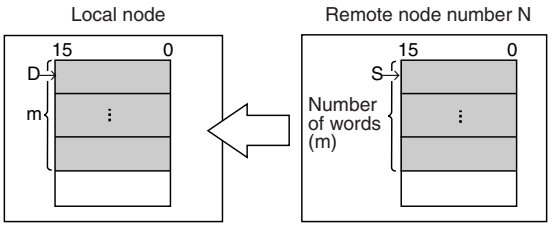
The range of node addresses is different for networks other than Ethernet.

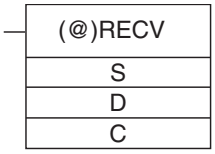
* The CJ2/CJ3 CPU Unit also supports the SEND2 instruction.

Note The message service does not guarantee that a message will reach the destination node. A message may be lost during transmission due to factors such as noise. To prevent this from occurring when using message services, it is common to set up retry processing at the node from which instructions are issued. With the SEND, RECV, and CMND instructions, retry processing is executed automatically by specifying the number of retries, so specify a number other than 0.

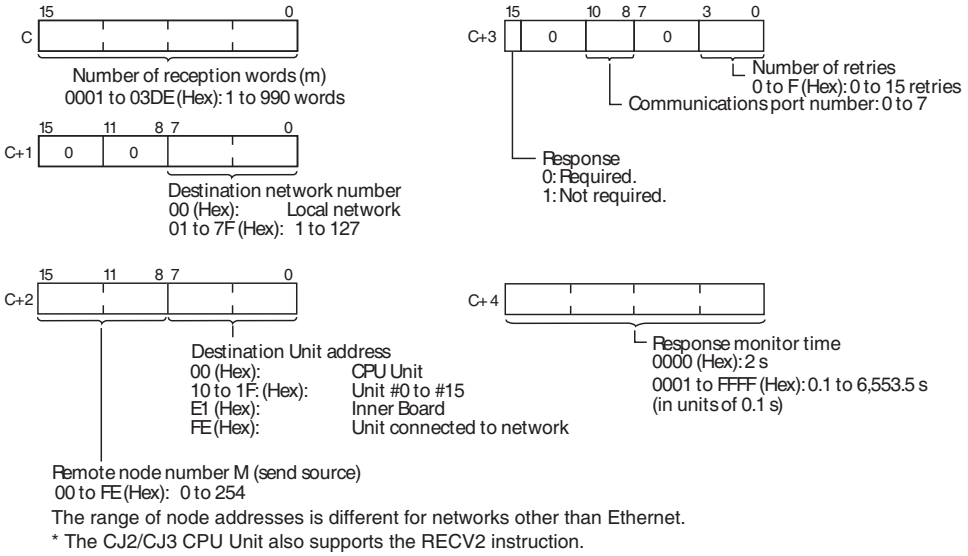
RECV

With the RECV instruction, the data in m number of words, starting from the beginning word S at the remote node (node address M) is received at the words starting from the beginning word D at the local node.





S: Remote node beginning word
D: Local beginning word
C: First word of control data (below)



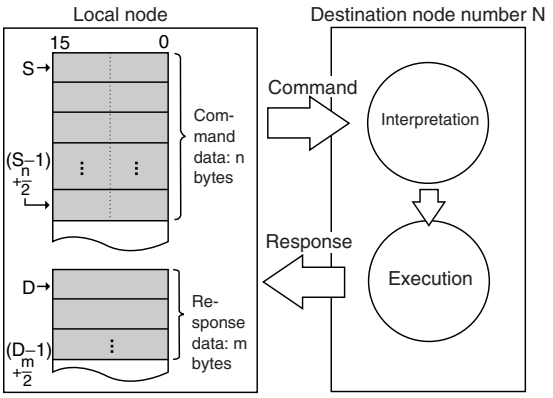
The range of node addresses is different for networks other than Ethernet.

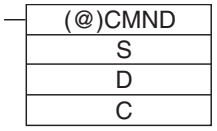
* The CJ2/CJ3 CPU Unit also supports the RECV2 instruction.

Note The message services function does not guarantee that a message will reach the destination node. A message may be lost during transmission due to factors such as noise. In order to prevent this from occurring when using message services, it is common to set up retry processing at the node from which instructions are issued. With the SEND, RECV, and CMND instructions, retry processing is executed automatically by specifying the number of retries, so specify a number other than 0.

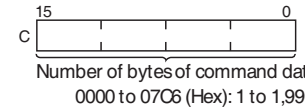
CMND

The CMND instruction sends n bytes of command data, starting from the beginning word S at the local node, to the node at node address N. the data in m number of words, starting from the beginning word S at the remote node (node address M) is received at the words starting from the beginning word D at the local node.

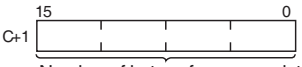




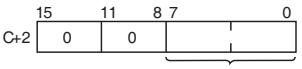
S: Beginning command storage word
D: Beginning response storage word
C: First word of control data (below)



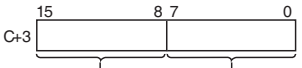
Number of bytes of command data (n)
0000 to 07C6 (Hex): 1 to 1,990 bytes



Number of bytes of response data (m)
0000 to 07C6 (Hex): 1 to 1,990 bytes



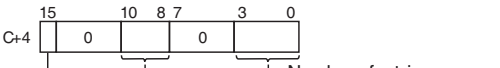
Destination network number
00 (Hex): Local network
01 to 7F (Hex): 1 to 127



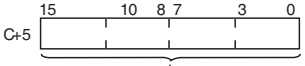
Destination Unit address
00 (Hex): CPU Unit
10 to 1F (Hex): Unit #0 to #15
E1 (Hex): Inner Board
FE (Hex): Unit connected to network

Destination node number N
00 to FE (Hex): 0 to 254

The same data can be broadcast to all nodes on the network by setting the destination node number to FF (Hex).



Number of retries
0 to F (Hex): 0 to 15 retries
Communications port number: 0 to 7
Response
0: Required.
1: Not required.



Response monitor time
0000 (Hex): 2 s
0001 to FFFF (Hex): 0.1 to 6,553.5 s
(in units of 0.1 s)

The range of node addresses is different for networks other than Ethernet.

* The CJ2/CJ3 CPU Unit also supports the CMND2 instruction.

Note The message services function does not guarantee that a message will reach the destination node. A message may be lost during transmission due to factors such as noise. In order to prevent this from occurring when using message services, it is common to set up retry processing at the node from which instructions are issued. With the SEND, RECV, and CMND instructions, retry processing is executed automatically by specifying the number of retries, so specify a number other than 0.

Commands Addressed to CS/CJ-series CPU Units

The following table provides a list of FINS commands that can be processed by a CS/CJ-series CPU Unit. For details, refer to the *CS/CJ-series Programmable Controllers Communications Commands Reference Manual* (W342).

For details on FINS commands that can be processed by the EtherNet/IP Unit or built-in EtherNet/IP port, refer to *Appendix E FINS Commands Addressed to EtherNet/IP Units or Built-in EtherNet/IP Ports*.

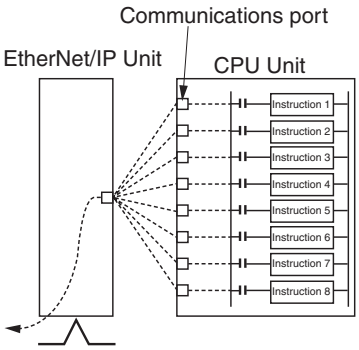
Usage	Command code		Name	Function
	MR	SR		
I/O memory area access	01	01	MEMORY AREA READ	Reads the contents of consecutive I/O memory area words.
	01	02	MEMORY AREA WRITE	Writes the contents of consecutive I/O memory area words.
	01	03	MEMORY AREA FILL	Writes the same data to the specified range of I/O memory area words.
	01	04	MULTIPLE MEMORY AREA READ	Reads the contents of specified non-consecutive I/O memory area words.
	01	05	MEMORY AREA TRANSFER	Copies the contents of consecutive I/O memory area words to another I/O memory area.
Parameter access (registered I/O tables, routing tables, etc.)	02	01	PARAMETER AREA READ	Reads the contents of consecutive parameter area words.
	02	02	PARAMETER AREA WRITE	Writes the contents of consecutive parameter area words.
	02	03	PARAMETER AREA FILL (CLEAR)	Writes the same data to the specified range of parameter area words.
Program area access	03	06	PROGRAM AREA READ	Reads the UM (User Memory) area.
	03	07	PROGRAM AREA WRITE	Writes to the UM (User Memory) area.
	03	08	PROGRAM AREA CLEAR	Clears the UM (User Memory) area.
Operating mode changes	04	01	RUN	Changes the CPU Unit's operating mode to RUN or MONITOR.
	04	02	STOP	Changes the CPU Unit's operating mode to PROGRAM.
Machine configuration reading	05	01	CPU UNIT DATA READ	Reads CPU Unit data.
	05	02	CONNECTION DATA READ	Reads the model numbers of the device corresponding to addresses.
Status reading	06	01	CPU UNIT STATUS READ	Reads the status of the CPU Unit.
	06	20	CYCLE TIME READ	Reads the maximum, minimum, and average cycle time.
Time data access	07	01	CLOCK READ	Reads the present year, month, date, minute, second, and day of the week.
	07	02	CLOCK WRITE	Changes the present year, month, date, minute, second, or day of the week.
Message display	09	20	MESSAGE READ/CLEAR	Reads and clears messages, and reads FAL/FALS messages.
Access rights	0C	01	ACCESS RIGHT ACQUIRE	Acquires the access right as long as no other device holds it.
	0C	02	ACCESS RIGHT FORCED ACQUIRE	Acquires the access right even if another device already holds it.
	0C	03	ACCESS RIGHT RELEASE	Releases the access right that has been acquired.
Error log	21	01	ERROR CLEAR	Clears errors or error messages.
	21	02	ERROR LOG READ	Reads the error log.
	21	03	ERROR LOG POINTER CLEAR	Clears the error log pointer.

Usage	Command code		Name	Function
	MR	SR		
File memory	22	01	FILE NAME READ	Reads file memory data.
	22	02	SINGLE FILE READ	Reads a specified length of file data from a specified position within a single file.
	22	03	SINGLE FILE WRITE	Writes a specified length of file data from a specified position within a single file.
	22	04	FILE MEMORY FORMAT	Formats (initializes) the file memory.
	22	05	FILE DELETE	Deletes specified files stored in the file memory.
	22	07	FILE COPY	Copies files from one file memory to another file memory in the same system.
	22	08	FILE NAME CHANGE	Changes a file name.
	22	0A	MEMORY AREA–FILE TRANSFER	Transfers or compares data between the I/O memory area and the file memory.
	22	0B	PARAMETER AREA–FILE TRANSFER	Transfers or compares data between the parameter area and the file memory.
	22	0C	PROGRAM AREA–FILE TRANSFER	Transfers or compares data between the UM (User Memory) area and the file memory.
	22	15	CREATE/DELETE DIRECTORY	Creates or deletes a directory.
Debugging	23	01	FORCED SET/RESET	Force-sets or force-resets bits, or releases force-set status.
	23	02	FORCED SET/RESET CANCEL	Cancels all bits that have been force-set or force-reset.

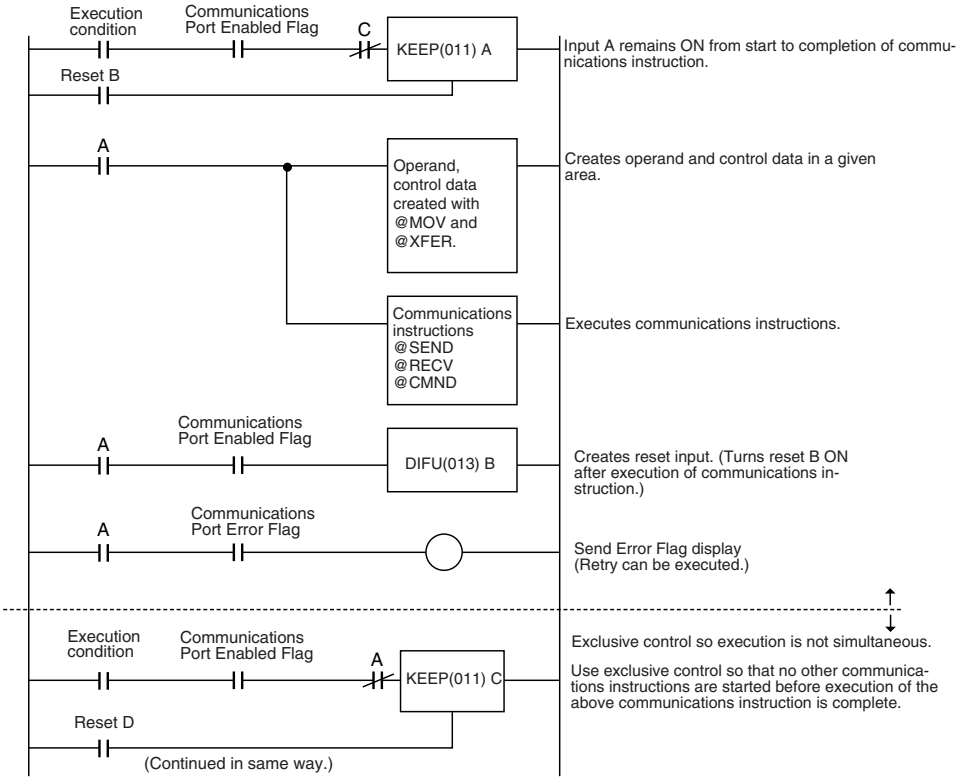
8-6-4 Writing Programs

Programs incorporating the SEND, RECV, and CMND instructions are generally created using the Communications Port Enabled Flag and the Communications Port Error Flag as input conditions. CS/CJ-series CPU Units have eight communications ports. Only one instruction can be executed at any given port at one time, however, so the program must not overlap the use of any of the ports. A program example is provided below.

Note The SEND2/RECV2/CMND2 that can be used with the CJ2/CJ3 CPU Unit can be used with up to 64 ports, and used with only automatic allocation.



There are eight communications ports, so up to eight communications instructions can be executed at a time. The number of messages that can be sent or received with a single CPU Bus Unit service, though, is not more than two each for the CPU Unit to the EtherNet/IP Unit and for the EtherNet/IP Unit to the CPU Unit.



The execution status of the SEND, RECV, and CMND instructions is always reflected by the communications flags (i.e., the Communications Port Enabled Flag and the Communications Port Error Flag). The CS/CJ-series CPU Unit's communications flags are allocated in the Auxiliary Area as shown in the following table.

Flag name	Address		Contents
	Word	Bits	
Communications Port Enabled Flag	A202	Bit 7: Port 7 Bit 6: Port 6 Bit 5: Port 5 Bit 4: Port 4 Bit 3: Port 3 Bit 2: Port 2 Bit 1: Port 1 Bit 0: Port 0	OFF: Execution enabled (being executed) ON: Execution disabled (not being executed)
Communications Port Error Flag	A219	Bit 7: Port 7 Bit 6: Port 6 Bit 5: Port 5 Bit 4: Port 4 Bit 3: Port 3 Bit 2: Port 2 Bit 1: Port 1 Bit 0: Port 0	0: Normal completion 1: Abnormal completion

Note In CS/CJ-series PLCs, communications ports 0 to 7 are also used when executing the PCMR(260) (PROTOCOL MACRO), TXDU(256), and RXDU(255) instructions, so these flags are shared by SEND(090), RECV(098), CMND(490), PCMR(260), TXDU(256), and RXDU(255).
SEND(090), RECV(098), and CMND(490) cannot be executed at a communications port if PCMR(260) TXDU(256), or RXDU(255) is being executed at that port.

Communications Port Completion Codes

The status of a SEND, RECV, and CMND instruction after execution is reflected as a communications port completion code, in one word (two bytes) of data as shown in the following table. (The value is 0000 during instruction execution.) The recorded status is saved until execution of the next instruction.

Word	Contents
A203	Communications Port 0 Completion Code
A204	Communications Port 1 Completion Code
A205	Communications Port 2 Completion Code
A206	Communications Port 3 Completion Code
A207	Communications Port 4 Completion Code
A208	Communications Port 5 Completion Code
A209	Communications Port 6 Completion Code
A210	Communications Port 7 Completion Code

The meanings of the communications port completion codes are the same as those for FINS commands and responses. Bits 08 to 15 in the communications port completion code correspond to the first byte of the response code, and bits 00 to 07 correspond to the second byte. For details, refer to *18-6 Troubleshooting with FINS Response Codes*.

Communications Port Error Flag and Completion Codes CMND(490)

Errors that occur when CMND is used generate a Communications Port Error Flag and are recorded in a communications port completion code only in the following cases:

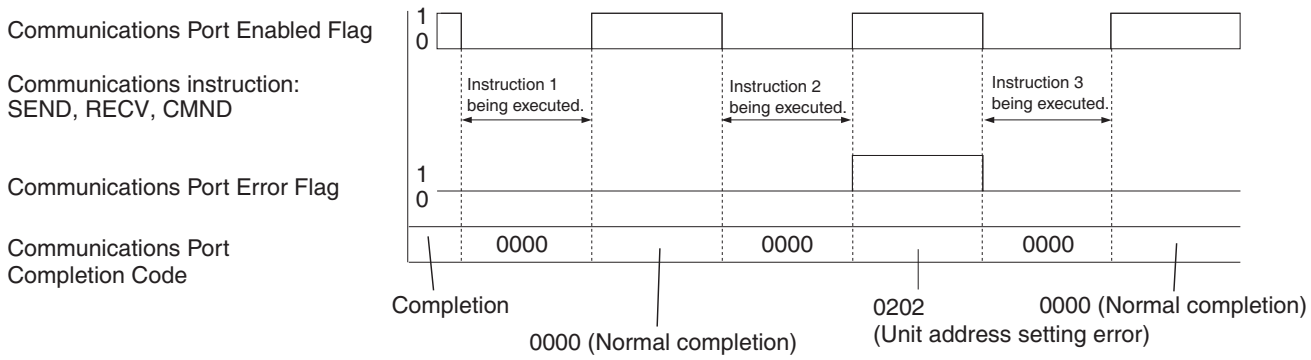
- When a response timeout error has occurred.
- When the number of communications data bytes exceeds the maximum value for the Unit (i.e., 2,000 bytes for the EtherNet/IP Unit or built-in EtherNet/IP port).
- When the actual number of response bytes is greater than the number of reception bytes that has been set. (The response is not stored in this case.)

Errors other than these are recorded in the response codes of the responses stored from the beginning response storage word onwards. Be careful of these, because there are no Communications Port Error Flags and they are not recorded in a communications port completion code.

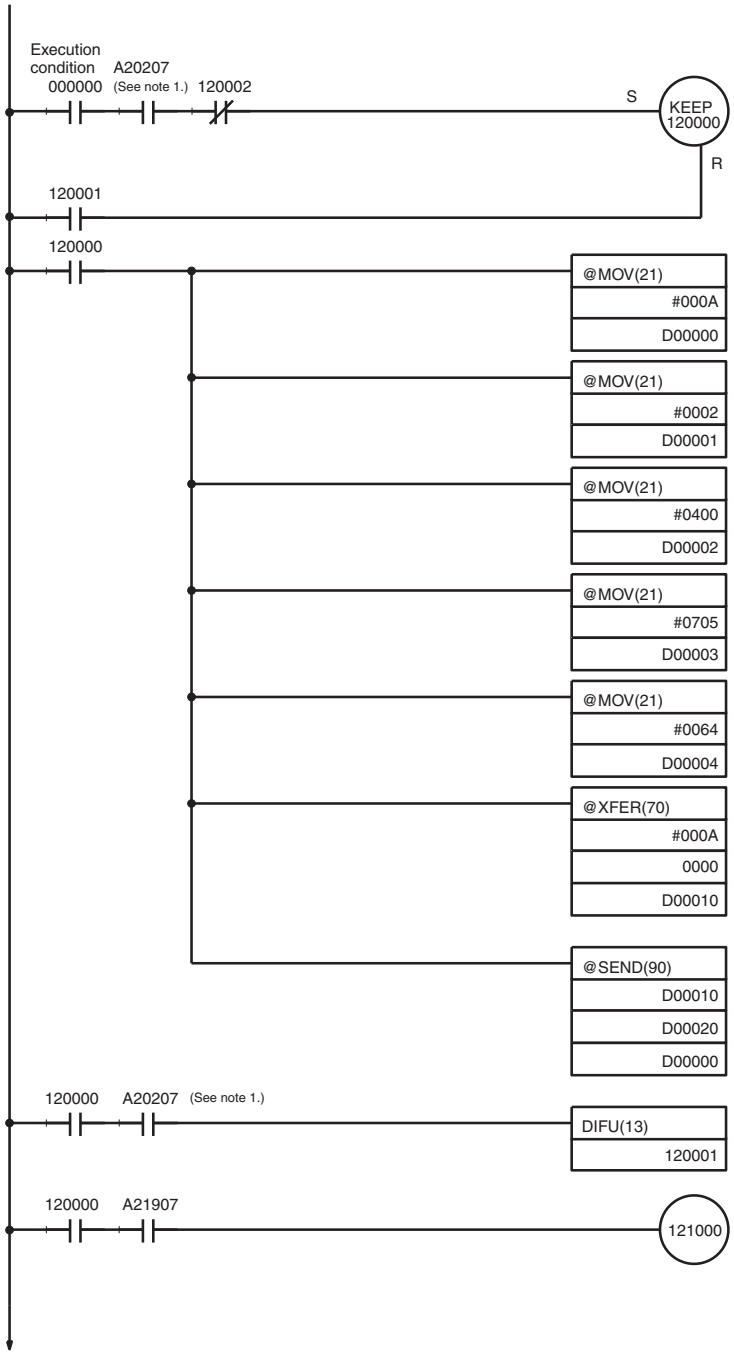
Timing of Communications Flag Changes

- The Communications Port Enabled Flag remains OFF during communications and turns ON when they are completed (regardless of whether or not an error occurs).
- The Communications Port Error Flag retains its status until the next transmission or reception.
- The Communications Port Error Flag turns OFF with the execution of the next communications instruction even if there was an abnormal completion.

Example



8-6-5 Program Example



When the Communications Port Enabled Flag for port 7 is ON, and RECV(098) is not being executed, the send execution program will start when execution condition CIO 000000 turns ON.

Input CIO 120000 remains ON from the start of SEND(090) execution until completion.

Control Data Creation

Word	Contents	Meaning
D0000	00 0A	Number of send words = 10
D0001	00 02	Destination network number = 2
D0002	04 00	Destination node number = 4 Destination unit address = 0
D0003	07 05	Response required. Communications port No. used = 7 Number of retries = 5
D0004	00 64	Response monitor time = 10 s

Send Data Creation

Ten words of data from word CIO 0000 is stored from D00010 onwards.

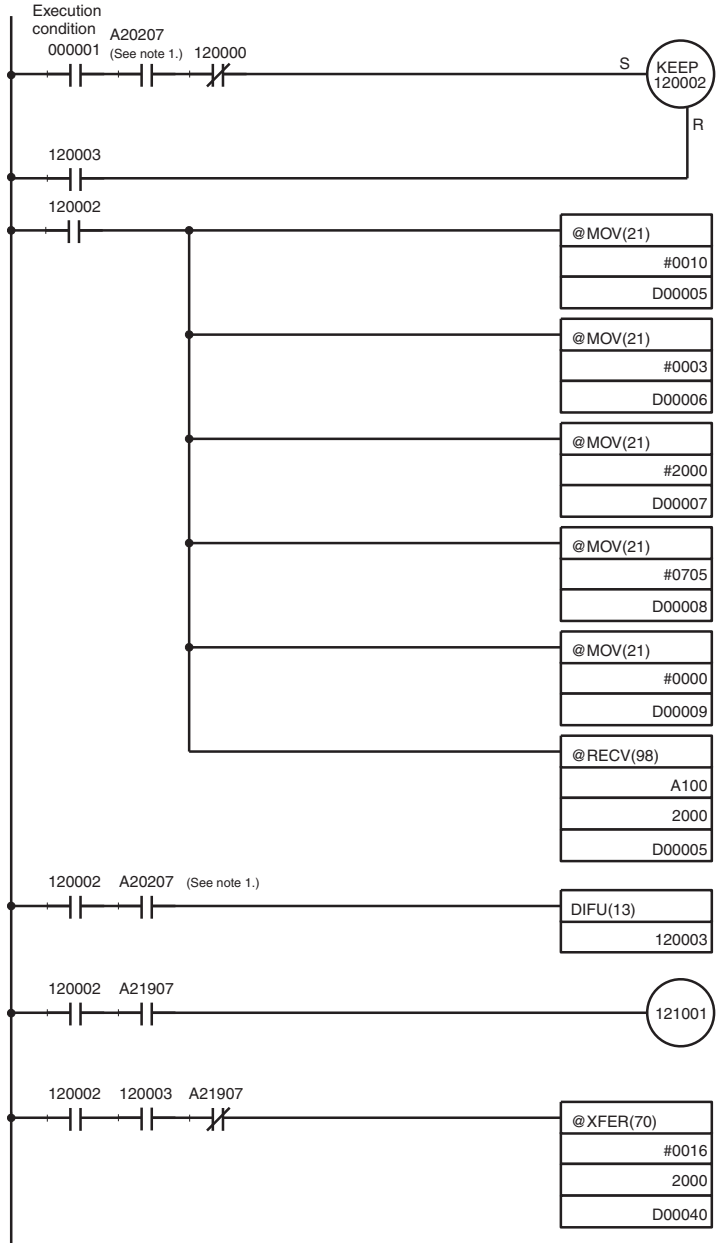
Ten words of data from D00010 at the local node is sent to D00020 onwards at network number 2, node number 4, unit address 0 (the PLC).

Reset Input Creation

Send Error Display

(Continued on next page.)

(Continued from previous page.)



When the Communications Port Enabled Flag for port 7 is ON, and SEND(090) is not being executed, the transmission execution program will start when execution condition CIO 000001 turns ON.

Input CIO 120002 remains ON from the start of RECV(098) execution until completion.

Control Data Creation

Word	Contents		Meaning
D0005	00	10	Number of reception words = 16
D0006	00	03	Source network number = 3
D0007	20	00	Source node number = 32 Source unit address = 0
D0008	07	05	Response required. Communications port No. used = 7 Number of retries = 5
D0009	00	00	Response monitor time = Default

A total of 16 words of data beginning from word A100 at network number 3, node number 32, unit address 0 (the PLC) is received at word CIO 2000 onwards of the local node.

Reset Input Creation

Reception Error Display

Reception Data Processing

If there is no reception processing completion error, the 16 words of data received from word CIO 2000 onwards is stored at D00040 onwards.

Note

1. With CS/CJ-series PLCs, the Communications Port Enabled Flags at bits 0 to 7 in word A202 turn OFF even when the PCMR(260) instruction is being executed using the ports corresponding to those flags.
2. Before using the sample program as is, confirm that the memory areas (words and bits) used in the sample program are not already being used in the user program o r by Special I/O Units.

8-7 Precautions on High Traffic in FINS Communications

When applications are constructed using FINS communications services, communications errors (from multiple response timeouts) may occasionally occur due to high traffic, depending on the system configuration and the application programs. This section describes precautions for systems with high traffic in FINS communications.

■ Conditions for High Traffic

A heavy communications load may occur at an EtherNet/IP Unit or built-in EtherNet/IP port if FINS messages and CIP messages from multiple nodes are concentrated on that EtherNet/IP Unit or built-in EtherNet/IP port. The EtherNet/IP Unit or built-in EtherNet/IP port and the CPU Unit may have insufficient processing capacity for the volume of FINS messages (commands) that are coming from the network.

For example, suppose that approximately 20 ms are required to process a single FINS frame (i.e., 20 ms from the time that the command is received at the EtherNet/IP Unit or built-in EtherNet/IP port until a response is sent). If 100 or more FINS frames (commands) are received at once from multiple communicating nodes, it will take approximately 2 seconds to send a response to the last command. If a timeout is set at the remote node for 2 seconds or less, then a timeout will be generated. A retry will begin due to the timeout, and the traffic to the EtherNet/IP Unit or built-in EtherNet/IP port will thus be increased even further, until ultimately the responses to all the nodes will be too slow. At this point, the system is overloaded.

■ Avoiding Errors due to High Traffic

To avoid high traffic from FINS communications, the communications load must be kept down to a reasonable level. To accomplish this, follow the procedure below.

1. Specify the node where FINS frames seem to be concentrated.
2. Estimate the total processing time for all of the FINS frames processed at that node. (For details, refer to *10-4-1 Maximum Transmission Delays (Excluding Delays in the Network)*.)
3. Set the timeout value for all of the SEND, RECV, and CMND FINS commands at all the remote nodes to at least 1.5 times the total processing time for all of the FINS frames.
4. As much as possible, implement communications traffic testing up to the point of actual system operation. If any problem occurs, adjust the traffic.
5. When a commercially-available protocol analyzer is used, then the actual FINS frame processing time (i.e., the time from when a command is received at the EtherNet/IP Unit or built-in EtherNet/IP port until a response is sent) can be measured under high traffic conditions and the communications traffic can be further adjusted as required.

SECTION 9
Message Communications

This section describes message communications using FINS commands sent from the ladder program in the CPU Unit of the PLC.

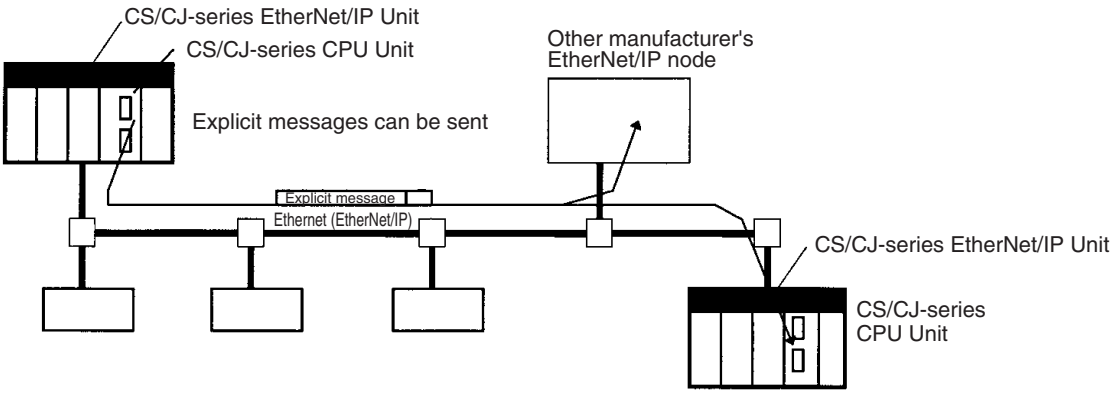
9-1 Sending Explicit Messages 274
9-1-1 Sending Explicit Messages Using CMND 282
9-2 Receiving Explicit Messages 287
9-2-1 PLC Object 288
9-2-2 Connection Configuration Object 300

9-1 Sending Explicit Messages

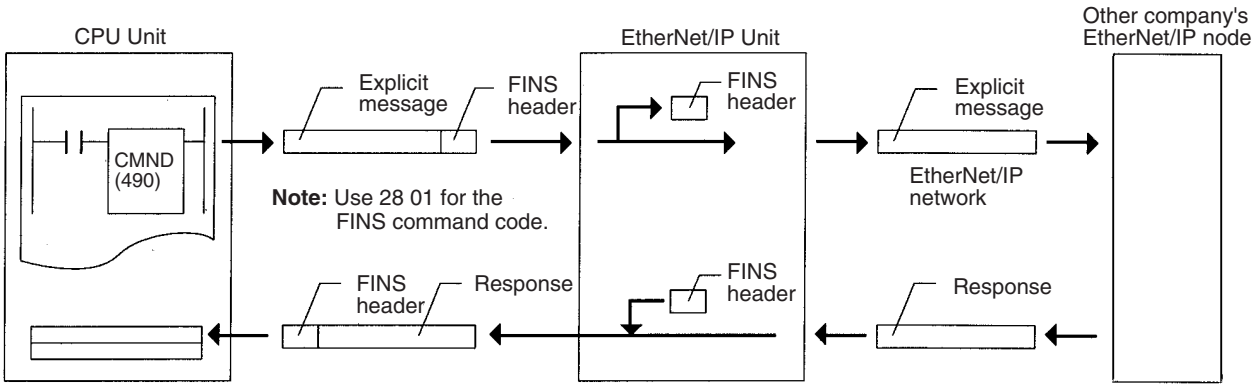
CS/CJ-series EtherNet/IP Units and built-in EtherNet/IP ports can send explicit messages. Only CIP unconnected message (UCMM) communications can be used to send explicit messages. Explicit messages can be sent to the following destinations.

- EtherNet/IP Units made by other manufacturers
- Other PLCs with a CS/CJ-series EtherNet/IP Unit or built-in EtherNet/IP port

Example



When the destination is another company's EtherNet/IP node, an explicit message can be sent to the EtherNet/IP Unit or built-in EtherNet/IP port using FINS command code 28 01 or 28 10, through the Connection Manager class's Unconnected Send service, as shown in the following diagram.



When sending an explicit message, set the local node's EtherNet/IP Unit or built-in EtherNet/IP port as the destination of the FINS command, and not the actual destination (other company's EtherNet/IP node). Specify the node address of the actual destination in the command data of the explicit message send command.

There are two ways to send an explicit message send command:

1,2,3... 1. CIP UCMM MESSAGE SEND command (28 10)

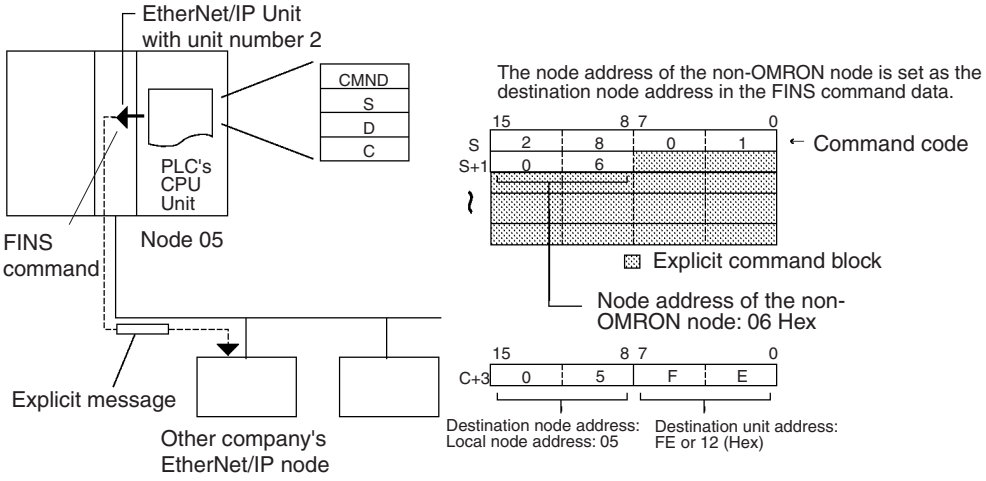
Messages can be routed through multiple CIP network layers. (Messages can be routed through 16 network levels. The explicit message send command may time out if routing is attempted for more than 16 networks.

2. EXPLICIT MESSAGE SEND command for DeviceNet Units (28 01)

This command is compatible with the DeviceNet Unit's explicit message send command (28 01) in the ladder program. The message must be sent

in the same network layer and the remote node's IP address range is limited.

The following diagram shows an example of actual node address specifications.



Note Depending on conditions, the destination slave may not always accept an explicit message. Always perform retry processing when sending explicit messages.

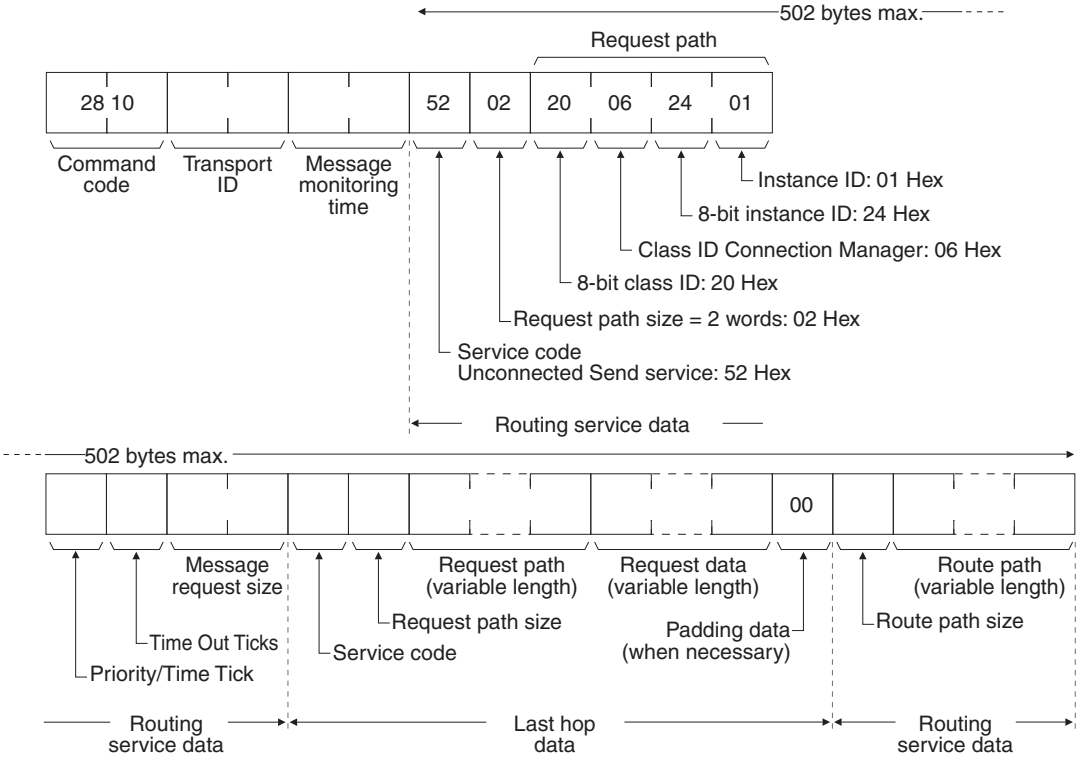
CIP UCMM MESSAGE SEND (28 10)

This command sends an explicit message for CIP routing to another node's specified class and receives a response. There are two command formats: one with a specified route path (path to the target device), and the other without the route path.

Command Block

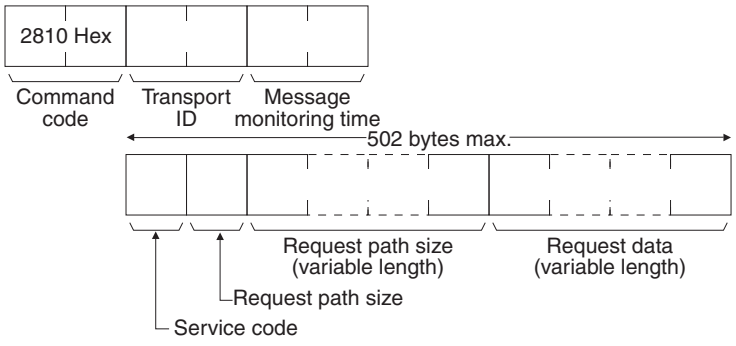
- Relay Hop Format

  The following format includes the route path (routing service data). Specify the entire routing path in the command's request path.



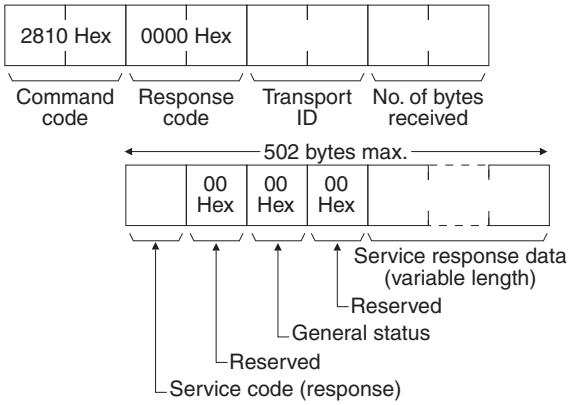
- Last Hop Format

  The following format does not include the route path.

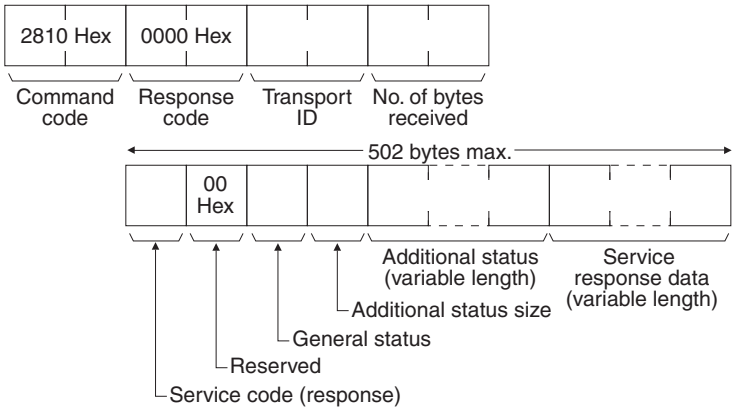


Response Block

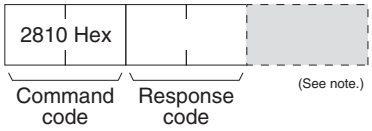
The following normal response is returned to a transmitted CIP UCMM MESSAGE SEND command if it was completed normally.



The following response is returned if an error occurs in a transmitted CIP UCMM MESSAGE SEND command.



The following response is returned if the CIP UCMM MESSAGE SEND command could not be sent or timed out.



Note: There may be additional data depending on the response code, e.g., for a relay error.

Parameters

Transport ID (command, response):

When multiple CIP UCMM MESSAGE SEND commands are being sent, the Transport ID identifies the commands. This Transport ID is returned unchanged in the response.

Message monitoring time (command):

Specifies the monitoring time in 10-ms units, in order to monitor the time from the point that the EtherNet/IP Unit or built-in EtherNet/IP port extracts the CIP explicit message from this command until a response is received. The monitoring time can be set between 0.01 and 655.35 s.

Service code (command, response):

In the command, this code is the service code defined for EtherNet/IP.
In the response, bit 15 of the service code specified in the command is turned ON and the resulting value is returned.

In the routing format for rely hops, the first service code (in the routing service data) is 52 Hex, which is the Unconnected Send service.

Request path size (command):

Specifies the number of words of data that are specified in the request path field.

In the routing format for relay hops, the first request path size (in the routing service data) is 02 Hex.

Request path (command):

Specifies the request path (class ID, instance ID, etc.) in bytes. If there is an odd number of bytes, pad the last byte with a 0 so that the data is in full word units.

In the routing format for relay hops, the first request path (in the routing service data) is 20 06 24 01 Hex (Connection Manager). For details, refer to the description of the *Route Path* in *Appendix D CIP Message Communications*.

Request data (command):

In the command, specify the data determined by the service code.
In the response, the reception data determined by the service code will be returned.

Priority/Time tick (command):

The timeout time specified by the Priority Time Tick is used as a base value to specify the actual timeout value. For details, refer to the description of the *Priority/Time Ticks and Time Out Ticks* at the end of *Appendix D CIP Message Communications*.

Time Out Ticks (command):

Specifies the base value of the timeout time. For details, refer to the description of the *Priority/Time Ticks and Time Out Ticks* at the end of *Appendix D CIP Message Communications*.

Message request size (command):

Specifies the number of bytes of data from the second service code to the request data. The data size is specified in LSB, MSB order.

For example, if there are 400 bytes, the data size is 0190 hex bytes, which is entered as 90 01 hex.

Padding data (command):

If the message request size specifies an odd number of bytes, use 00 hex as padding in the last byte. The padding data is not required if there is an even number of bytes.

Route path size (command):

Specifies the number of words of data that are specified in the route path field.

Route path (command):

Specifies the path (route path) to the target device. For details, refer to the description of the *Route Path* in *Appendix D CIP Message Communications*.

No. of bytes received (response):

This hexadecimal value is returned to indicate the number of bytes of data received after the service code (response).

General status (response):

The general status defined in EtherNet/IP is returned. The normal response is 00 hex. For details, refer to the description of the *Response Codes* in *Appendix D CIP Message Communications*.

Additional status size (response):

This hexadecimal value is returned to indicate the number of words of data in the additional status field.

Additional status (response):

The additional status defined in EtherNet/IP is returned. For details, refer to the description of the *Response Codes* in *Appendix D CIP Message Communications*.

Service response data (response):

The reception data determined by the service code is returned.

Description

- The CIP UCMM MESSAGE SEND command is used to send an EtherNet/IP-defined explicit message to another company's node and receive a response.
- Unlike other FINS commands, the destination of a CIP UCMM MESSAGE SEND command's control data is the local node's EtherNet/IP Unit or built-in EtherNet/IP port, and the actual destination node is specified in the command's route path.
- When an EtherNet/IP Unit or built-in EtherNet/IP port receives an explicit message, it automatically returns a response to the message.
- When specifying the timeout time, the proper values are different for last-hop and relay-hop methods. With the last-hop method, set the timeout time for the actual request service processing. With the relay-hop method, the timeout for the relay path must be added to the timeout time for the actual request service processing.

  In CIP routing, the node/Unit performing the routing subtracts the timeout time for 1 hop, deletes its own address from the routing information, and relays the message to the next node/Unit.

  Set the following timeout values for command processing.

  The maximum number of relay nodes (Units) is 16. If the number is more than 16, the explicit message send command may time out even if the conditions of network and each node (Unit) are normal. If more than 16 relay nodes (Units) have been set, a constant time must be specified for the request service processing timeout time (normally 0000 hex).

  - Priority Time Tick and Time Out Ticks = (5 s $\times$ Number of relay nodes/Units) + Request processing timeout
  - Message monitoring time $\geq$ Priority Time Tick and Time Out Ticks
  - CMND timeout set value = Message monitoring time

  A timeout may occur sooner than the actual set value, depending on the point where the timeout occurs in the path.
- General status = 01 hex, and Additional status = 0204 hex

  A FINS timeout error response (0205 hex) may occur if the CMND timeout set value or message monitoring time is less than the Priority Time Tick and Time Out Ticks.

Note

1. For details on the parameters of explicit messages, refer to the EtherNet/IP and CIP specifications.
2. Acquire EtherNet/IP and CIP specifications from the ODVA.

   Website: https://www.odva.org/

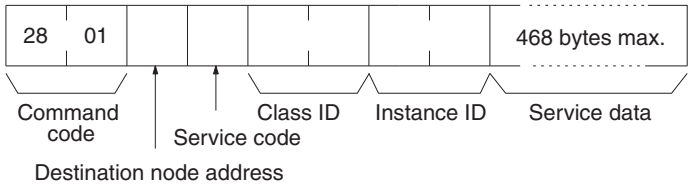
EXPLICIT MESSAGE SEND (28 01)

EXPLICIT MESSAGE SEND will send a DeviceNet Unit-compatible explicit message to the specified class of another node and receive a response.

The other node is specified with the destination node address in the command. The actual destination IP address is as follows.

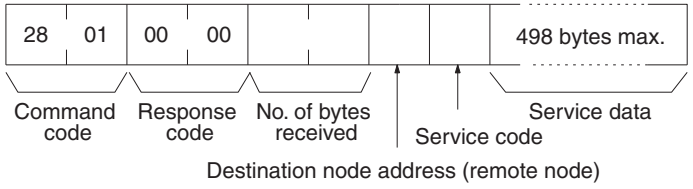
Destination IP address = (Local IP address & Subnet mask) + Destination node address

Command Block



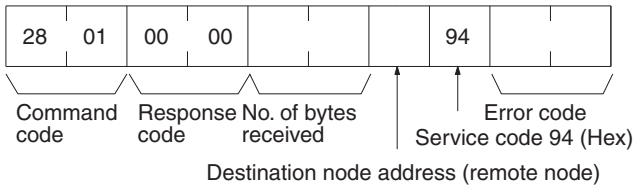
Response Block

Normal Response

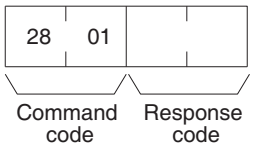


Error Responses

The following response is returned if an error occurs for the explicit message.



The following response is returned if the explicit message cannot be sent or times out.



Parameters

Destination node address (command):

The node address of the destination of the explicit message.

The node address of the local EtherNet/IP Unit or built-in EtherNet/IP port is specified in the control data for the CMND, but the node address of the actual destination is specified here in the FINS command. The destination node address cannot be set to 00 hex or FF hex.

Service code (command, response):

A service code defined for EtherNet/IP. In a normal response, bit 15 of the service code specified in the command will be turned ON and returned. In an error response, 94 Hex will always be returned.

Class ID (command):

The class ID of the destination of the explicit message.

Instance ID (command):

The instance ID of the destination of the explicit message.

Service data (command, response):

The data defined for the services codes.
In the response, the reception data determined by the service code will be returned.

No. of bytes received (response):

The number of bytes received from the destination node address (remote node).

Destination node address (remote node):

The node address of the OMRON Special I/O Slave Unit or Slave manufactured by another company to which the explicit message was sent is returned.

Error code (response):

An error code defined in EtherNet/IP (1-byte general status and 2-byte additional status) is returned. The data format is DeviceNet-compatible (2 bytes total), so the returned Error Code is converted to the 1-byte general status and a 1-byte additional status (high byte only).

Description

- The EXPLICIT MESSAGE SEND command is used to send an EtherNet/IP-defined explicit message to another company's node and receive a response.
- Unlike other FINS commands, the destination of a EXPLICIT MESSAGE SEND command's control data is the local node's EtherNet/IP Unit or built-in EtherNet/IP port, and the actual destination node is specified in the command's route path.

  Always specify the local node's EtherNet/IP Unit or built-in EtherNet/IP port in the CMND instruction's control data. An error will occur if another node's Master Unit is specified as the destination.
- When an EtherNet/IP Unit or built-in EtherNet/IP port receives an explicit message, it automatically returns a response to the message.
- A time of 2 s is used for request service processing timeouts.
  Set the CMND instruction's timeout set value to 2 s or longer.

  When there is a timeout, the error code will be 0102 hex.
  When the CMND instruction's timeout set value is less than 2 s, a FINS timeout error response of 0205 hex may occur.

Note

1. For details on the parameters of explicit messages, refer to the EtherNet/IP specifications.
2. The Open DeviceNet Vendor Association, Inc. (ODVA) can be contacted at the following address to obtain copies of the EtherNet/IP and CIP specifications.

   ODVA, Inc.
   Ann Arbor, Michigan 48108-5006 USA

   Email: odva@odva.org

   TEL: 1-734-975-8840

   WEB: https://www.odva.org/

9-1-1 Sending Explicit Messages Using CMND

With a CS/CJ-series EtherNet/IP Unit or built-in EtherNet/IP port, a CMND in the CPU Unit's ladder program can send CIP UCMM explicit messages.

Send the CIP UCMM explicit message's command data in a FINS command following the 2810 hex FINS command code.

The CIP UCMM explicit message's response is received following the 2810 hex FINS command code and the FINS completion code.

The following command is used: [CMND S D C]

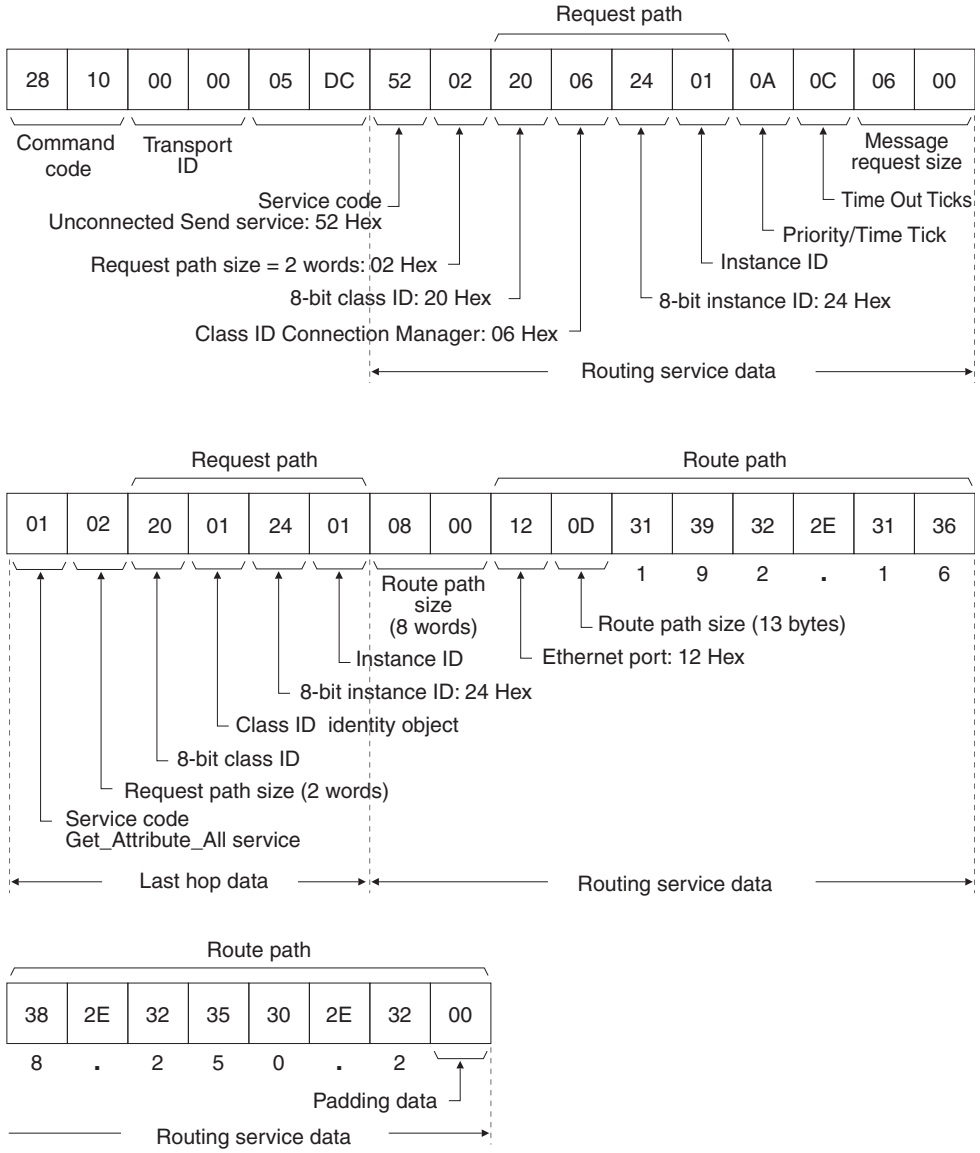
S: First command word

D: First response word

C: First control data word

Command data is set in order starting with the word specified for the CMND operand S (first command word) and continuing with words with higher addresses in I/O memory in the command block format.

Command Format Example: Get_Attribute_All Service to Identity Object

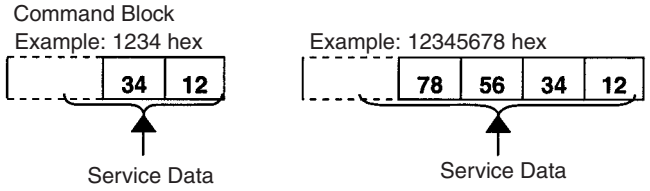


Setting the Command Data for CMND

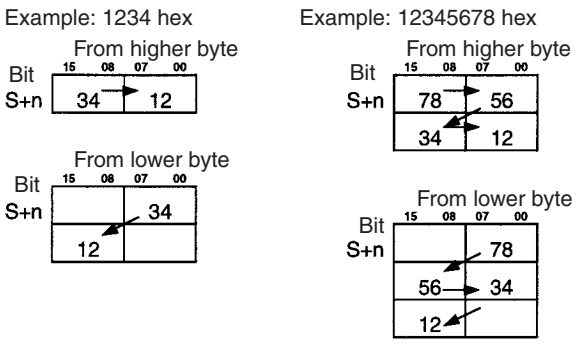
Bit	15 08	07 00		
S+0	28	10	FINS command code	
S+1	00	00	Transport ID	
S+2	05	DC	Message monitoring time	
S+3	52	02	Service code = 52 hex, Request path size = 02 hex	
S+4	20	06	8-bit class ID = 20 hex, Class ID = 06 hex (Connection Manager)	
S+5	24	01	8-bit instance ID = 24 hex (request path), Instance ID = 01 hex	
S+6	0A	0C	Priority/Time Tick = 0A hex, Time Out Ticks = 0C hex	
S+7	06	00	Message request size	
S+8	01	02	Service code = 01 hex (Get_Attribute_All service), Request path size = 02 hex	
S+9	20	01	Link path	8-bit class ID = 20 hex, Class ID = 01 hex (Identity Object)
S+10	24	01		8-bit instance ID = 24 hex, Instance ID = 01 hex
S+11	08	00	Route path size = 8 words	
S+12	12	0D	Ethernet port = 12 hex (Extended Link Address Size = 1 hex, Ethernet port number = 2 hex), Route path size = 13 bytes	
S+13	31	39	1 9	
S+14	32	2E	2 .	
S+15	31	36	1 6	
S+16	38	2E	8 .	Route path: IP address
S+17	32	35	2 5	192.168.250.2
S+18	30	2E	0 .	
S+19	32	00	2	

The response data is set in the same way, starting from the word specified for CMND operand D (first response word) and continuing with words with higher addresses in I/O memory in the response block format.

Note Request path data or request data that is in word (2-byte) or double-word (4-byte) units, such as word data and ERROR CLEAR codes, is specified from low to high (U) bytes in command block format. For example, to specify word data 1234 hex, specify 34 hex and then 12 hex. To specify the double word data 12345678 hex, specify 78 hex, 56 hex, 34 hex, and then 12 hex. The command blocks are shown in the following diagram.



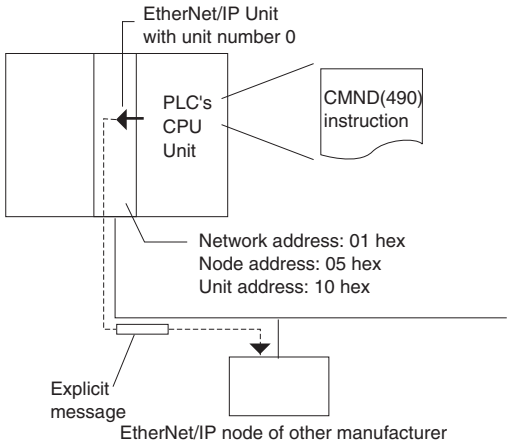
The format from CMND(490) operand S onwards will be set as follows:



Similarly, when the additional status data and service response data in the response block is in word (2-byte) or double-word (4-byte) units, such as word

data and ERROR CLEAR codes, is also returned in the same order from low to high bytes in the response block.

Example: Sending Explicit Messages Using CMND



Operation

The identity object information (class ID = 01 hex) is read from the other company's EtherNet/IP node at IP address 192.168.250.2, using the CIP UCMM MESSAGE SEND command, 28 10. The command data is stored in the DM Area starting at DM01000, and the response data is stored in the DM Area starting at D02000. If the command ends with an error, the end code is stored in D00006 and command transmission is retried.

Command Details

[CMND S D C]

S = D01000: First command word

D01000 = 2810 hex	Command Code
D01001 = 0000 hex	Transport ID: 0000 hex
D01002 = 05DC hex	Message monitoring time: 15.00 s
D01003 = 5202 hex	Slave code: 52 hex (Unconnected Send) Request path size: 2 words
D01004 = 2006 hex	Request path: 20 06 24 01 hex (Connection Manager) Class ID: 06 hex
D01005 = 2401 hex	Instance ID: 01 hex

Words S+6 to S+19 contain the request data.

D01006 = 0A0C hex	Priority/Time_Tick: 0A hex Time Out Ticks: 0C hex
D01007 = 0600 hex	Message request size: 6 bytes

Words S+8 to S+10 contain the request message request.

D01008 = 0102 hex	Service: 01 hex (Get_Attribute_All) Request path size: 2 words

Words S+9 and S+10 contain the request path.

D01009 = 2001 hex	8-bit class ID: 20 hex Class ID: 01 hex
D01010 = 2401 hex	8-bit instance ID: 24 hex Instance ID: 01 hex (Identity object)

Words S+11to S+19 contain the root path.

D01011 = 0800 hex	Route path size: 8 words
D01012 = 120D hex	Extended link address size = 1 hex Route path size: 13 bytes (characters) = 0D hex
D01013 = 3139 hex	IP address: “19”
D01014 = 322E hex	IP address: “2.”
D01015 = 3136 hex	IP address: “16”

D01016 = 382E hex IP address: “8.”
D01017 = 3235 hex IP address: “25”
D01018 = 302E hex IP address: “0.”
D01019 = 3200 hex IP address: “2”
Padding data: 00 hex

D = D02000: First response word at local node
C = D00000: First control word

D00000 = 0028 hex Number of command bytes: 40 bytes
D00001 = 0064 hex Number of response bytes: 100 bytes
D00002 = 0001 hex Destination network address: 1
D00003 = 0510 hex Destination node address: 5
Destination unit address: FE hex (or 10 hex)
D00004 = 0000 hex Response, communications port 0, no retries
D00005 = 00A0 hex Response monitoring time: 16.0 s

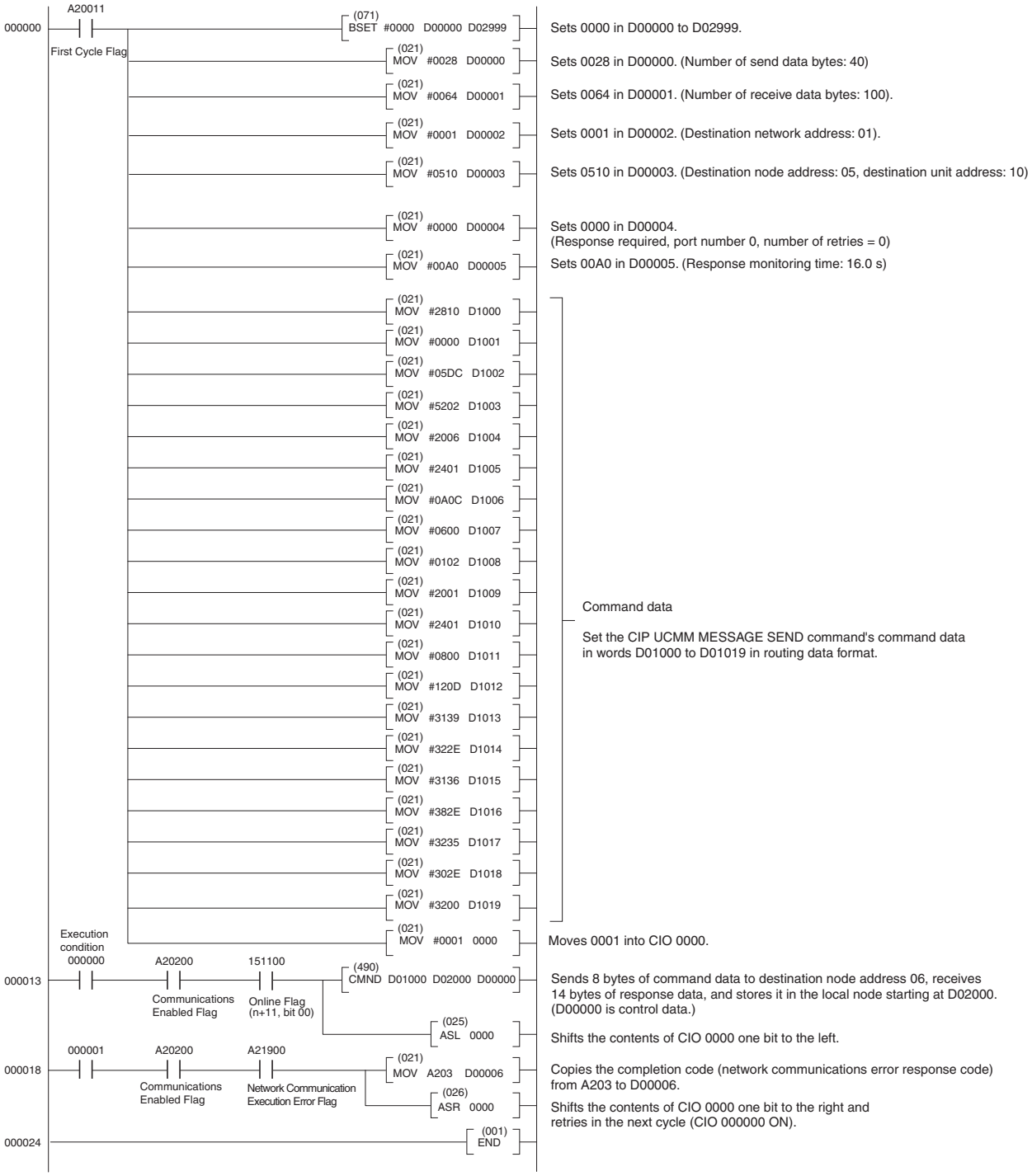
Response

D02000 = 2810 hex Command code
D02001 = 0000 hex FINS completion code
D02002 = 0000 hex Transport ID
D02003 = 001D hex Number of bytes received: 29 bytes
D02004 = 8100 hex Service code (response): 81 hex
Reserved: 00 hex
D02005 = 0000 hex General status: 00 hex
Reserved: 00 hex

Words C+6 to C+18 contain the service response data.

D02006: 2F00 hex
D02007: 0C00 hex
D02008: 0C00 hex
D02009: 0101 hex
D020010: 3000 hex
D020011: 5303 hex
D020012: 0011 hex
D020013: 0A43 hex
D020014: 5331 hex
D020015: 572D hex
D020016: 4549 hex
D020017: 5032 hex
D020018: 3100 hex

Program Example



9-2 Receiving Explicit Messages

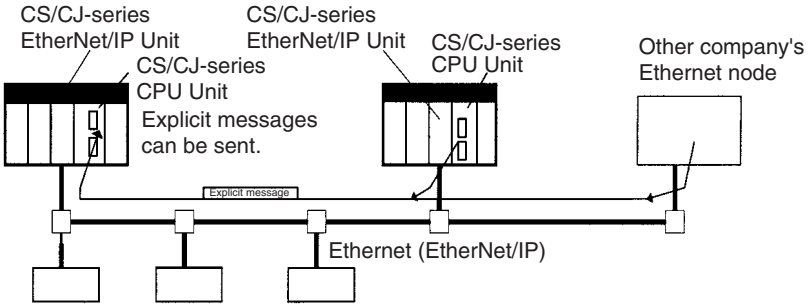
The CS/CJ-series EtherNet/IP Units (built-in port) can receive Explicit message. The Unit will receive messages addressed to the PLC Object, process service requests addressed to the CPU Unit, and return responses. The CS/CJ-series EtherNet/IP Units and built-in EtherNet/IP ports support CIP unconnected message (UCMM) communications and CIP connected (Class 3) communications as reception functions.

Explicit messages can be received from the following sources:

- EtherNet/IP nodes made by other manufacturers
- OMRON PLCs with a CS/CJ-series EtherNet/IP Unit or a CPU Unit with a built-in EtherNet/IP port.*

  * Messages from CS/CJ-series EtherNet/IP Units and built-in EtherNet/IP ports must be CIP unconnected messages (UCMM).

Example



The CS/CJ-series EtherNet/IP Units (built-in port) are equipped with the following objects, and can execute services associated with those objects.

- PLC Object
- Connection Configuration Object

9-2-1 PLC Object

List of PLC Object Services

PLC Objects provide the following services.

Status Read/Write for CPU Units

Services	Service code	Class ID	Instance ID	Request service data	Contents
CPU Unit Information Read	0E Hex	C4 Hex (2F Hex) (See note 1.)	00 Hex	Attribute ID = 64 Hex	Reads the operating mode of the CPU Unit.
				Attribute ID = 65 Hex	Reads if there is a fatal or non-fatal error in the CPU Unit.
				Attribute ID = 66 Hex	Reads CPU Unit model.
CPU Unit Write	10 Hex			Attribute ID = 64 Hex, Attribute Value	Changes the operating mode of the CPU Unit.
				Attribute ID = 65 Hex Attribute Value	Clears errors.
CPU Unit Status Read	40 Hex			None	Reads the detailed status of the CPU Unit. Operation status: Stop, run, CPU standby Operating modes: PROGRAM, MONITOR, RUN Fatal error information: Error flags, including memory errors, I/O bus errors, system errors Messages: Message No. when MSB instruction executed by CPU Unit Error codes: Error code for the most serious errors Error messages: Messages stored in CPU Unit when FAL/FALS instruction executed

I/O Memory Read/Write for CPU Units

Service	Service code	Class ID	Instance ID	Request service data	Contents
Byte Data Read	1C Hex	C4 Hex (2F Hex) (See note 1.)	Specifies area (01 Hex to 20 Hex) (See note 2.)	Address, No. of read bytes	Reads the specified node data in byte units. The word data is read in order, from high to low bytes. Read data: 200 bytes max.
Word Data Read	1D Hex			Address, No. of read words	Reads the specified node data in word units. The word data is read in order, from high to low bytes. Read data: 200 bytes max.
Byte Data Write	1E Hex			Address, byte data	Writes the specified node data in byte units. The word data is specified in order, from high to low bytes. Write data: 200 bytes max.
Word Data Write	1F Hex			Address, word data	Writes the specified node data in word units. The word data is specified in order, from high to low bytes. Write data: 200 bytes max.

Note (1) For an EtherNet/IP Unit or built-in EtherNet/IP port excluding CS1W/CJ1W-EIP21S, the class ID depends on the unit version as shown in the figure below.

Models	EtherNet/IP's Unit version	Class ID
CS1W/CJ1WEIP21S CJ3M-CPU3□	Ver.1.0 or later	C4
CS1W/CJ1W-EIP21 CJ2B-EIP21(CJ2H-CPU6□EIP) CJ2M-EIP21(CJ2M-CPU3□)	Ver.2.0 or later	C4
	Ver.1.0	2F

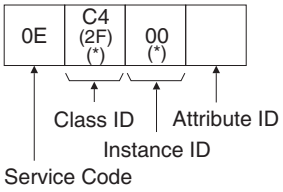
Note that the class ID is C4 hex for CS1W/CJ1W-EIP21S.

(2) You can specify up to the value corresponding to the number of EM Area banks that the CPU Unit has. However, for the CS1D-CPU68HA, you can specify up to 14 hex here although the CPU Unit has EM Area banks that allow for specifying up to 18 hex.

CPU Information Read (Service Code: 0E Hex)

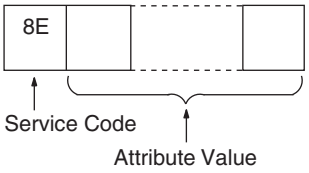
Reads CPU Unit information, including operating mode, fatal/non-fatal errors, and the CPU Unit model.

Command Block



Note A body format of either 8 bits or 16 bits is possible.

Response Block



Parameters

Service code (command, response): 0E Hex is specified for commands. For responses, the highest bit be ON and 8E Hex will be returned.

Class ID (command):
The class ID is C4 hex.

Note that the class ID is 2F hex for CS1W/CJ1W-EIP21 or CJ2H-CPU6□-EIP Unit version 1.0.

Instance ID (command): Always 00 Hex.

Attribute ID (command): The read information is specified by the attribute ID. The attribute IDs are listed in the following table.

Attribute ID (Hex)	Contents	Attribute value size
64	CPU Unit operating mode	1 word (2 bytes)
65	CPU Unit errors	1 word (2 bytes)
66	CPU Unit model	22 bytes

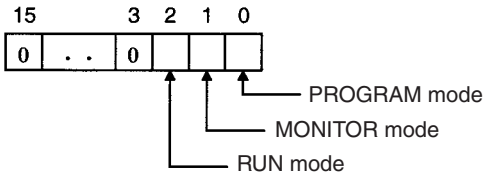
- CPU Operating Mode (when Attribute ID = 64 Hex)
  Reads the CPU Unit operating mode.
- CPU Unit Errors (when Attribute ID = 65 Hex)
  Reads if there are any fatal or non-fatal errors in the CPU Unit.
- CPU Unit Model (when Attribute ID = 66 Hex)
  Reads the CPU Unit model.

Read data (response): The specified information is returned in order.

- CPU Unit operating mode (attribute ID = 64 Hex).

The CPU Unit operating mode is returned in 1-word (2-byte) hexadecimal format, as follows:

0001 Hex: PROGRAM mode; 0002 Hex: MONITOR mode;
0004 Hex: RUN mode

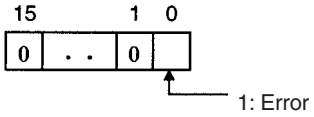


Note The codes for the above modes are 1-word (2-byte) data and are returned in low byte first. For example, for PROGRAM mode, the code is returned as 01 Hex followed by 00 Hex.

- CPU Unit Errors (when Attribute ID = 65 Hex)

The CPU Unit fatal/non-fatal error data is returned in 1-word (2-byte) hexadecimal format, as follows:

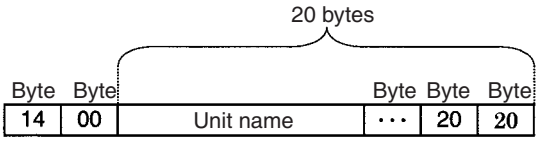
01 Hex: Error; 00 Hex: No error.



- CPU Unit Model (when Attribute ID = 66 Hex)

The CPU Unit model is returned in ASCII.

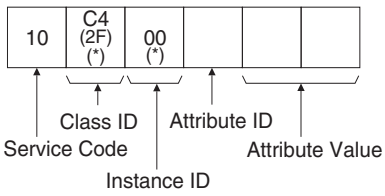
Size: 2 bytes (Always 1400 Hex) + Model: 20 bytes (fixed). Unused area is filled with 20 Hex (spaces) and returned.



CPU Unit Write (Service Code: 10 Hex)

This PLC Object service writes CPU Unit information, including the operating mode and clearing errors.

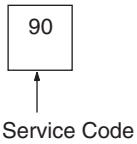
Command Block



For EtherNet/IP Units or built-in EtherNet/IP ports excluding CS1W/CJ1W-EIP21S, the class ID depends on the unit version. (Refer to *Parameters* below.)

Note A body format of either 8 bits or 16 bits is possible.

Response Block



Parameters

Service code (command, response): 10 Hex is specified for commands. For responses, the highest bit will turn ON and 90E Hex will be returned.

Class ID (command):
The class ID is C4 hex.

Note that the class ID is 2F hex for CS1W/CJ1W-EIP21 or CJ2H-CPU6□-EIP Unit version 1.0.

Instance ID (command): Always 00 Hex.

Attribute ID (command): Information to write is specified by the attribute ID. The attribute IDs are listed in the following table.

Attribute ID (Hex)	Contents	Attribute value size
64	CPU Unit operating mode	1 word (2 bytes)
65	CPU Unit errors	1 word (2 bytes)

- CPU Operating Mode (Attribute ID = 64 Hex)
  Changes the CPU Unit operating mode.
  The Attribute Values are as follows:
  0001 Hex: PROGRAM mode; 0002 Hex: MONITOR mode;
  0004 Hex: RUN mode

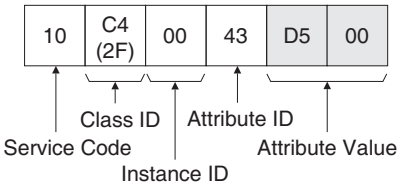
Note The specified code for the above operating modes are 1-word (2-byte data, and are specified with the low byte first. For example, for PROGRAM mode, the code is specified as 01 Hex followed by 00 Hex. Accordingly, the low to high bytes for the above codes are set as high to low bytes in I/O memory, when setting the codes as data for operand S of CMND(490).

- Clearing CPU Unit Errors (when Attribute ID = 65 Hex)
  Clears any fatal or non-fatal errors in the CPU Unit. Sets the error clear code to Attribute Value. The error clear codes are listed in the following table.

Error code (Hex)	Data cleared
FFFE	Current error (clears the highest priority error)
0008B	Interrupt task error
009A	Basic I/O error
009B	PLC Setup error
02F0	Inner Board non-fatal error
0300 to 035F	Special I/O Unit error
00A0 to 00A1	SYSMAC BUS error
0500 to 055F	Special I/O Unit setting error
00E7	I/O verification error When registered and actual I/O tables are different When disconnecting or connecting I/O Units
00F7	Battery error
0200 to 020F	CS/CJ-series CPU Bus Unit error (last 2 digits are binary code for the Unit No.) For parity errors generated when data transferred between CS/CJ-series CPU Bus Unit and CPU Unit For watchdog timer errors in CS/CJ-series CPU Bus Unit
0400 to 040F	CPU Bus Unit setting error (last 2 digits are binary code for the Unit No.)
4101 to 42FF	System error (FAL): FAL instruction executed

Note Error clear codes are 1-word (2-byte) data, so the above codes are specified with the low byte first. The low to high bytes for the above codes are set as high to low bytes in I/O memory, when setting the codes as data for operand S of CMND(490). For example, to specify

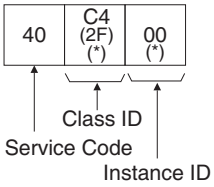
battery error 00F7 Hex, specify the error code as F7 Hex followed by 00 Hex, as shown in the following diagram.



CPU Unit Status Read (Service Code: 40 Hex)

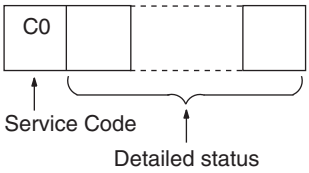
This PLC Object service reads status details (operation status, operating mode, fatal and non-fatal errors, etc.) from the CPU Unit.

Command Block



Note A body format of either 8 bits or 16 bits is possible.

Response Block



Parameters

Service code (command, response): 40 Hex is specified for commands. For responses, the highest bit will turn ON and C0 Hex will be returned.

Class ID (command):
The class ID is C4 hex.

Note that the class ID is 2F hex for CS1W/CJ1W-EIP21 or CJ2H-CPU6□-EIP Unit version 1.0.

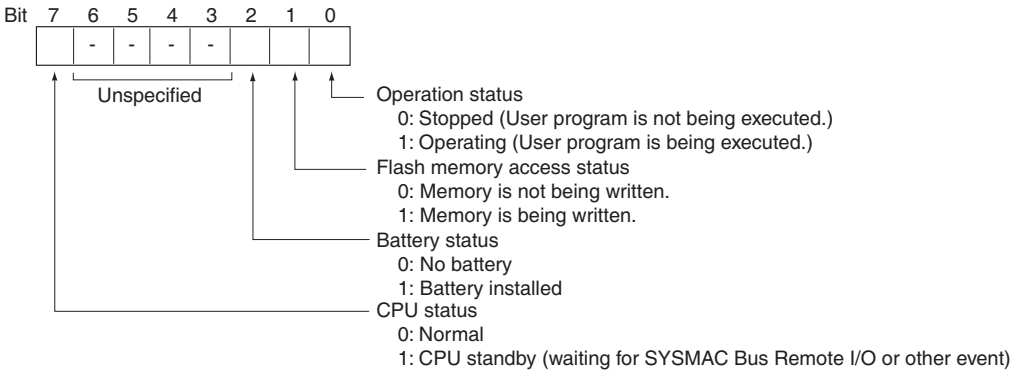
Instance ID (command): Always 00 Hex.

Read data (response): The read data is given in the following table. The data is returned after the service code in the order shown in the table (high to low).

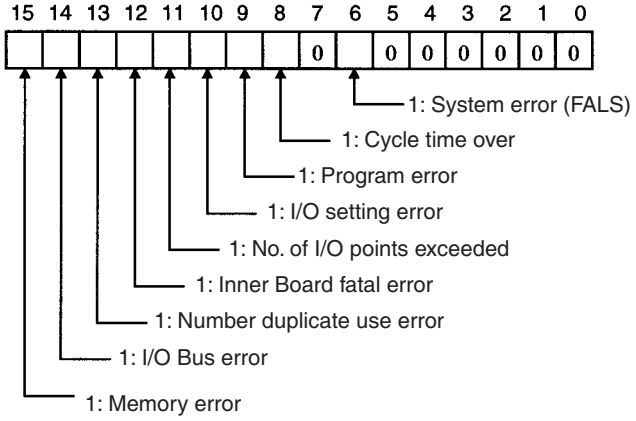
Operation Status
RUN mode
Fatal error information (L)
Fatal error information (H)
Non-fatal error information (L)
Non-fatal error information (H)
Message exists/does not exist (L)
Message exists/does not exist (H)
Error code (L)
Error code (H)
Error message (16 bytes)

- **Operation status:** Returns the operation status of the CPU Unit in 1-byte (2-digit) hexadecimal.

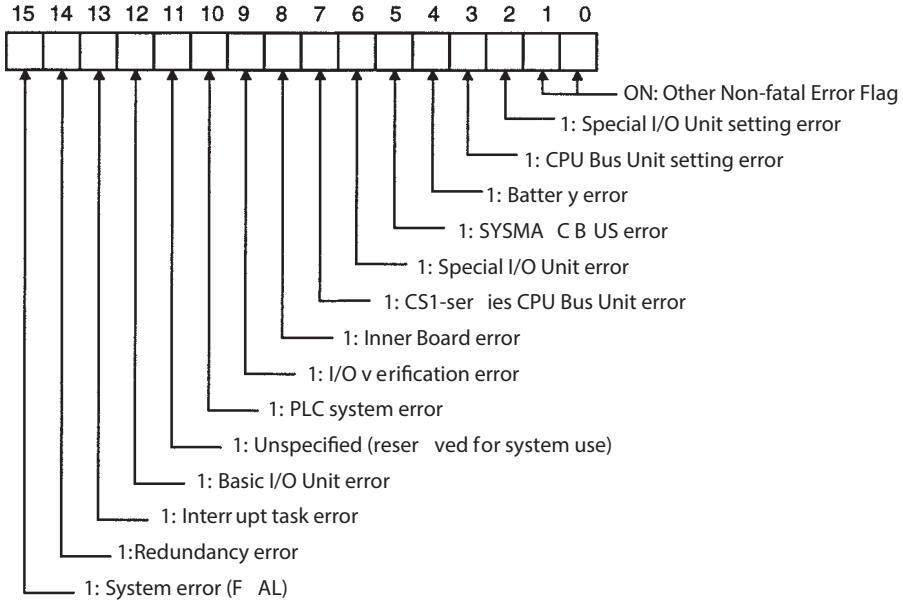
The values of bits 3 to 6 are not fixed. Always mask them when addressing the status data.



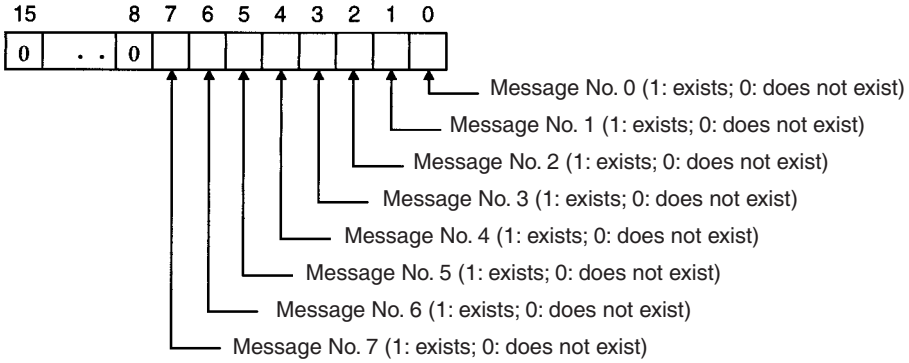
- **Operating mode:** Returns the operating mode of the CPU Unit in 1-byte (2-digit) hexadecimal.
  0001 Hex: PROGRAM mode; 0002 Hex: MONITOR mode;
  0004 Hex: RUN mode
- **Fatal error information:** Returns the fatal error information for the CPU Unit in 2 bytes (low to high).



- **Non-fatal error information:** Returns the non-fatal error information for the CPU Unit in 2 bytes (low to high).



- **Message Exists/Does Not Exist:** When the MSG instruction is executed by the CPU Unit, the bit corresponding to the message number will turn ON and be returned in 2 bytes (from low to high bytes).



- **Error Code**: The highest priority error code of the errors existing when the command is executed will be returned in 2-byte decimal (from low to high bytes). If there are no errors, the error code will be 0000.

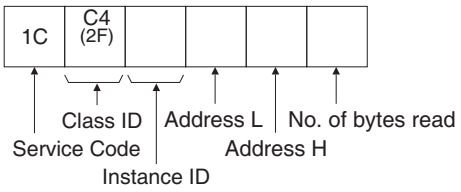
  Note For information on the severity of error codes, refer to the *CS1 Series CPU Unit Operation Manual* (W339) or the *CJ Series CPU Unit Operation Manual* (W393).

- **Error Messages:** If the above error codes have occurred when FAL/FALS instructions are executed with registered messages, those messages are returned in 16-byte ASCII. If there are no registered messages or if the error codes have not occurred due to execution of FAL/FALS instructions, the code is returned in ASCII with 20 Hex (space) in 16 bytes.

Byte Data Read (Service Code: 1C Hex)

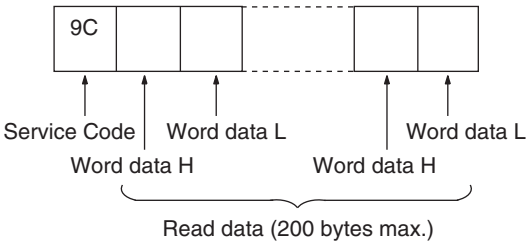
Byte Data Read reads any I/O memory area data in a CPU Unit. The read word data is in byte units. The response block data is returned in low-to-high byte order.

Command Block



Note A body format of either 8 bits or 16 bits is possible.

Response Block



Parameters

Service code (command, response): 1C Hex is specified for commands. For responses, the highest bit will turn ON and 9C Hex will be returned.

Class ID (command):
The class ID is C4 hex.

Note that the class ID is 2F hex for CS1W/CJ1W-EIP21 or CJ2H-CPU6□-EIP Unit version 1.0.

Instance ID (command): The memory area that will read the data is specified as shown in the following table.

Instance ID (Hex)	CPU Unit memory area for read	Word range
01	CIO	0000 to 6143
03	DM	D00000 to D32767
04	WR	W000 to W511
05	HR	H000 to H1535
08 to 20	EM, banks 0 to 18	En_00000 to En_32767 (n: 0 to 18)

Address L, Address H (command): The address of the first word from which to read the data is specified in hexadecimal as shown below.
Address L: The lower 2 digits when the first word address is given in 4-digit hexadecimal.
Address H: The higher 2 digits when the first word address is given in 4-digit hexadecimal.

No of Read Bytes (command): The number of bytes of read data is specified in 1-byte (2-digit) hexadecimal. The range is 01 to C8 Hex (1 to 200 decimal).

No. of bytes received (response): The number of bytes received from the destination node address (remote node) is returned in hexadecimal.

Destination node address (response): The node address of the CS/CJ-series EtherNet/IP Unit or built-in EtherNet/IP port that returned the response is returned in hexadecimal.

Read data (response): The specified area, word, and byte data is returned in order from word H (high byte: bits 8 to 15) to word L (low byte: bits 0 to 7). If an odd number is specified for the number of read bytes, the last 1 byte of data will be read to the high word.

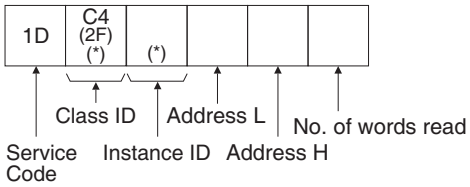
Important Points

The actual address L, address H, and number of read bytes that can be specified depends on the model of the CPU Unit, and the data area being read. Do not exceed the boundary of the data areas for the PLC you are using.

Word Data Read (Service Code: 1D Hex)

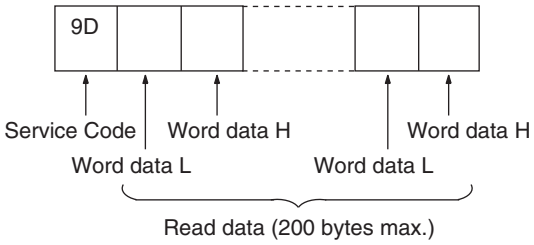
Word Data Read reads I/O memory area data in a CPU Unit. The read word data is in word units. The response block data is returned in low-to-high byte order.

Command Block



Note A body format of either 8 bits or 16 bits is possible.

Response Block



Parameters

Service code (command, response): ID Hex is specified for commands. For responses, the highest bit will turn ON and 9D Hex will be returned.

Class ID (command):
The class ID is C4 hex.

Note that the class ID is 2F hex for CS1W/CJ1W-EIP21 or CJ2H-CPU6□-EIP Unit version 1.0.

Instance ID (command): The type of memory area that will read the data is specified as shown in the following table.

Instance ID (Hex)	CPU Unit memory area for read	Word range
01	CIO	0000 to 6143
03	DM	D00000 to D32767
04	WR	W000 to W511
05	HR	H000 to H1535
08 to 20	EM, banks 0 to 18	En_00000 to En_32767 (n: 0 to 18)

Address L, Address H (command): The address of the first word to read the data from is specified in hexadecimal as shown below.
Address L: The lower 2 digits when the first word address is given in 4-digit hexadecimal.
Address H: The higher 2 digits when the first word address is given in 4-digit hexadecimal.

No of Read Words (command): The number of words of read data is specified in 1-byte (2-digit) hexadecimal. The range is 01 to 64 Hex (1 to 100 decimal).

Read data (response): The specified area, word, and byte data is returned in order from word L (low byte: bits 0 to 7) to word H (high byte: bits 8 to 15).

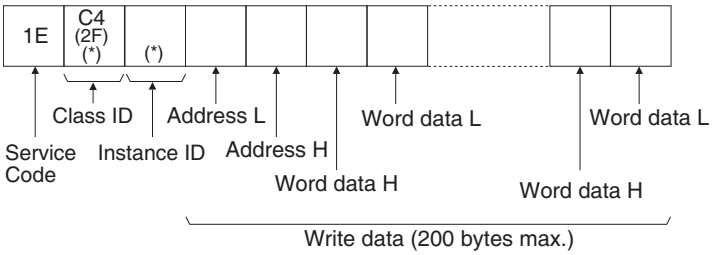
Important Points

The actual address L, address H, and number of write data bytes that can be specified depends on the model of the CPU Unit, and the data area being written. Do not exceed the boundary of the data areas for the PLC you are using.

Byte Data Write (Service Code: 1E Hex)

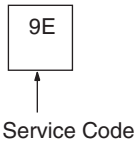
Byte Data Write writes data to an I/O memory area in a CPU Unit. The write word data is in byte units. The command block is specified in high-to-low byte order, as shown in the following diagram.

Command Block



Note A body format of either 8 bits or 16 bits is possible.

Response Block



Parameters

Service code (command, response): IE Hex is specified for commands. For responses, the highest bit will turn ON and 9E Hex will be returned.

Class ID (command):
The class ID is C4 hex.

Note that the class ID is 2F hex for CS1W/CJ1W-EIP21 or CJ2H-CPU6□-EIP Unit version 1.0.

Instance ID (command): The type of memory area to which the data will be written is specified as shown in the following table.

Instance ID (Hex)	CPU Unit memory area for write	Word range
01	CIO	0000 to 6143
03	DM	D00000 to D32767
04	WR	W000 to W511
05	HR	H000 to H1535
08 to 20	EM, banks 0 to 18	En_00000 to En_32767 (n: 0 to 18)

Address L, Address H (command): The address of the first word to which the data will be written is specified in hexadecimal as shown below.
Address L: The lower 2 digits when the first word address is displayed in 4-digit hexadecimal.
Address H: The higher 2 digits when the first word address is displayed in 4-digit hexadecimal.

Write data (response): The specified area and write data is returned in order from word H (higher byte: bits 8 to 15) to word L (lower byte: bits 0 to 7). For byte data write, specify an even number.

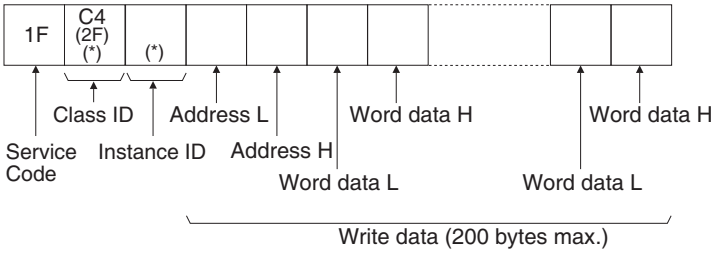
Important Points

The actual address L, address H, and number of write data bytes that can be specified depends on the model of the CPU Unit, and the data area being written. Do not exceed the boundary of the data areas for the PLC you are using.

Word Data Write (Service Code: 1F Hex)

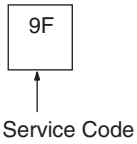
Word Data Write writes data to any I/O memory area in a CPU Unit. The write word data is in word units. The response block data is returned in low-to-high byte order.

Command Block



Note A body format of either 8 bits or 16 bits is possible.

Response Block



Parameters

Service code (command, response): IF Hex is specified for commands. For responses, the highest bit will turn ON and 9F Hex will be returned.

Class ID (command):
The class ID is C4 hex.

Note that the class ID is 2F hex for CS1W/CJ1W-EIP21 or CJ2H-CPU6□-EIP Unit version 1.0.

Instance ID (command): The memory area to which the data is written is specified as shown in the following table.

Instance ID (Hex)	CPU Unit memory area for write	Word range
01	CIO	0000 to 6143
03	DM	D00000 to D32767
04	WR	W000 to W511
05	HR	H000 to H1535
08 to 20	EM, banks 0 to 18	En_00000 to En_32767 (n: 0 to 18)

Address L, Address H (command): The address of the first word to which the data is written is specified in hexadecimal as shown below.
Address L: The lower 2 digits when the first word address is displayed in 4-digit hexadecimal.
Address H: The higher 2 digits when the first word address is displayed in 4-digit hexadecimal.

Write data (response): The specified area and write data is returned in order from word L (lower byte: bits 0 to 7) to word H (higher byte: bits 8 to 15).

Important Points

The actual address L, address H, and number of write data bytes that can be specified depends on the model of the CPU Unit, and the data area being written. Do not exceed the boundary of the data areas for the PLC you are using.

9-2-2 Connection Configuration Object

List of Connection Configuration Object Services

Connection Configuration Objects provide the following services.

Service	Service Code	Class ID	Instance ID	Request Data	Description
Open Connections by Node	32 hex (*)	F3 hex	00 hex	• Target node ID • Connection Establish Error Open Continuation Disable Flag • Connection Establish Timeout Time per Connection	Opens all connections to the specified target node.
Close Connections by Node	33 hex			• Target node ID • Connection Close Timeout Time per Connection	Closes all connections to the specified target node.

The command format and response format to send the above services by sending the CIP UCMM MESSAGE SEND command (28 10) with CMND instruction are described next. Only the following formats are provided.

- The command last hop data of the command format
- The service response data of the response format

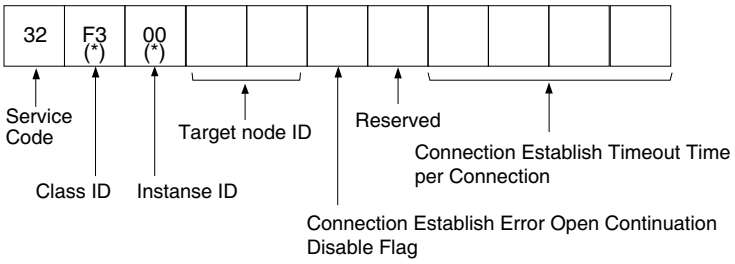
For the format of the CIP UCMM MESSAGE SEND command (28 10), refer to *9-1 Sending Explicit Messages*.

In the format descriptions, each box represents one byte.

Open Connections by Node (Service Code: 32 Hex)

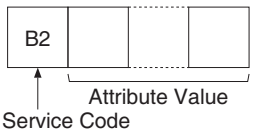
This service opens all connections to the specified target node.

Command Block



Note A body format of either 8 bits or 16 bits is possible.

Response Block



Parameters

Service code (command, response):
A service code of 32 hex is specified for commands.
For responses, the highest bit will be ON and B2 Hex will be returned.

Class ID (command):
Always F3 Hex.

Instance ID (command):
Always 00 Hex.

Request data (command):

Name	Size	Range of values	Description
Target Node ID	2 bytes	0 to FF hex	Set the ID of the target node for which to open the connections.
Connection Establish Error Open Continuation Disable Flag	1 byte	0 or 1	Specify whether to continue connection open processing until a connection is successfully established after establishing a connection fails. 0: OFF (continue) 1: ON (do not continue)
Reserved	1 byte	00 hex	Reserved.
Connection Establish Timeout Time per Connection	4 bytes	0 to FFFFFFFF hex*1	Specify the connection open timeout time per connection. The unit is milliseconds. Default: 5,000 If you set more than one connection, do not exceed the following range. Number of connections × The applicable set value ≤ 5,000

*1 The default is used in operation if the value is not between 20 and 5,000.

Response data (response):

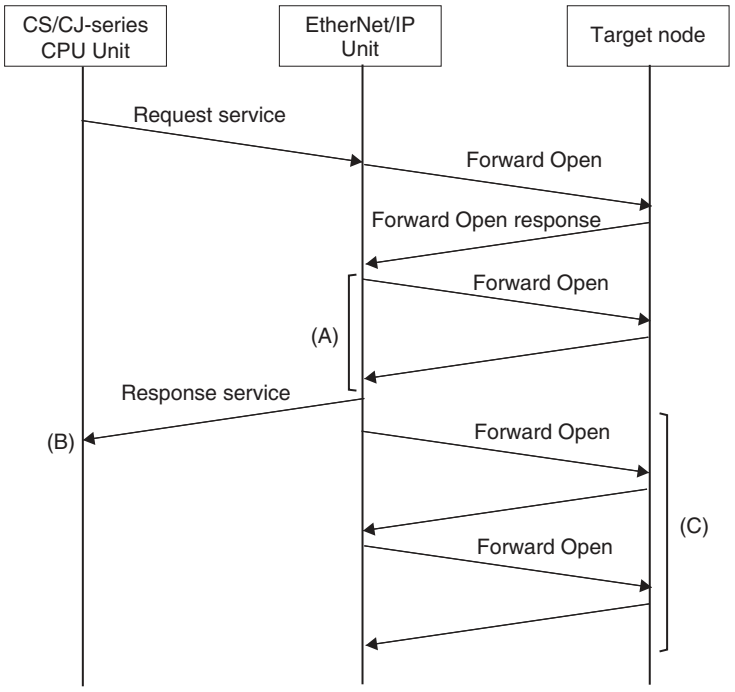
Name	Size	Value	Description
Connection Open status	2 bytes	0 hex	All connections with the target node were established normally.
		1 hex	One or more of the connections to the target node could not be established. However, the connections may still be established by re-execution*1 of connection open processing.
		2 hex	One or more of the connections to the target node could not be established. Error processing*2 is required to establish all of the connections.

*1 If the Connection Establish Error Open Continuation Disable Flag is set to OFF, connection open processing is performed again automatically. If this flag is ON, you must execute this service again.

*2 For details on error processing, refer to *14-3 Protocol Overview*.

Process Flow

The process flow of the Open Connections by Node service is given below.



(A) If more than one connection is set for the specified target node, connection open processing with Forward_Open is repeated for each connection.

(B) The response service is returned at the following times.

- When responses have been received for Forward_Open for all connections
- When a response is not received for a Forward_Open within the time set for the Connection Open Timeout Time per Connection

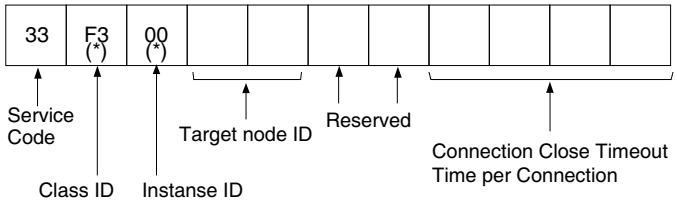
(C) If opening a connection for (A) fails and the Connection Establish Error Open Continuation Disable Flag is OFF, connection open processing is

repeated until the connection is established. If the flag is ON, nothing is done.

Close Connections by Node (Service Code: 33 Hex)

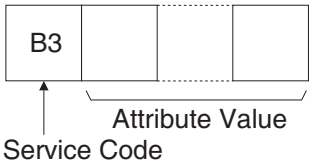
This service closes all connections to the specified target node.

Command Block



Note A body format of either 8 bits or 16 bits is possible.

Response Block



Parameters

Service code (command, response):
A service code of 33 hex is specified for commands.
For responses, the highest bit will be ON and B3 Hex will be returned.

Class ID (command):
Always F3 Hex.

Instance ID (command):
Always 00 Hex.

Request data (command):

Name	Size	Range of values	Description
Target Node ID	2 bytes	0 to FF hex	Set the ID of the target node for which to open the connections.
Reserved	1 byte	00 hex	Reserved.
Reserved	1 byte	00 hex	Reserved.
Connection Close Timeout Time per Connection	4 bytes	0 to FFFFFFFF hex*1	Specify the connection close time-out time per connection. The unit is milliseconds. If you set more than one connection, do not exceed the following range. Number of connections × The applicable set value ≤ 5,000

*1 The default value of 5,000 is used in operation if the value is not between 20 and 5,000.

SECTION 10
Communications Performance and Communications Load

This section describes the communications performance in an EtherNet/IP network, and shows how to estimate the I/O response times and transmission delays.

10-1 Communications System 306
10-1-1 Tag Data Link Communications Method 306
10-1-2 Calculating the Number of Connections 309
10-1-3 Network Transmission Delay Time 310
10-2 Adjusting the Communications Load 313
10-2-1 Checking Bandwidth Usage for Tag Data Links 314
10-2-2 Tag Data Link Bandwidth Usage and RPI 315
10-2-3 Adjusting Device Bandwidth Usage 316
10-2-4 Changing the RPI 317
10-2-5 RPI Setting Examples 321
10-3 I/O Response Time in Tag Data Links 328
10-3-1 Timing of Data Transmissions 328
10-3-2 EtherNet/IP Unit or Built-in Port Data Processing Time 328
10-3-3 Effect on the CPU Unit's Cycle Time 330
10-3-4 Tag Data Link I/O Response Time Calculation Example 331
10-4 Message Service Transmission Delay 337
10-4-1 Maximum Transmission Delays (Excluding Delays in the Network) 337

10-1 Communications System

10-1-1 Tag Data Link Communications Method

Packet Interval (RPI) Settings

In EtherNet/IP tag data links, the data transmission period is set for each connection as the packet interval (RPI). The target device will send data (i.e., output tags) once each packet interval (RPI), regardless of the number of nodes. Also, the heartbeat frame is sent from the originator to the target for each connection. The target uses the heartbeat to check to see if errors have occurred in the connection with the originator. The data transmission period of the heartbeat frame depends on the packet interval (RPI) settings.

■ Heartbeat Frame Transmission Period

- Packet interval < 100 ms
  The heartbeat frame transmission period is 100 ms.
- Packet interval ≥ 100 ms
  The heartbeat frame transmission period is the same as the RPI.

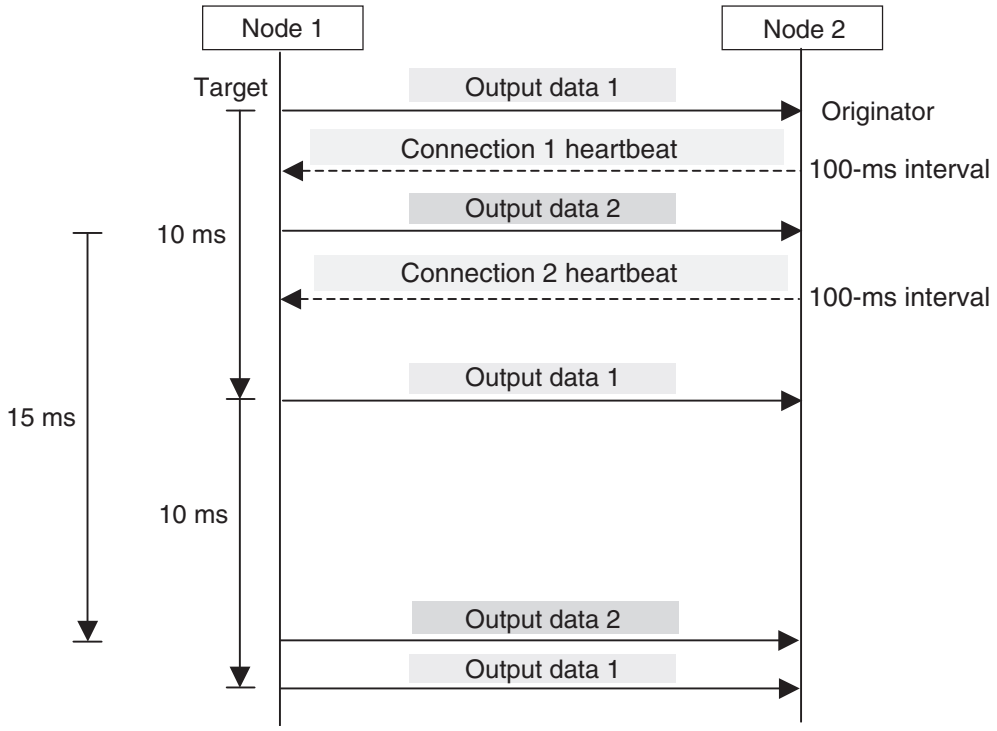
Example

In this example, 2 tag data link connections are set for node 2 (the originator) and node 1 (the target).

The packet interval (RPI) for output data 1 is set to 10 ms.

The packet interval (RPI) for output data 2 is set to 15 ms.

In this case, output data 1 is sent from node 1 to node 2 every 10 ms, and output data 2 is sent from node 1 to node 2 every 15 ms, as shown in the following diagram. Also, data is sent from node 2 (the originator) to node 1 (the target) with a heartbeat of 100 ms for connection 1 and a heartbeat of 100 ms for connection 2.



Requested Packet Interval (RPI) and Bandwidth Usage

The weighted number of packets transferred each second is called the bandwidth usage. "N" in this section represents a weighing factor according to the packet data size.

The bandwidth usage is calculated from the RPI, heartbeat, and the factor of N as follows for each connection:

Bandwidth used in a connection
= (1,000 ÷ RPI (ms) × N) + (1,000 ÷ Heartbeat transmission period (ms))

N = Tag data link's allowable bandwidth ÷ (Tag data link's allowable bandwidth + Coefficient × Data size per connection)

Model	EtherNet/IP Unit version	Allowed tag data link communications bandwidth	Coefficient	N
CS1W/CJ1W-EIP21S CJ3M-CPU3□	1.0 or later	12,000	-4.155	1 to 2
CS1W/CJ1W-EIP21	3.0 or later	12,000	-4.155	1 to 2
CJ2B-EIP21 (CJ2HCPU6□-EIP)	2.1 or earlier	6,000	0	1
CJ2M-EIP21 (CJ2MCPU3□)	2.0 or later	3,000	0	1

Use the following equation to calculate the total bandwidth used by each Unit (refers to as an EtherNet/IP Unit in the following examples).

Total bandwidth used by Unit = Total bandwidth used by originator connections
+ Total bandwidth used by target connections

Note Connections set as target connections must also be added to the total bandwidth used by target connections.

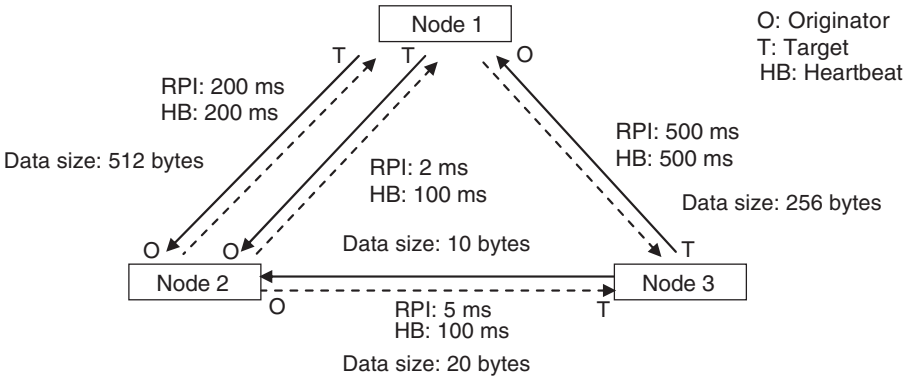
Make the connection settings so that the Unit's total bandwidth used does not exceed its upper value.

Example

Node 1 has both originator and target connections, and sends 512 bytes of data at an RPI of 200 ms and 10 bytes of data at an RPI of 2 ms, and receives 256 bytes of data at an RPI of 500 ms.

Node 2 has originator connections only, and receives 512 bytes of data at an RPI of 200 ms, 10 bytes of data at an RPI of 2 ms, and 20 bytes of data at an RPI of 5 ms.

Node 3 has target connections only, and sends 20 bytes of data at an RPI of 5 ms, and 256 bytes of data at an RPI of 500 ms.



Each node's total bandwidth used is calculated as follows:

■ **Communication using Units with unit version 2.1 or earlier (See note 1.)**

- Total bandwidth used for node 1 Unit
  = 1,000 / 200 ms × 1 + 1,000 / 2 ms × 1 + 1,000 / 500 ms × 1 (for data)
  + 1,000 / 200 ms + 1,000 / 100 ms + 1,000 / 500 ms (for heartbeat)
  = 524
- Total bandwidth used for node 2 Unit
  = 1,000 / 200 ms × 1 + 1,000 / 2 ms × 1 + 1,000 / 5 ms × 1 (for data)
  + 1,000 / 200 ms + 1,000 / 100 ms + 1,000 / 100 ms (for heartbeat)
  = 730
- Total bandwidth used for node 3 Unit
  = 1,000 / 5 ms × 1 + 1,000 / 500 ms × 1 (for data)
  + 1,000 / 100 ms + 1,000 / 500 ms (for heartbeat)
  = 214

All of the Units are within the upper value of the total bandwidth used of 6,000 pps, so they can transfer data.

Note (1) This is applicable to EtherNet/IP Units or built-in EtherNet/IP ports with unit version 2.1 or earlier excluding CS1W/CJ1W-EIP21S.

■ **Communication using Units with unit version 3.0 (See note 1.)**

Data size (bytes)	Factor N
10	12,000 / (12,000 - 4.155 × 10) = 1.003
20	12,000 / (12,000 - 4.155 × 20) = 1.007
256	12,000 / (12,000 - 4.155 × 256) = 1.097
512	12,000 / (12,000 - 4.155 × 512) = 1.215

- Total bandwidth used for node 1 Unit
  = 1,000 / 200 ms × 1.215 + 1,000 / 2 ms × 1.003 + 1,000 / 500 ms × 1.097 (for data)
  + 1,000 / 200 ms + 1,000 / 100 ms + 1,000 / 500 ms (for heartbeat)
  = 527
- Total bandwidth used for node 2 Unit
  = 1,000 / 200 ms × 1.215 + 1,000 / 2 ms × 1.003 + 1,000 / 5 ms × 1.007 (for data)
  + 1,000 / 200 ms + 1,000 / 100 ms + 1,000 / 100 ms (for heartbeat)
  = 734
- Total bandwidth used for node 3 Unit
  = 1,000 / 5 ms × 1.007 + 1,000 / 500 ms × 1.097 (for data)
  + 1,000 / 100 ms + 1,000 / 500 ms (for heartbeat)
  = 216

All of the Units are within the upper value of the total bandwidth used of 12,000 pps, so they can transfer data.

Note (1) This is applicable to EtherNet/IP Units or built-in EtherNet/IP ports with unit version 3.0 excluding CS1W/CJ1W-EIP21S, and CS1W/CJ1W-EIP21S with unit version 1.0.

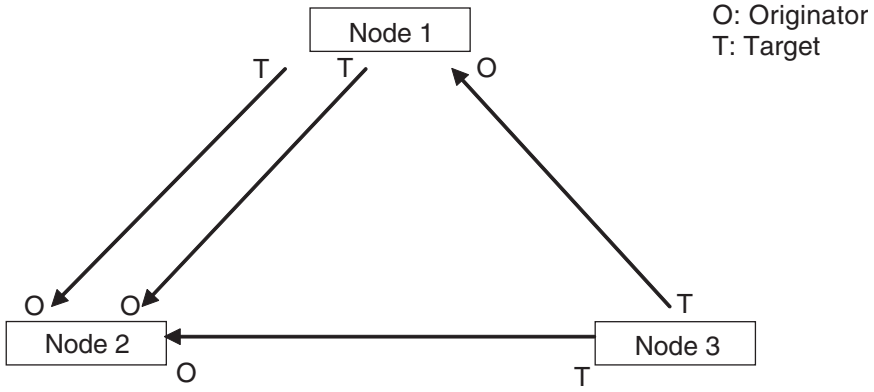
10-1-2 Calculating the Number of Connections

The maximum number of connections for the Unit is 256 (32 for the CJ2M-EIP21).

The number of connections must be set to 256 or less (32 or less for the CJ2M-EIP21) combining both connections that the Unit opens as the originator and connections that are opened from an originator with the Unit as the target.

Example

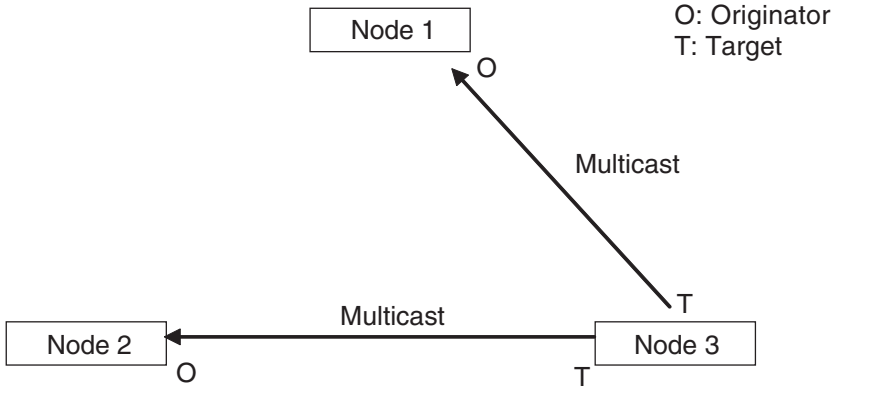
Node 1 opens two connections as the target with node 2 and one connection as the originator with node 3. Therefore, the total is three connections. Node 2 opens two connections as the originator with node 1 and one connection as the target with node 3. Therefore, the total is three connections. Node 3 opens one connection as the target with node 1 and one connection as the target with node 2. Therefore, the total is two connections. In either case, the connections can be opened because the maximum number of connections for the Unit is less than 256 (32 for the CJ2M-EIP21).



Also, if multicast is set, one packet will be sent, but the number of connections will be consumed.

Example

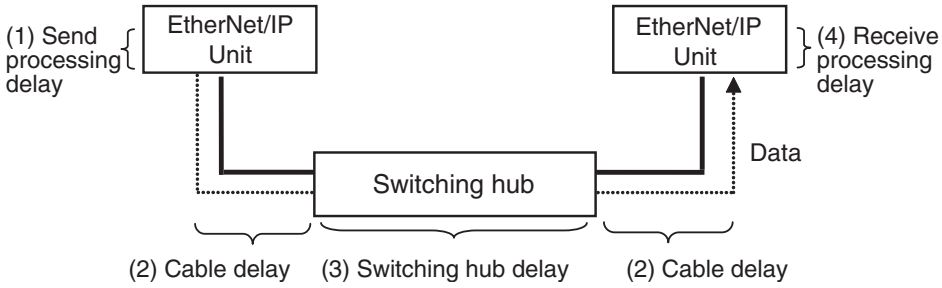
Node 3 sends one multicast packet to node 1 and node 2. At that time, node 3 opens one connection as the target with node 1 and one connection as the target with node 2 for a total of two connections. Caution is required because the number of connections consumed is the same as for unicast connections even when multicast connections are set.



10-1-3 Network Transmission Delay Time

In an EtherNet/IP network, the tag data link packets are sent once each packet interval (RPI), but several delays occur between the transmission of packets from each node and the arrival of the packets at the destination nodes. The following diagram shows the 4 major delay sources.

Total network transmission delay = (1) Send processing delay + (2) Cable delays + (3) Switching hub delay + (4) Receive processing delay

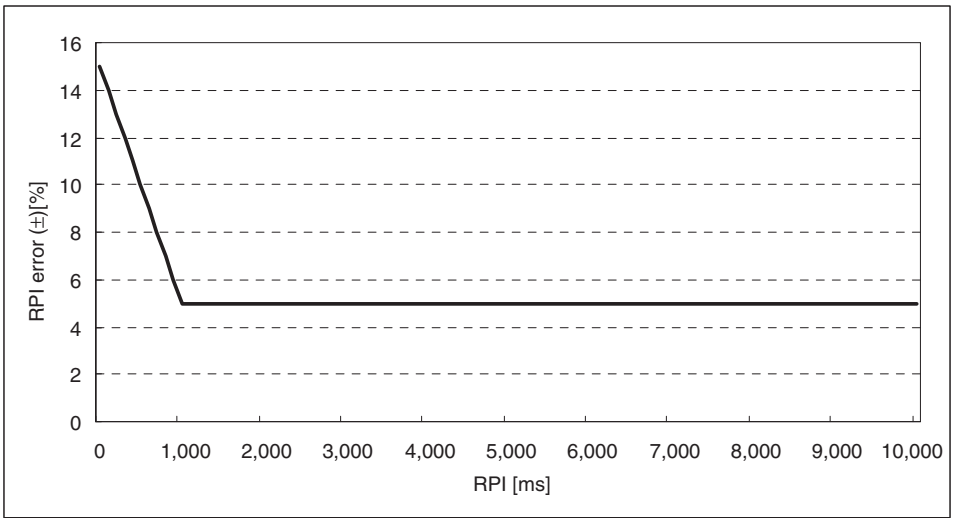


The lengths of these delays depend on many factors, such as the tag data link connection settings (number of connections and data sizes), number of nodes, the switching hub being used, and cable lengths. Each delay is described in detail below.

1. Send Processing Delay

The send processing delay is the delay that occurs within the EtherNet/IP Unit or built-in EtherNet/IP port when data packets are sent once each packet interval. This delay varies with the RPI error shown in the following graph, so the send processing time is the maximum value for each RPI.

Packet interval (RPI)	RPI error (±) (%)
0.5 to 1,000 ms	15 – (RPI (ms) ÷ 100)
1,000 ms to 10,000 ms	5% of the RPI



2. Cable Delay

The cable delay is the time required for the data signal to pass through the cable and reach the destination. When an STP (shielded twisted-pair) cable of category 5, 5e, or higher is being used, the maximum cable delay is 545 ns/100 m. The cable delay represents a very small percentage of the total tag data link delay.

3. Switching Hub Delay

The switching hub delay is the delay time between the arrival of the packet at the switching hub and the output of the packet from the hub's transmission port. This delay depends on the total number of connections used for reception and data sizes used in the tag data links. In addition, this delay depends on the switching hub maker and model, but the delay can be approximated with the following table. (For a precise estimate, contact the switching hub manufacturer.)

The following values are the delays when cascade connections are not being used. If cascade connections are used, more nodes can be connected, but the switching hub delays will increase.

Words per connection	Number of connections used for reception				
	16	32	64	128	256
2 words	0.2 ms	0.3 ms	0.5 ms	1.0 ms	1.9 ms
200 words	0.7 ms	1.3 ms	2.5 ms	5.0 ms	10.0 ms
400 words	1.2 ms	2.3 ms	4.6 ms	9.1 ms	18.2 ms
600 words	1.7 ms	3.3 ms	6.6 ms	13.2 ms	26.4 ms
722 words	2.0 ms	4.0 ms	7.9 ms	15.7 ms	31.4 ms

4. Receive Processing Delay

The receive processing delay is the delay that occurs within the EtherNet/IP Unit or built-in EtherNet/IP port from the reception of the data packet at the Unit until the completion of reception processing in the Unit. This delay depends on the size of the connections used in the tag data links and the number of connections. In practice, the delay depends on the number of connections used in tag data links with less than 200 words. If the number of connections is "n", the maximum delay can be calculated with the following equation.

Maximum reception processing delay = 1 + (n × 0.043) ms

The size of the connections may cause a delay when the data sizes are smaller and a large number of packets may be received in a fixed interval, because the data may wait for receive processing.

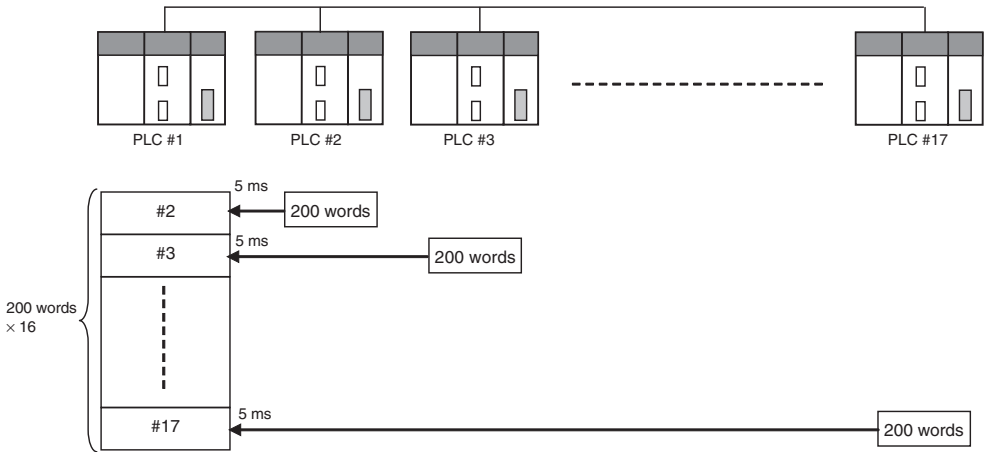
Example Calculation of the Tag Data Link Delay

This example shows how to calculate the tag data link delay when the following tag data link connection settings have been made.

In this case, 17 EtherNet/IP Units or built-in EtherNet/IP ports are being used, and one Unit is receiving 200 words of data from each of the other Units at a packet interval (RPI) of 5 ms. Thus, 16 tag data link connections are used. The length of the cables between the Units is 50 m for all connections.

Send processing delay = 5 ms × (15 − 5/100)% = 0.7475 ms
Cable delay = 545 ns × 50 m/100 = 272.5 ns
Switching hub delay = 0.7 ms
Receive processing delay = 1 + (16 × 0.043) ms = 1.688 ms

Tag data link delay = 0.7475 ms + 0.0002725 ms + 0.7 ms + 1.688 ms
≈ 3.14 ms


PLC #1
PLC #2
PLC #3
PLC #17
5 ms
#2
200 words
5 ms
#3
200 words
200 words
× 16
5 ms
#17
200 words

10-2 Adjusting the Communications Load

In an Ethernet network using a switching hub, the network bandwidth is not shared by all of the nodes; independent transmission paths are established between individual nodes through the switching hub.

A dedicated communications buffer is established in the switching hub for communications between the nodes and full-duplex communications (simultaneous transmission and reception) are performed asynchronously with other transmission paths. The communications load in other transmission paths does not affect communications, so packet collisions do not occur and stable, high-speed communications can be performed.

The switching hub functions shown in the following table determine the performance of tag data links.

Item	Description
Buffer capacity	This is the amount of data that can be buffered when packets accumulate at the switching hub.
Multicast filtering	This function transfers multicast packets to specific nodes only.
QoS function	This function performs priority control on packet transfers.

The following table shows the tag data link settings that can be made for individual EtherNet/IP Units as well as the setting ranges.

Item	Contents	Settings
Network bandwidth	Physical Ethernet baud rate	100 Mbps or 10 Mbps
Allowed tag data link communications bandwidth	Maximum number of tag data link packets that can be processed in 1 second (pps: packets per second)	12,000 pps (CJ2M-EIP21: 3,000 pps) (See note 1.)
Connection resources	Number of connections that can be established	256 max. (Other CPU Units: 32 max.)
Packet interval (RPI: Requested Packet Interval)	Refresh cycle for tag data	0.5 to 10,000 ms (CJ2M-EIP21: 1 to 1,000 ms) (in 0.5 ms units)

Note (1) For EtherNet/IP Units or built-in EtherNet/IP ports with unit version 2.1 or earlier excluding CS1W/CJ1W-EIP21S, this is 6,000 pps.

When the tag data link settings exceed the capabilities of the switching hub being used, increase the RPI value. Particularly when using a switching hub that does not support multicast filtering, the settings must be made considering that multicast packets will be sent even to nodes without connection settings.

In addition, if the required tag data link performance cannot be achieved with the switching hub's capabilities, reevaluate the overall network configuration and correct it by taking steps such as selecting a different switching hub or splitting the network.

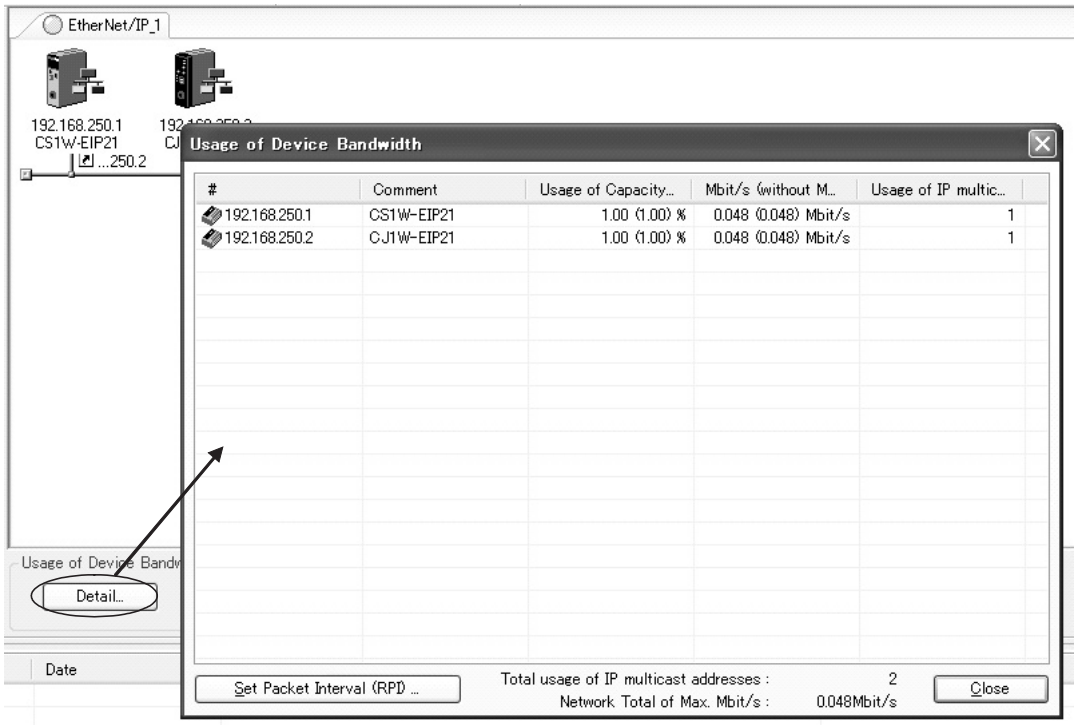
The following sections show how to check the device bandwidth being used by the tag data links in the designed network, and how to set the appropriate values.

Note If the Network Configurator is used to set the connection type in the connection settings to a multicast connection, multicast packets will be used. If the connection type is set to a point-to-point connection, multicast packets will not be used.

10-2-1 Checking Bandwidth Usage for Tag Data Links

The Network Configurator can display the bandwidth actually used for tag data links at each EtherNet/IP Unit, based on the connections set in the network configuration.

The device bandwidth used by tag data links can be checked by clicking the **Detail** Button in the Usage of Device Bandwidth Area at the bottom of the Network Configuration Window.



Item	Description
#	The IP address of the device.
Comment	A description of the device. The comment is displayed below the device icon. The model number of the device is displayed by default.
Usage of Capacity	The percentage of the allowable communications bandwidth used for tag data links for the device is displayed. Bandwidth used ÷ Allowable tag data link bandwidth The values outside parentheses are for when multicast filtering is used. The values inside parentheses are for when multicast filtering is not used.
Mbit/s	The bandwidth used for communications by the device of the 100-Mbps network bandwidth is shown. The values outside parentheses are for when multicast filtering is used. The values inside parentheses are for when multicast filtering is not used.
Usage of IP Multicast Addresses	The number of multicast IP addresses actually used for communications by the device is shown.

Item	Description
Total usage of IP multicast addresses	The number of multicast IP addresses used in the entire network is shown. This value is used to estimate the number of multicast filters for switching.
Network Total of Max. Mbit/s	The total network bandwidth used for tag data link communications in the entire network is shown. Tag data links will not operate normally if 100 Mbps is exceeded for the network bandwidth.

Checking the Usage of Capacity and Network Bandwidth for Tag Data Links

The percentage of the allowable communications bandwidth for tag data links for each EtherNet/IP Unit is displayed as the *Usage of Capacity* and the bandwidth used for tag data link communications in the entire network is displayed as the *Mbit/s*.

The usage of capacity and used network bandwidth that are displayed in parentheses are for a switching hub that does not use multicast filtering. In this case, multicast packets will be sent to even the nodes without connection settings, so the displayed values will include these packets as well.

These values can be adjusted according to instructions in *10-2-4 Changing the RPI*.

Checking the Total Number of Multicast IP Addresses in the Network

When using a switching hub that provides multicast filtering, there must be enough multicast filters for the network being used. The number of multicast IP address used in the entire network that is displayed by the Network Configurator as the *Network Total of Max. Mbit/s* is based on connection settings.

Make sure that the number of multicast IP addresses used in the entire network does not exceed the number of multicast filters supported by the switching hub. If necessary, change to a switching hub with enough multicast filters, or adjust the usage of capacity and network bandwidth for tag data links (*Mbit/s*) values given for a switching hub without multicast filtering (i.e., the values in parentheses). Adjust these values according to instructions in *10-2-4 Changing the RPI*.

Checking the Total Maximum Network Bandwidth

The Network Configurator displays the total maximum bandwidth that can be used for the entire network as the *Network Total of Max. Mbit/s*. This value indicates the maximum bandwidth that can be used on the transmission paths when switching hubs are cascaded. If the value exceeds the bandwidth of a cascade connection in the actual network, the maximum bandwidth for part of the communications path may be exceeded, depending on how the network is wired.

If this occurs, either calculate the bandwidth usage for each communications path and be sure that the maximum bandwidth is not exceeded for any cascade connection, or adjust the bandwidth for all cascade connections so that the total maximum network bandwidth is not exceeded. Adjust the bandwidth according to instructions in *10-2-4 Changing the RPI*.

10-2-2 Tag Data Link Bandwidth Usage and RPI

The usage of capacity can be adjusted using the RPI setting. If the RPI is made shorter, the usage of capacity will increase. If the RPI is made longer, the usage of capacity will decrease.

The RPI can be set in any one of the following ways.

- Setting the same interval for all connections
- Setting a particular device's connection
- Setting a particular connection

When the same RPI is set for all connections, the usage of capacity will basically increase proportionally as the RPI is made shorter.

Example:
If the RPI is set to 50 ms for all connections and the usage of capacity is 40%, the usage of capacity may increase to 80% when the RPI is reduced to 25 ms for all connections.

Note Performing message communications or other network operations from the Network Configurator (such as monitoring or other operations that place a load on the network) or from the user application when the tag data link bandwidth usage of capacity is between 80% and 100% can create an excessive load on the network and result in timeouts. If timeouts occur, increase one or all of the RPI settings or reduce the usage of capacity.

10-2-3 Adjusting Device Bandwidth Usage

Switching Hubs without Multicast Filtering (100-Mbps Hubs)

- Is the network bandwidth without multicast filtering usage under 100 Mbps for each node? (This appears as “Mbit/s” in the dialog box shown on page 314.)
  → If any node exceeds 100 Mbps, change the connections settings, such as the RPI.
- Is the usage of capacity without multicast filtering under 100% for each node? (This appears as “Usage of Capacity” in the dialog box shown on page 314.)
  → If any node exceeds 100%, change the connections settings, such as the RPI.
- Is the total network bandwidth usage under 100 Mbps? (This appears as “Network Total of Max. Mbit/s” in the dialog box shown on page 314.)
  → If the total bandwidth usage exceeds 100 Mbps, the bandwidth of part of the transmission path (e.g., a switching hub or media converter) had been exceeded as the result of how the network was wired (e.g., switch hub or cascade connection), causing a tag data link to operate abnormally. Check the bandwidth of the transmission path for all cascade connections. If the bandwidth is exceeded, rewire the network or increase the bandwidth between switching hubs (e.g., to 1 Gbps). If these countermeasures are not possible, change the connection settings, e.g., the RPI settings, and adjust the bandwidth for all cascade connections until the total network bandwidth is not exceeded.

Switching Hubs with Multicast Filtering (100-Mbps Hubs)

- Is the network bandwidth usage under 100 Mbps for each node?
  → If any node exceeds 100 Mbps, change the connections settings, such as the RPI.
- Is the usage of capacity under 100% for each node?
  → If any node exceeds 100%, change the connections settings, such as the RPI.
- Is the total network bandwidth usage under 100 Mbps? (This appears as “Network Total of Max. Mbit/s” in the dialog box shown on page 314.)
  → If the total bandwidth usage exceeds 100 Mbps, the bandwidth of part of the transmission path (e.g., a switching hub or media converter) had been exceeded as the result of how the network was wired (e.g., switch hub or cascade connection), causing a tag data link to operate abnormally. Check the bandwidth of the transmission path for all cascade connections. If the bandwidth is exceeded, rewire the network or increase the bandwidth between switching hubs (e.g., to 1 Gbps). If these countermeasures are not possible, change the connection settings, e.g., the RPI settings, and adjust the bandwidth for all cascade connections until the total network bandwidth is not exceeded.

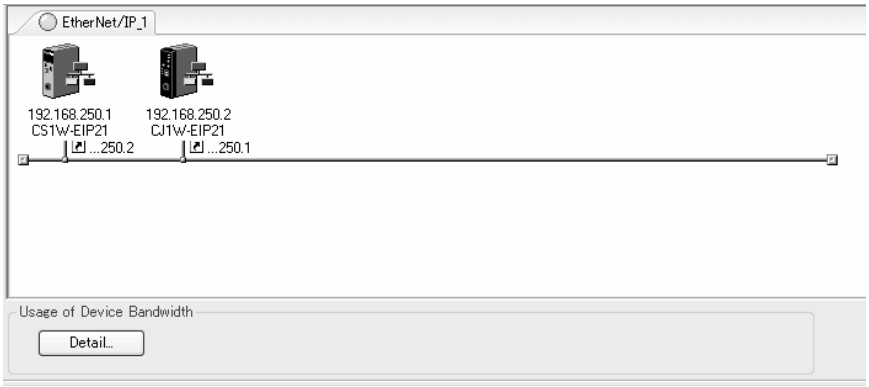
- Is the network bandwidth usage without multicast filtering under 100 Mbps for each node or the usage of capacity without multicast filtering under 100% for each node? (These appear as “Mbit/s” and “Usage of Capacity” in the dialog box shown on page 314.)
  → If the total bandwidth usage exceeds 100 Mbps, the bandwidth of part of the transmission path (e.g., a switching hub or media converter) had been exceeded as the result of how the network was wired (e.g., switch hub or cascade connection), causing a tag data link to operate abnormally. Check the bandwidth of the transmission path for all cascade connections. If the bandwidth is exceeded, rewire the network or increase the bandwidth between switching hubs (e.g., to 1 Gbps). If these countermeasures are not possible, change the connection settings, e.g., the RPI settings, and adjust the bandwidth for all cascade connections until the total network bandwidth is not exceeded.

10-2-4 Changing the RPI

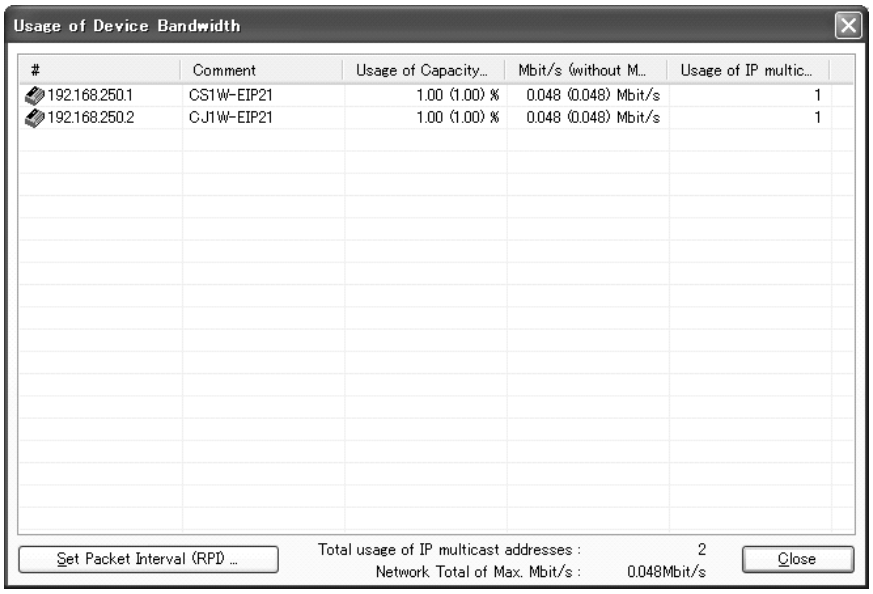
You can check the usage of capacity offline without multicast filtering against the tag data link's allowable bandwidth by following the procedures in *10-2-1 Checking Bandwidth Usage for Tag Data Links*. The usage of capacity without multicast filtering can be adjusted against the tag data link's allowable bandwidth by changing the packet interval (RPI). If the required communications performance cannot be achieved by changing the settings, reevaluate the network starting with the network configuration.

1,2,3... 1. Make the required settings in the Network Configurator’s Network Configuration Window.

2. Click the **Detail** Button in the Usage of Device Bandwidth Area at the bottom of the Network Configuration Window.



The Usage of Device Bandwidth Dialog Box will be displayed.



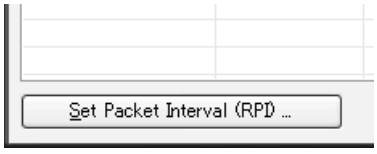
The *Usage of Capacity* column will show the percentage of the allowed tag data link bandwidth being used, and the *Mbit/s* column will show the network bandwidth being used.

3. The usage of capacity can be adjusted by changing the associated devices' RPI settings.
   The RPI settings can be changed with the following three methods.

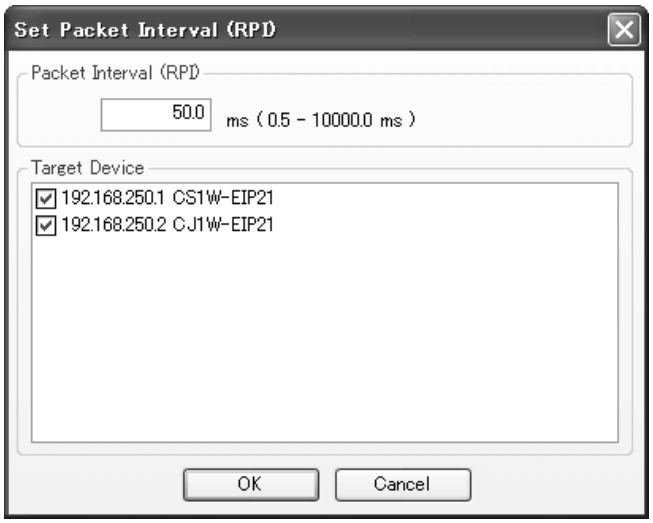
   Method 1: Same Packet Interval Set for all Connections

   The usage of capacity can be adjusted by changing the RPI for all of the connections at the same time.

   a. Click the **Set Packet Interval (RPI)** Button at the bottom of the Usage of Device Bandwidth Dialog Box.



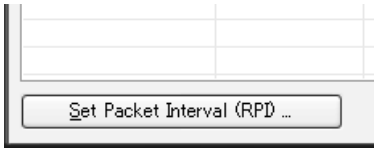
   b. The Set Packet Interval (RPI) Dialog Box will be displayed. Input a new RPI value, and click the **OK** Button.



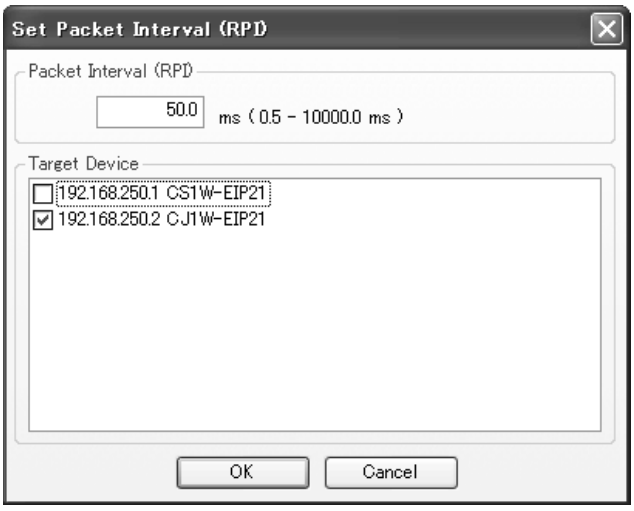
Method 2: Changing a Particular Device's RPI Setting

The usage of capacity can be adjusted for only a particular device by changing the packet intervals (RPI) for all of the device's connections together. In this case, the usage of capacity will also change for the devices that are the target devices of the connection which was adjusted.

a. Click the **Set Packet Interval (RPI)** Button at the bottom of the Usage of Device Bandwidth Dialog Box.



b. The Set Packet Interval (RPI) Dialog Box will be displayed. In the *Target Device* Area, deselect the target devices that are not being adjusted by removing the check marks.



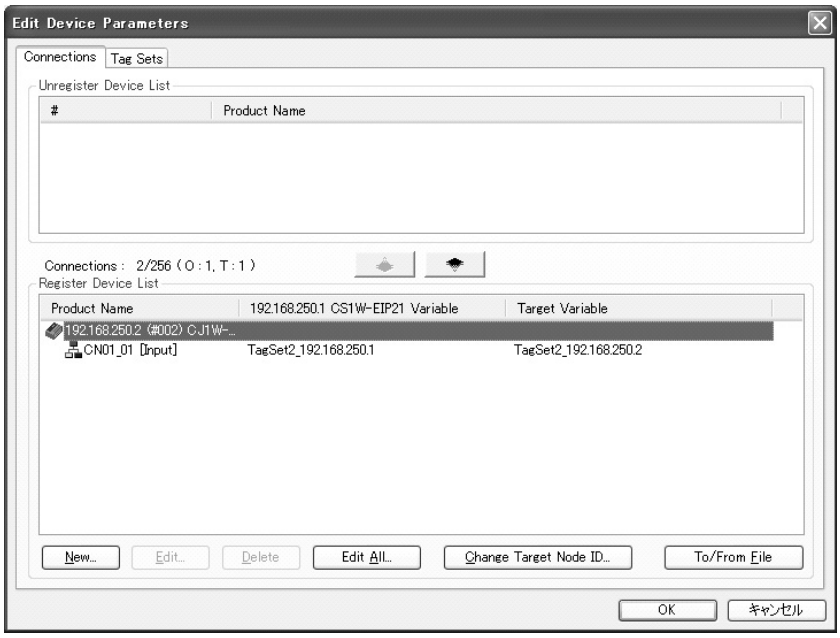
c. Input a new RPI value, and click the **OK** Button.

Method 3: Changing a Particular Connection's RPI Setting

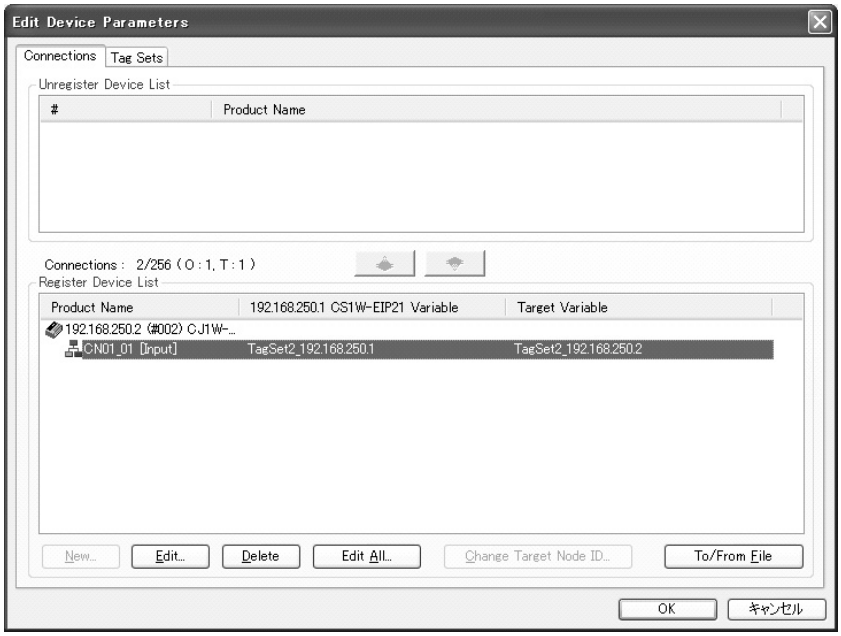
The usage of capacity can be adjusted by individually changing the packet intervals (RPI) setting for a particular connection. In this case, the usage of capacity will also change for the device that is the target device of the connection which was adjusted.

a. Click the **Close** Button at the bottom of the Usage of Device Bandwidth Dialog Box.

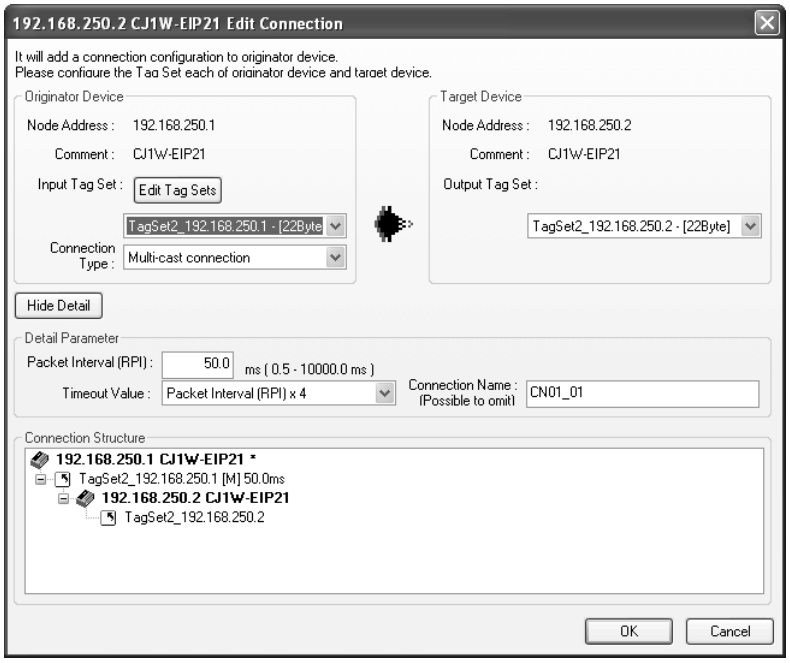
b. Double-click the device that is set as the originator of the desired connection. The Edit Device Parameters Dialog Box will be displayed.



c. In the Register Device List, select the connection for which you want to change the RPI, and click the **Edit** Button.



d. The device's Edit Connections Dialog Box will be displayed. Input a new RPI value, and click the **OK** Button.



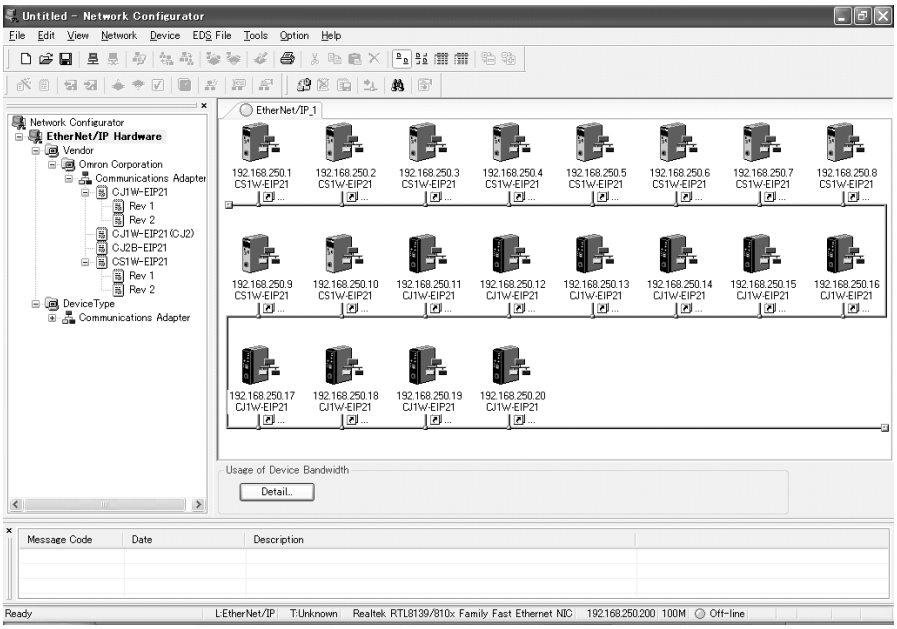
4. If the usage of capacity cannot be adjusted to the desired level when the setting described above has been performed, reconsider the network configuration considering the following points. Refer to *10-2-3 Adjusting Device Bandwidth Usage*.
   - Reduce the number of nodes and number of connections.
   - Split the network.
5. Check the bandwidth usage again.

   If the connection settings have been changed, click the **Detail** Button in the Usage of Device Bandwidth Area at the bottom of the Network Configuration Window and check bandwidth usage according to the instructions in *10-2-1 Checking Bandwidth Usage for Tag Data Links*. It is particularly important to check the usage of capacity when an individual connection's RPI setting was changed without using the **Set Packet Interval (RPI)** Button at the bottom of the Usage of Device Bandwidth Dialog Box.
6. Run user tests to verify that there are no problems with the new settings.

10-2-5 RPI Setting Examples

The following examples explain how to calculate the packet intervals (RPI) in the following network configuration.

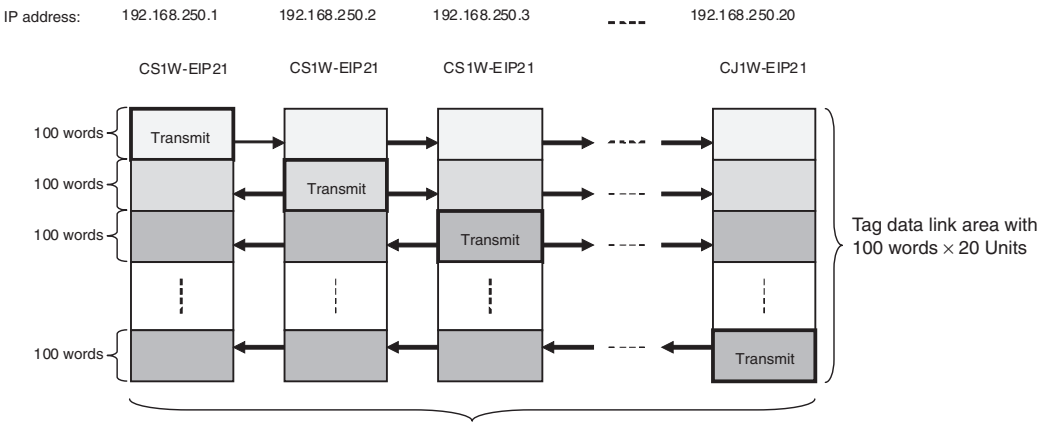
Example Conditions



Connections

In this example, there are 10 CS1W-EIP21 Units and 10 CJ1W-EIP21 Units for a total of 20 devices connected in the network. Each device has one 100-word tag for transmission and nineteen 100-word tags for reception, so that the Units exchange data mutually.

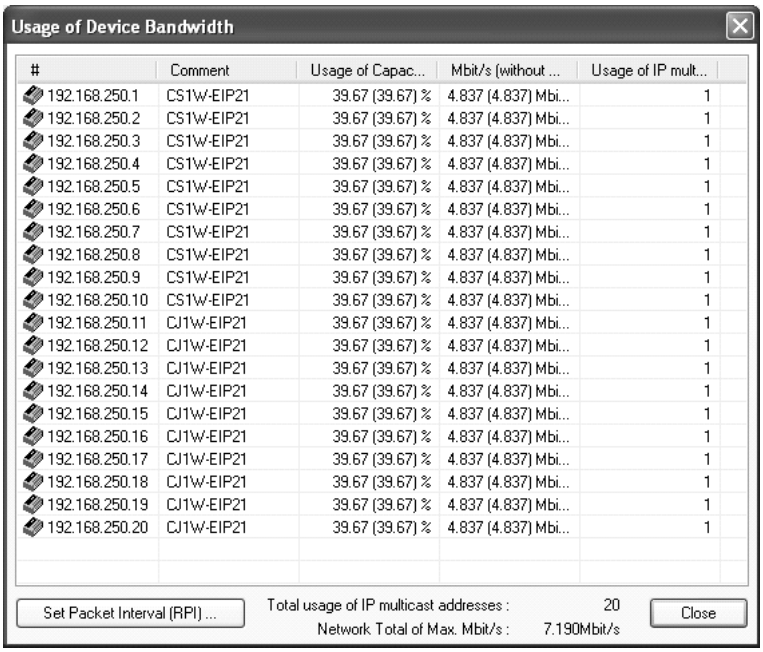
By default, the packet intervals (RPI) are set to 10 ms for all of the connections. The devices' IP addresses range from 192.168.250.1 to 192.168.250.20.



10 CS1W-EIP21 Units + 10 CJ1W-EIP21 Units = 20 Units total
The RPI is 10 ms (Ethernet default) for all connections.

Checking the Device Bandwidth Usage

When the **Detail** Button is clicked in the Usage of Device Bandwidth Area, it is apparent that the percentage of the allowed tag data link bandwidth being used by each device's tag data link (Usage of Capacity) is 39.67%, as shown in the following dialog box.

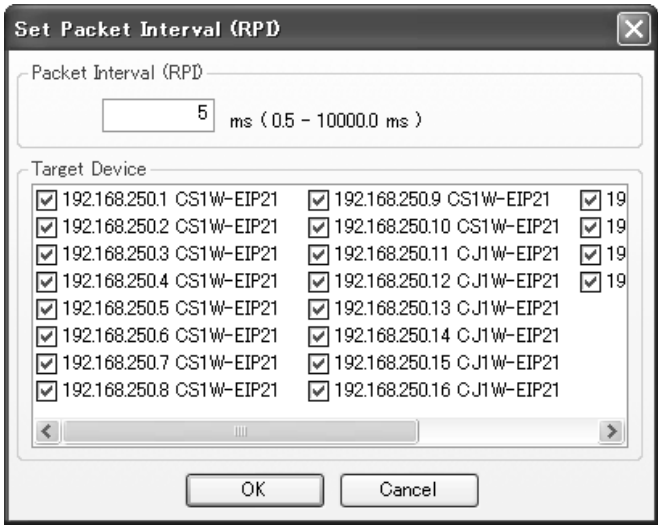


Changing the Settings

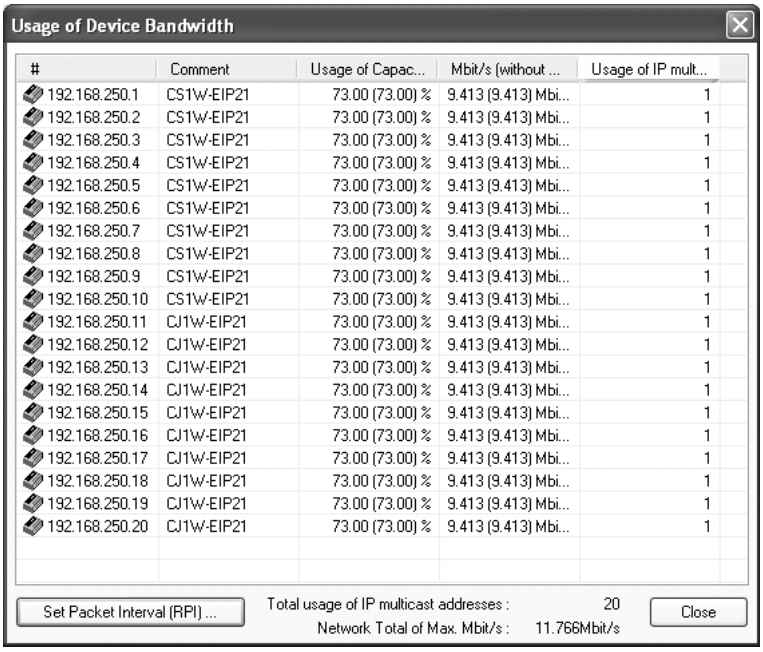
Method 1: Same Packet Interval Setting for All Connections

The percentage of the allowed tag data link bandwidth being used (Usage of Capacity) was 39.67% with the RPI set to 10.0 ms for all of the connections, so the RPI will be set to 5.0 ms, with a target of 80% or less of the allowable bandwidth.

Click the **Set Packet Interval (RPI)** Button at the bottom of the Usage of Device Bandwidth Dialog Box. The Set Packet Interval (RPI) Dialog Box will be displayed. Input 5.0 ms as the new RPI value, and click the **OK** Button.



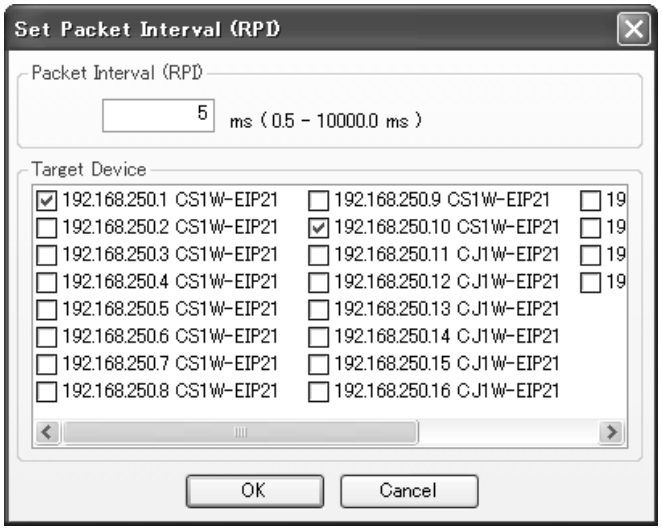
If the packet interval for all connections has been set to the same setting, the dialog box will show that the usage of capacity for the tag data link's allowable communications bandwidth is 73.00% and the fastest set value is 5.0 ms.



Method 2: Changing the Packet Interval (RPI) of Only Specific Devices

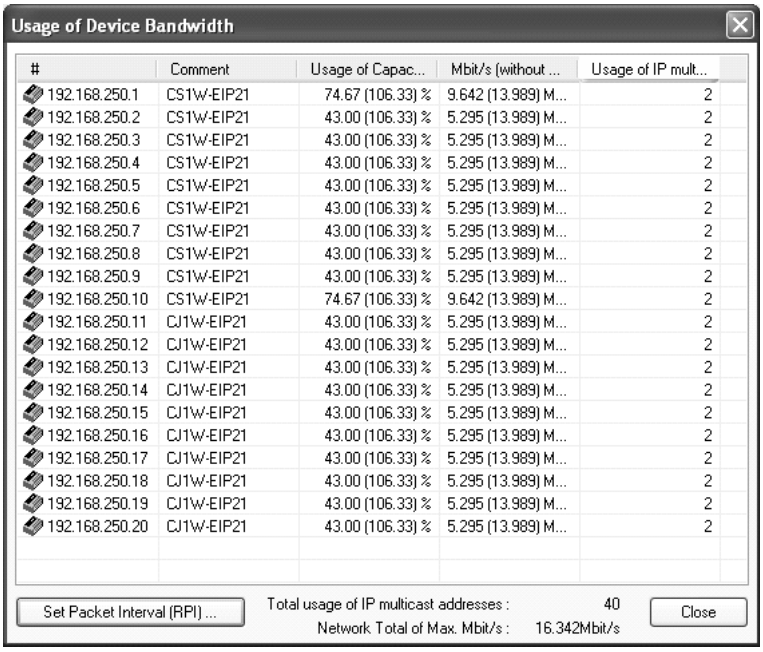
In this example, we want faster tag data links for devices 192.168.250.1 and 192.168.250.10 only. Click the **Set Packet Interval (RPI)** Button at the bottom of the Usage of Device Bandwidth Dialog Box to display the Set Packet Interval (RPI) Dialog Box.

In the Target Device Area, deselect all devices other than 192.168.250.1 and 192.168.250.10 by removing the corresponding check marks. Input 5.0 ms as the new RPI value, and click the **OK** Button.



The percentage of the allowed tag data link bandwidth being used (Usage of Capacity) increases to 74.67% for devices 192.168.250.1 and 192.168.250.10, which indicates that the RPI is set to a higher speed for these devices' connections.

The Usage of Capacity values also indicate that the Usage of Capacity has increased (from 39.67% to 43.00%) for all of the other devices, which connect with devices 192.168.250.1 and 192.168.250.10.



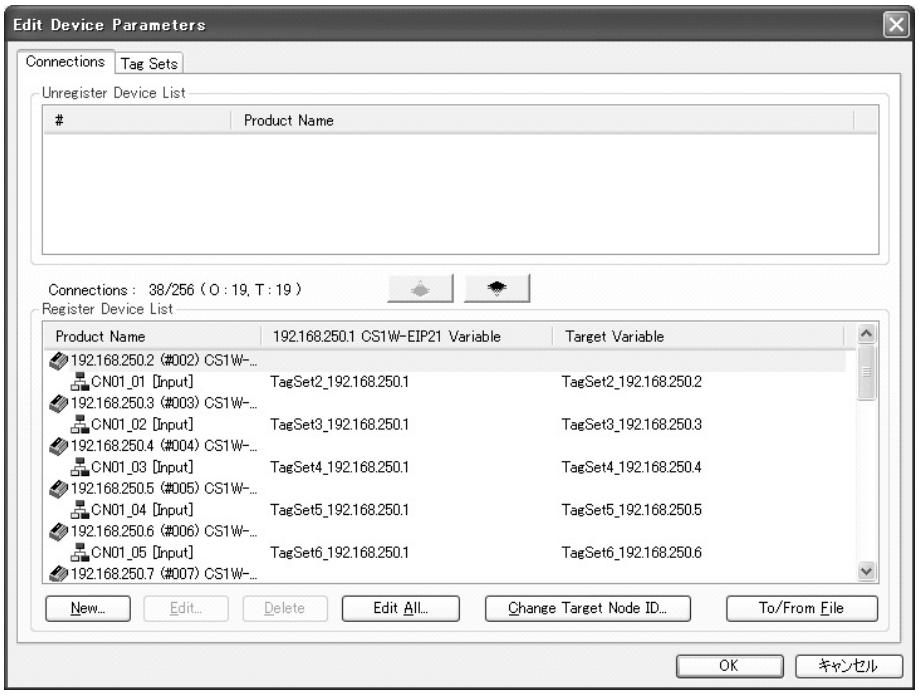
#	Comment	Usage of Capac...	Mbit/s (without ...	Usage of IP mult...
192.168.250.1	CS1W-EIP21	74.67 (106.33) %	9.642 (13.989) M...	2
192.168.250.2	CS1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.3	CS1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.4	CS1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.5	CS1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.6	CS1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.7	CS1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.8	CS1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.9	CS1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.10	CS1W-EIP21	74.67 (106.33) %	9.642 (13.989) M...	2
192.168.250.11	CJ1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.12	CJ1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.13	CJ1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.14	CJ1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.15	CJ1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.16	CJ1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.17	CJ1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.18	CJ1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.19	CJ1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2
192.168.250.20	CJ1W-EIP21	43.00 (106.33) %	5.295 (13.989) M...	2

In this case, if there is no multicast filter, the value becomes 106.33%. If there is no multicast filter for a switching hub, communications errors may occur depending on the communications load of the EtherNet/IP Unit or built-in EtherNet/IP Unit port.

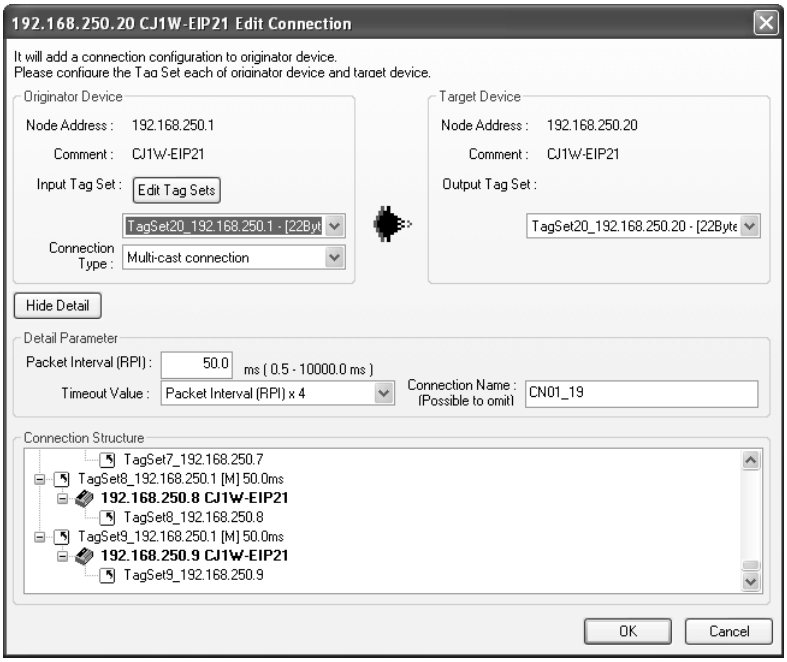
Method 3: Changing the Packet Interval (RPI) of Only Specific Connections

In this example, we want a faster tag data links for just a particular connection of device 192.168.250.1.

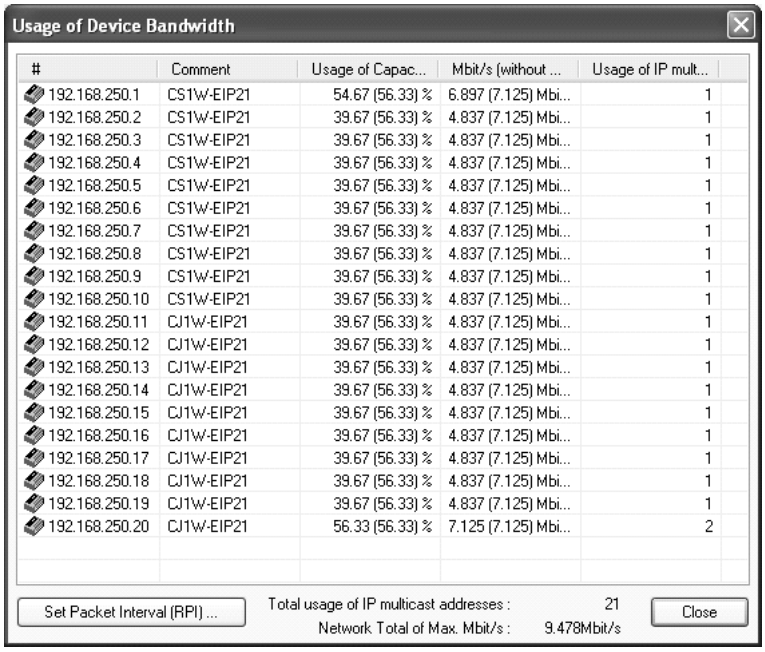
Double-click device 192.168.250.1 in the Network Configuration Window.



Information about the connection with device 192.168.250.20 is registered in the Register Device List. Double-click this connection to edit the settings.



In the Edit Connection Dialog Box, input 1.0 ms as the new RPI value, and click the **OK** Button. The tag data link bandwidth being used by device 192.168.250.1 (Usage of Capacity) increases to 54.67%, which indicates that a RPI is set to a higher speed for this device.



#	Comment	Usage of Capac...	Mbit/s (without ...	Usage of IP mult...
192.168.250.1	CS1W-EIP21	54.67 (56.33) %	6.897 (7.125) Mbi...	1
192.168.250.2	CS1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.3	CS1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.4	CS1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.5	CS1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.6	CS1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.7	CS1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.8	CS1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.9	CS1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.10	CS1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.11	CJ1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.12	CJ1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.13	CJ1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.14	CJ1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.15	CJ1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.16	CJ1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.17	CJ1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.18	CJ1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.19	CJ1W-EIP21	39.67 (56.33) %	4.837 (7.125) Mbi...	1
192.168.250.20	CJ1W-EIP21	56.33 (56.33) %	7.125 (7.125) Mbi...	2

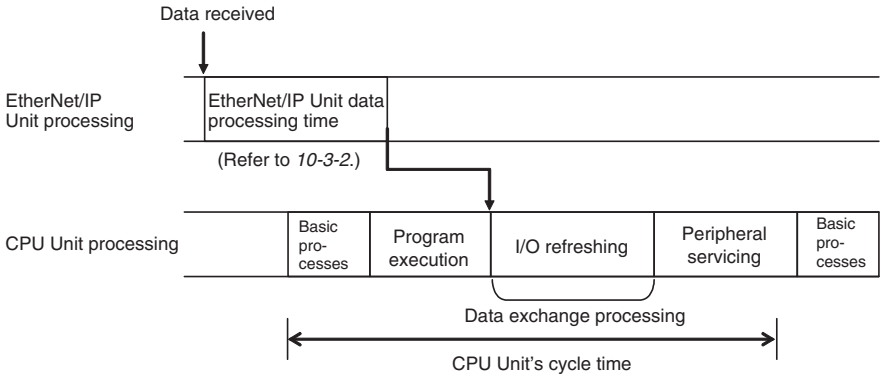
In this case, the tag data link bandwidth being used by device 192.168.250.20 (Usage of Capacity) also increases (from 39.67% to 56.33%).

10-3 I/O Response Time in Tag Data Links

10-3-1 Timing of Data Transmissions

The following diagram shows the timing of tag data link transmissions between the EtherNet/IP Unit or built-in port and the CPU Unit.

The data transmission is processed during the I/O refresh period. Send data is processed with transmission at regular intervals, and received data is processed together with the send data when new data has been received from other nodes. The following diagram shows the timing of data transmissions.



If there is an interrupt for data transmission processing, the CPU Unit's cycle time is extended by that interrupt processing time. Refer to *10-3-2 EtherNet/IP Unit or Built-in Port Data Processing Time* for details.

10-3-2 EtherNet/IP Unit or Built-in Port Data Processing Time

The following formula approximates the time required for the EtherNet/IP Unit or CJ2H built-in port to process data transmissions with the CPU Unit (i.e., the data processing time).

Approximation of the data processing time for an EtherNet/IP Unit or Built-in Port
(0.0008 × Number of data transmission words) + 1.0 ms

The maximum number of tag data link words that can be transferred by one EtherNet/IP Unit or built-in port is 184,832 words. However, if the number of tag data link words exceeds the number of words that can be exchanged with the CPU Unit at one time, the data will be divided and transferred in multiple data exchanges. The following table shows the number of words that each CPU Unit can exchange at one time.

CPU Unit	Number of words per data transmission
When connected to the CS1/CJ1/CP1H CPU Units	When using the status area with the default settings Output/Send: 7,469 words max. (If there are more words, the data will be divided.) Input/Receive: 7,469 words max. (If there are more words, the data will be divided.) **Note** The total amount of send data and receive data that can be exchanged at one time is about 14,938 words maximum. When using the status area with the user settings Output/Send: 7,405 words max. (If there are more words, the data will be divided.) Input/Receive: 7,405 words max. (If there are more words, the data will be divided.) **Note** The total amount of send data and receive data that can be exchanged at one time is about 14,810 words maximum.
When connected to the CJ2 CPU, or CJ2H-CPU6□-EIP or CJ2M-CPU3□ built-in port	When using the status area with the default settings Output/Send: 6,432 words max. (If there are more words, the data will be divided.) Input/Receive: 6,432 words max. (If there are more words, the data will be divided.) **Note** The total amount of send data and receive data that can be exchanged at one time is about 12,864 words maximum. When using the status area with the user settings Output/Send: 6,368 words max. (If there are more words, the data will be divided.) Input/Receive: 6,368 words max. (If there are more words, the data will be divided.) **Note** The total amount of send data and receive data that can be exchanged at one time is about 12,736 words maximum.
CJ3M-CPU3□	Output/send: 640 words max. (If there are more words, the data will be separated into multiple transmissions.) Input/receive: 640 words max. (If there are more words, the data will be separated into multiple transmissions.) **Note** The total amount of send data and receive data that can be transferred at one time is about 640 words maximum.

The number of data exchanges may double as given in the following table according to the relation with the CPU Unit's cycle time and the data processing time of the EtherNet/IP Unit or CJ2H built-in port.

Condition	Number of data transmissions
CPU Unit's cycle time > EtherNet/IP Unit or built-in port data processing time	Number of data transmissions based on the data size
CPU Unit's cycle time ≤ EtherNet/IP Unit or built-in port data processing time	Number of data transmissions × 2 based on the data size

Note (1) To use the tag data link and socket service functions at the same time with the CS1W/CJ1W-EIP21S and CJ3M-CPU3□, use the method by CMND instruction.

For information on the socket services, refer to *SECTION 14 Socket Services*.

(2) With CS/CJ-series PLCs, consecutive data area words specified in the tag set will be transferred together if possible. Up to 19 send data blocks can be processed in one data transmission; up to 20 receive data blocks can be processed in one data transmission. If there are more blocks, the data will be divided and transferred in separate data transmissions.

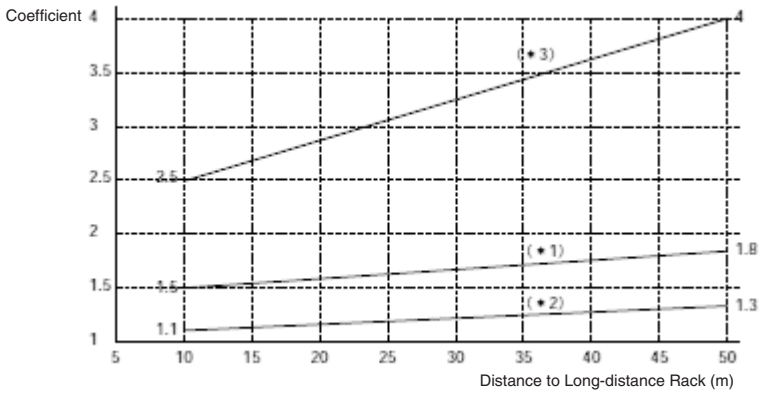
(3) The preceding data processing time approximation is the standard formula when a higher priority processing event does not occur in peripheral servicing. For example, if an instruction such as SEND, RECV, or FAL is executed, the instruction's processing will have higher priority, so the data processing time may be longer.

10-3-3 Effect on the CPU Unit's Cycle Time

The CPU Unit's cycle time is affected when the EtherNet/IP Unit or built-in port refreshes tag data and status data with the CPU Unit. This effect depends on the size of the tag data links, and can be approximated with the values in the following table. When there are multiple EtherNet/IP Units or built-in ports, the effect is cumulative.

CPU Unit	Effect of EtherNet/IP Unit or CJ2H built-in port only	Total effect when tag data links are being used
CJ2H	CPU Rack: 0.1 ms Expansion Rack: 0.13 ms	CPU Rack: Value from left column + 0.1 ms + No. of words transferred × 0.33 μs (See note 2.) Expansion Rack: Value from left column + 0.1 ms + No. of words transferred × 0.45 μs
CJ2M CJ3M	CPU Rack: 0.14 ms Expansion Rack: 0.16 ms	CPU Rack: Value from left column + 0.02 ms + No. of words transferred × 0.78 μs Expansion Rack: Value from left column + 0.02 ms + No. of words transferred × 0.92 μs
CJ1/CP1H	0.25 ms	0.25 ms + 1.5 ms + (Number of words × 1 μs)
CJ1M	0.17 ms	0.17 ms + 0.1 ms + (Number of words × 0.7 μs)
CJ1-H	0.1 ms	0.1 ms + 0.1 ms + (Number of words × 0.7 μs)
CS1	0.2 ms	0.2 ms + 1.5 ms + (Number of words × 1 μs)
CS1-H	0.1 ms	0.1 ms + 0.1 ms + (Number of words × 0.7 μs)
Long-distance Rack	0.2 ms × Coefficient 2	(0.2 ms × Coefficient 2) + 1.5 ms + (Number of words × 1 μs × Coefficient 3)

Note (1) When one of the listed CPU Bus Units is mounted in a CS-series Long-distance Rack, the I/O refreshing time is extended by the distance to the Rack in which the Unit is mounted, regardless of the model of the CPU Unit. The following graph shows the coefficients (2 and 3) required to calculate this effect.



(2) The additional time for CJ2H CPU Units with unit version 1.1 or later will be as follows if high-speed interrupts are enabled.

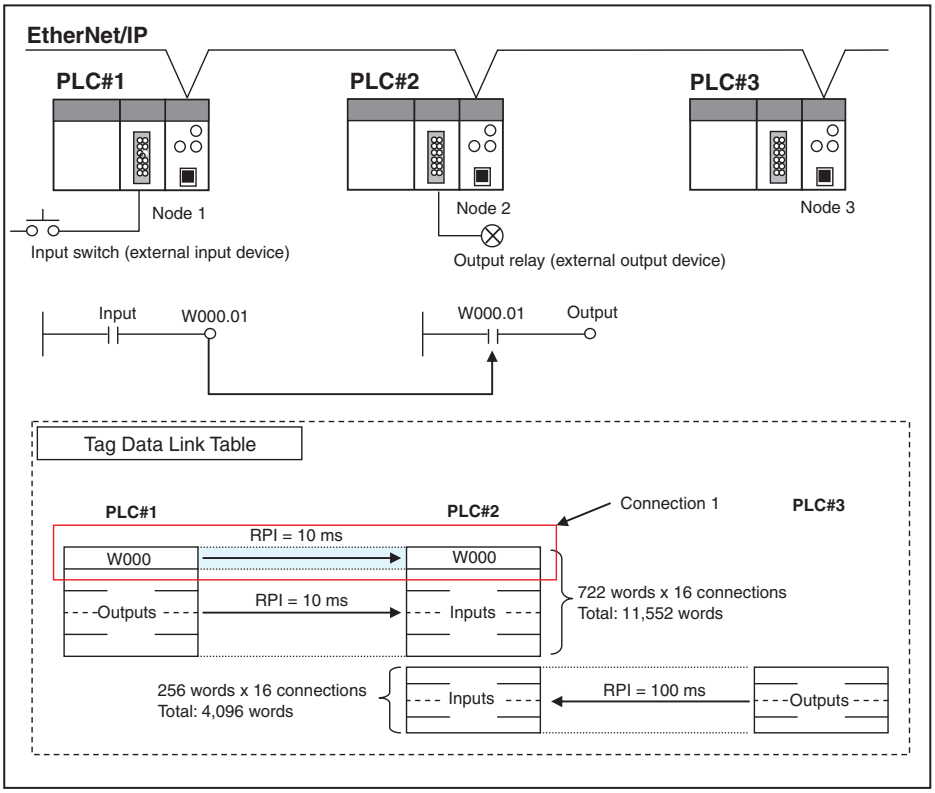
0.1 ms + Number of words transferred × 0.87 μs

(3) If you execute a message service, the event execution time will be added separately.

10-3-4 Tag Data Link I/O Response Time Calculation Example

When using the tag data link functions of the EtherNet/IP Unit or built-in port, there is a time lag between the point when the data link area's data changes due to an input at a node and the point when the change is output at another node's data link area. This time lag is called the tag data link I/O response time.

This example shows how to calculate the minimum and maximum I/O response times in the following configuration for connection 1 opened between node 1 and node 2.

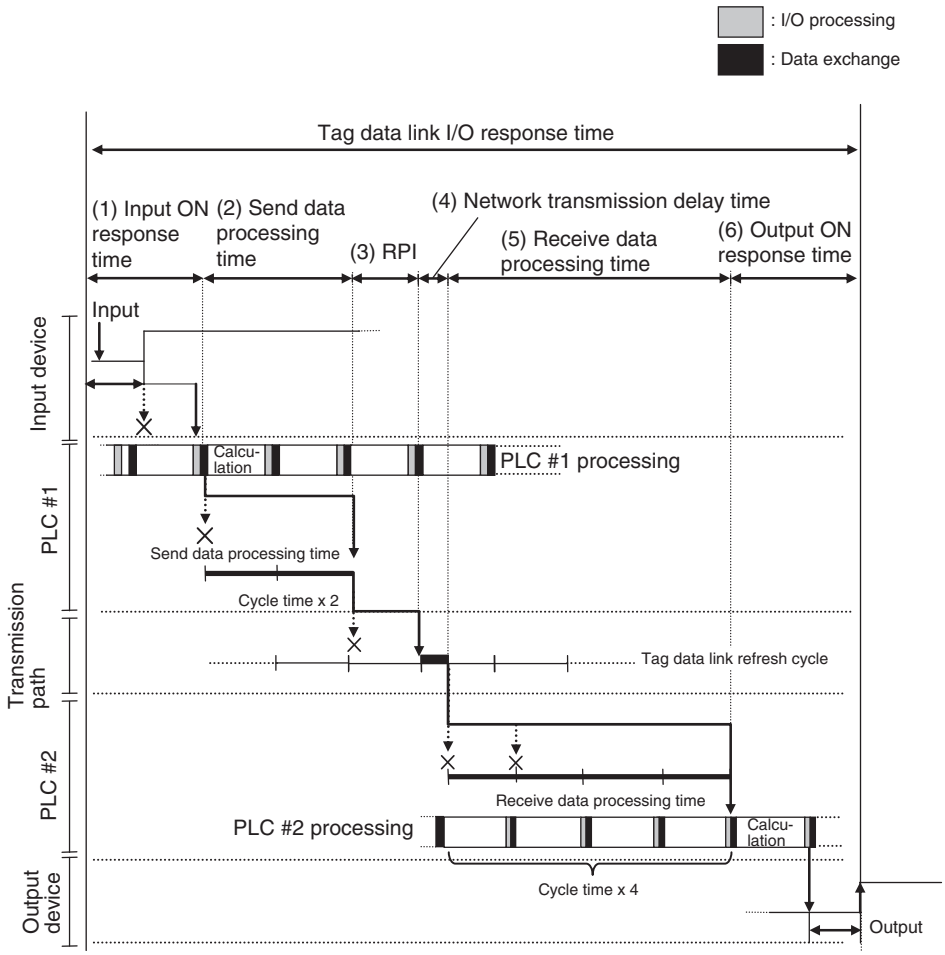


The following table gives the items required to find the I/O response time and values used in calculations for this system configuration.

Item		Value used in calculation example	
		PLC#1	PLC#2
External I/O device delay time		Input device delay: 1.5 ms	Output device delay: 2.0 ms
Cable length		50 m	
CPU Unit model		CJ2H CPU Unit	CJ2H CPU Unit
RPI		10 msec	---
Number of receive connections		0	32
CPU Unit cycle time		10 msec	15 msec
Total number tag data link words	Number of send words	11,552	None
	Number of receive words	None	15,648

Maximum Tag Data Link I/O Response Time

You can find the maximum I/O response time from the total of (1) to (6) in the following figure.



(1) Node 1 (PLC #1) Input ON Response Time

This is the delay time for the external input device from when the input occurs until the switch actually turns ON and the time until the input data is stored in the memory area of the CPU Unit for PLC #1. In this system, the input switch delay time is 1.5 ms. Also, one CPU cycle time is required until the data is stored in the memory area of the CPU Unit. Therefore, the input ON response time is 1.5 ms + 10 ms, or 11.5 ms.

(2) Node 1 (PLC #1) Send Data Processing Time

This is the time until memory data in the CPU Unit is transferred to the EtherNet/IP Unit. If the amount of data that can be processed in one data transmission with the CPU Unit is exceeded, data transmission will be performed over multiple cycles of the CPU Unit, and so time is calculated for the number of transmissions times the CPU Unit cycle times. The following table gives the send data processing times and breakdown for node 1 (PLC #1) in this system configuration. Refer to *10-3-2 EtherNet/IP Unit or Built-in Port Data Processing Time* for details on the calculation formula for each item.

Item	Calculation formula	Time
A CPU Unit cycle time for PLC #1		10 m sec
B Number of transmissions based on the data size	Number of data transmission words (11,552 words) ÷ 6,432 words (using a CJ2 CPU Unit)	2
C EtherNet/IP Unit data processing time	0.0008 × 6,432 + 1.0 (Maximum number of transmission words per cycle)	6.15 m sec
D Number of data transmissions	A 10 m sec > C 6.15 m sec To meet the conditions, the number of transmissions is the same as B.	2
Total: (2) Send data processing time	CPU Unit cycle time of A PLC #1 × D Number of data transmissions	20 m sec

(3) Packet Interval (RPI)

This is the communications refresh cycle set for each connection using the Network Configurator. In this system, it is the refresh cycle for connection 1 (10 ms), which includes W000.01.

(4) Network Transmission Delay Time

This is the total of the send processing delay, receive processing delay, switching hub delay, and cable delay. Refer to *10-1-3 Network Transmission Delay Time* for details on the calculation formula for network delay time. In this system, it is 5.2 ms.

Delay item	Calculation formula	Max. delay time
A Send processing delay	10 m sec × (15-10 msec/100)%	1.49 msec
B Cable delay	545 nsec + 50 m/100	272.5 nsec
C Switching hub delay	2 msec + Approx. 0.7 msec	2.7 msec
D Receive processing delay	1 + (0 connection × 0.043)	1.0 msec
Total: (4) Network Transmission Delay Time	A + B + C + D	5.2 msec

(5) Node 2 (PLC #2) Receive Data Processing Time

This is the time to transfer the data received by the EtherNet/IP Unit or built-in port to the memory area in the CPU Unit. Receive data is transferred in the order that it is received, but if the amount of data that can be processed in one transmission is exceeded, multiple cycles are required to transfer the data. Also, data transmission is performed only once per CPU Unit cycle. Therefore, if data transfer has ended in the cycle in which data is received, the start of transmission for received data will be delayed by one CPU Unit cycle time.

In this system configuration, data transfer is performed a maximum of three times based on the data size of node 2 (PLC #2) to transfer received data for node 1 (PLC #1) and node address 3 (PLC #3). Also, the cycle time of PLC #2 is 15 ms, the effect on the CPU Unit cycle time is 2.3 ms, and the data processing time for the EtherNet/IP Unit or CJ2H built-in port is 6.15 ms. The number of data transmissions is thus calculated as 3. In addition, the number of data transmissions is calculated as a maximum of 4 (3 + 1) because it is necessary to consider a delay of one CPU Unit cycle time in transferring received data.

Item	Calculation formula	Time
A CPU Unit cycle time	---	15 msec
B Number of transmissions based on the data size	Number of data transmission words (15,648 words) ÷ 6,432 words (using a CJ2 CPU Unit)	3
C EtherNet/IP Unit data processing time	0.0008 × 6,432 + 1.0 (Maximum number of transmission words per cycle)	6.15 msec
D Number of data transmissions	A 10 m sec > C 6.15 m sec To meet the condition to enable processing in one data transmission, the number of transmissions is the same as B plus 1. (Delay of one CPU Unit cycle time)	4
Total: (5) Receive data processing time	A Cycle time × D Number of data transmissions	60 msec

(6) Output ON response time

This is the delay time for the external output device from when the output bit turns ON in the memory of the CPU Unit until the output is actually performed. In this system configuration, the delay time for an output relay is 2.0 ms. Also, one CPU cycle time is required until the data is stored in the memory area of the CPU Unit.

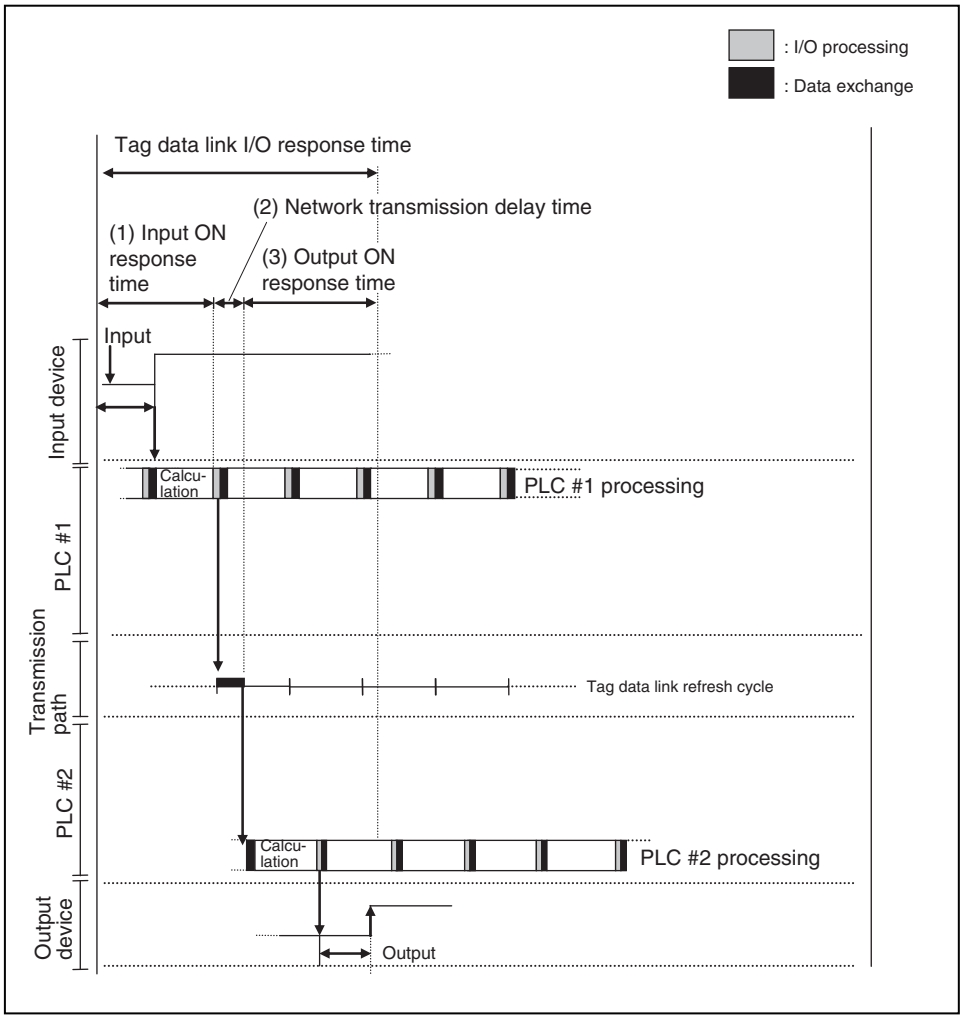
Item	Time
A CPU Unit cycle time of PLC #2	15 msec
B Output relay delay time	2.0 msec
Total: (6) Node 2 (PLC #2) output ON response time	17.0 msec

The maximum tag data link I/O response time for this system configuration found from the total of (1) to (6) is 124 ms.

(1) Node 1 (PLC #1) input ON response time	11.5 msec
(2) Node 1 (PLC #1) send data processing time	20 msec
(3) Packet Interval (RPI)	10 msec
(4) Network Transmission Delay Time	5.5 msec
(5) Node 2 (PLC #2) receive data processing time	60 msec
(6) Output ON response time	17 msec
Maximum I/O response performance (total of (1) to (6))	124 msec

Note The I/O response time may be longer due to noise, or other events.

Minimum Tag Data Link I/O Response Time



The minimum tag data link I/O response time, which occurs when there are no processing delays, is calculated as follows.

(1) Node 1 (PLC #1) input ON response time	Input switch delay time	1.5 ms
	CPU Unit cycle time of PLC #1	10.0 ms
(2) Transmission time (722 send data words)		0.121 msec
(3) Node 2 (PLC #1) output ON response time	CPU Unit cycle time of PLC #2	15.0 ms
	Output relay delay time	2.0 ms
Total (tag data link I/O response time)		28.6 ms

When the baud rate is 100 Mbps, the transmission time can be calculated with the following equation. If a network delay does not occur, just this transmission time is added.

Transmission time =
(Number of send data words $\times$ 2 + 74) $\times$ 8 $\times$ 0.00001 ms

Note The I/O response time may be longer due to noise, or other events.

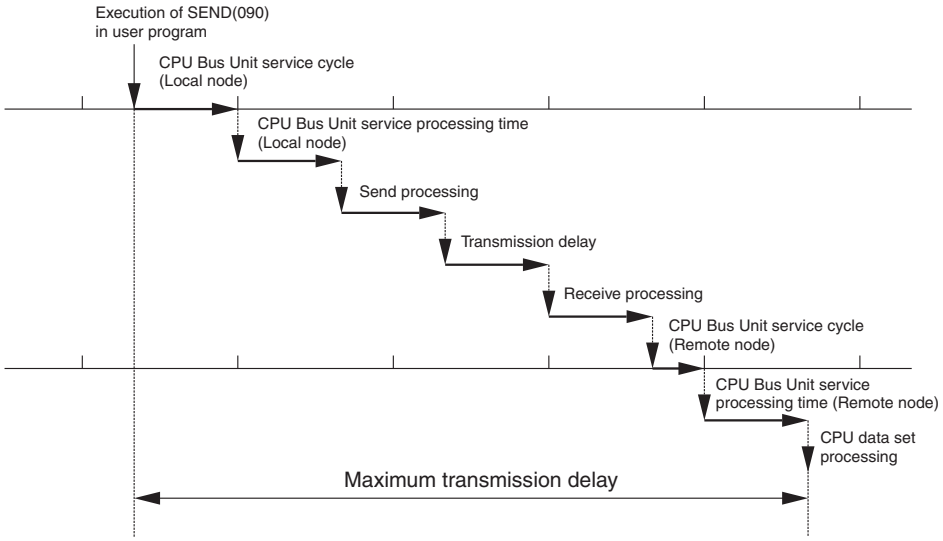
10-4 Message Service Transmission Delay

This section explains the maximum transmission delay that can occur between the execution of a SEND/SEND2(090), RECV/RECV2(098), or CMND/CMND2(490) instruction in the ladder program until completion of the instruction. This delay does not include the time required for the tag data link or the execution time of the ladder program itself.

10-4-1 Maximum Transmission Delays (Excluding Delays in the Network)

Use the following equation to calculate the maximum transmission delay that can occur between the execution of a SEND(090) or RECV(098) instruction in the ladder program until completion of the instruction.

SEND(090) Instruction



Maximum transmission delay =

CPU Bus Unit service cycle (local node)
+ CPU Bus Unit service processing time (local node)
+ Send processing
+ Transmission delay
+ Receive processing
+ CPU Bus Unit service cycle (remote node)
+ CPU Bus Unit service processing time (remote node)

CPU Bus Unit Service Cycle (Local Node)

The following table shows the service cycle, which depends on the CPU Unit's CPU processing mode setting.

CPU execution mode	Processing time details
Normal Mode (See note.)	One CPU Unit cycle time
Priority peripheral servicing	
Parallel processing with synchronous memory access	
Parallel processing with asynchronous memory access	0.2 ms + peripheral servicing time (1 ms max. for peripheral servicing of each Special I/O Unit, CPU Bus Unit, peripheral port, RS-232C port, and Inner Board)

Note CJ2/CJ3 CPU Units support only Normal Mode.

For details, refer to the *CPU Unit's Operation Manual*.

CPU Bus Unit Service Processing Time (Local Node)

The following table shows the CPU Bus Unit service processing time, which depends on the CPU Unit's CPU processing mode setting.

CPU execution mode	Processing time details
Normal Mode (See note.)	Set peripheral servicing time Default: 4% of CPU Unit cycle time (10% for CJ2/CJ3 CPU Units)
Priority peripheral servicing	
Parallel processing with synchronous memory access	
Parallel processing with asynchronous memory access	1 ms max.

Note CJ2/CJ3 CPU Units support only Normal Mode.

For details, refer to the *CPU Unit's Operation Manual*.

Send Processing

(Number of words being transferred × 0.002) + 0.550 ms

Transmission Delay

The transmission delay time depends on the baud rate set for the EtherNet/IP Unit or built-in EtherNet/IP port, as shown in the following table. (There may be additional delays due to the other devices in the network, such as switching hubs.)

Baud rate	Delay time
100Base-TX	(Number of words being transferred × 0.0013) + 0.0118 ms
10Base-T	(Number of words being transferred × 0.0019) + 0.0157 ms

Receive Processing

(Number of words being transferred × 0.003) + 0.704 ms

CPU Bus Unit Service Cycle (Remote Node)

The following table shows the CPU Bus Unit service cycle, which depends on the CPU Unit's CPU processing mode setting.

CPU execution mode	Processing time details	
Normal Mode (See note.)	One CPU Unit cycle time	
Priority peripheral servicing	EtherNet/IP Unit or built-in EtherNet/IP port is given priority.	Time slice instruction execution time
	EtherNet/IP Unit or built-in EtherNet/IP port is not given priority.	One CPU Unit cycle time
Parallel processing with synchronous memory access	One CPU Unit cycle time	
Parallel processing with asynchronous memory access	0.2 ms + peripheral servicing time (1 ms max. for peripheral servicing of each Special I/O Unit, CPU Bus Unit, peripheral port, RS-232C port, and Inner Board)	

Note CJ2/CJ3 CPU Units support only Normal Mode.

For details, refer to the *CPU Unit's Operation Manual*.

CPU Bus Unit Service Processing Time (Remote Node)

The following table shows the CPU Bus Unit service processing time, which depends on the CPU Unit's CPU processing mode setting.

CPU execution mode	Processing time details	
Normal Mode (See note.)	Set peripheral servicing time Default: 4% of CPU Unit cycle time (10% for CJ2 CPU Units)	
Priority peripheral servicing	EtherNet/IP Unit or built-in EtherNet/IP port is given priority.	Time slice peripheral servicing execution time
	EtherNet/IP Unit or built-in EtherNet/IP port is not given priority.	Set peripheral servicing time (Default: 4% of CPU Unit cycle time)
Parallel processing with synchronous memory access	Set peripheral servicing time Default: 4% of CPU Unit cycle time (10% for CJ2/CJ3 CPU Units)	
Parallel processing with asynchronous memory access	1 ms max.	

Note CJ2/CJ3 CPU Units support only Normal Mode.

For details, refer to the *CPU Unit's Operation Manual*.

Note Depending on the actual operating environment, the transmission time may be longer than the one calculated with the equations given here. The following factors can cause longer transmission times: other traffic on the network, window sizes of network nodes, other traffic at the EtherNet/IP Unit or built-in EtherNet/IP port itself (e.g., simultaneous tag data link communications), and the system configuration.

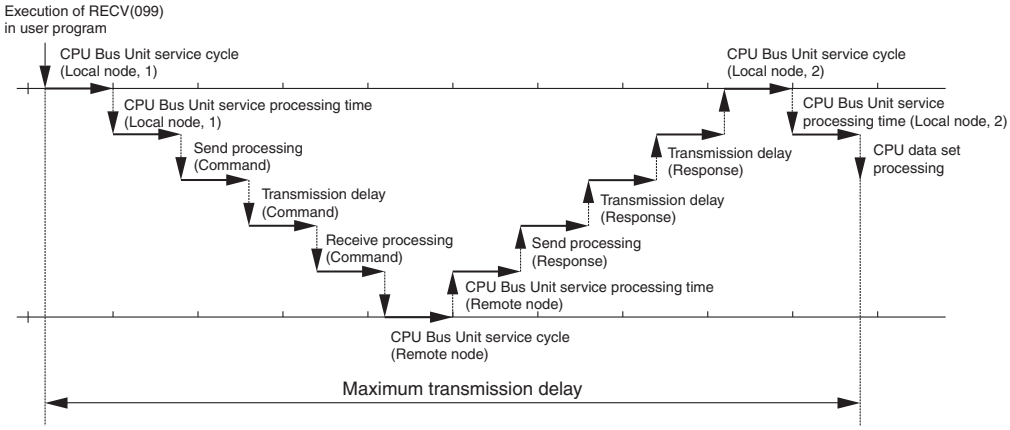
Example Calculation

In this example, SEND(090) is used to send 256 words of data between two PLCs. The maximum transmission delay is calculated based on the following operating conditions.

- Local node's CPU cycle time: 10 ms
- Local node's CPU execution mode: Normal
- Local node's CPU peripheral servicing time: Default (4%)
- Remote node's CPU cycle time: 5 ms
- Remote node's CPU execution mode: Normal
- Remote node's CPU peripheral servicing time: Default (4%)
- Baud rate: 100Base-TX

Item	Calculated value
CPU Bus Unit service cycle (local node)	10 ms
CPU Bus Unit service processing time (local node)	0.4 ms
Send processing	$(256 \times 0.002) + 0.550 = 1.062 \cong 1.1$ ms
Transmission delay	$(256 \times 0.0013) + 0.0118 = 0.3446 \cong 0.3$ ms
Receive processing	$(256 \times 0.003) + 0.704 = 1.472 \cong 1.5$ ms
CPU Bus Unit service cycle (remote node)	5 ms
CPU Bus Unit service processing time (remote node)	0.2 ms
Maximum transmission delay	10 + 0.4 + 1.1 + 0.3 + 1.5 + 5 + 0.2 = 18.5 ms

RECV(098) Instruction



Maximum transmission delay =

CPU Bus Unit service cycle (Local node, 1)
+ CPU Bus Unit service processing time (Local node, 1)
+ Send processing (Command)
+ Transmission delay (Command)
+ Receive processing (Command)
+ CPU Bus Unit service cycle (remote node)
+ CPU Bus Unit service processing time (remote node)
+ Send processing (Response)
+ Transmission delay (Response)
+ Receive processing (Response)
+ CPU Bus Unit service cycle (Local node, 2)
+ CPU Bus Unit service processing time (Local node, 2)

CPU Bus Unit Service Cycle (Local Node, 1)

The following table shows the service cycle, which depends on the CPU Unit's CPU processing mode setting.

CPU execution mode	Processing time details
Normal Mode (See note.)	One CPU Unit cycle time
Priority peripheral servicing	
Parallel processing with synchronous memory access	0.2 ms + peripheral servicing time (1 ms max. for peripheral servicing of each Special I/O Unit, CPU Bus Unit, peripheral port, RS-232C port, and Inner Board)
Parallel processing with asynchronous memory access	

Note CJ2/CJ3 CPU Units support only Normal Mode.

For details, refer to the *CPU Unit's Operation Manual*.

CPU Bus Unit Service Processing Time (Local Node, 1)

The following table shows the CPU Bus Unit service processing time, which depends on the CPU Unit's CPU processing mode setting.

CPU execution mode	Processing time details
Normal Mode (See note.)	Set peripheral servicing time
Priority peripheral servicing	Default: 4% of CPU Unit cycle time (10% for CJ2/CJ3 CPU Units)
Parallel processing with synchronous memory access	1 ms max.
Parallel processing with asynchronous memory access	

Note CJ2/CJ3 CPU Units support only Normal Mode.

For details, refer to the *CPU Unit's Operation Manual*.

Send Processing

Command	0.550 ms
Response	(Number of words being transferred × 0.002) + 0.550 ms

Transmission Delay

The transmission delay time depends on the baud rate set for the EtherNet/IP Unit or built-in EtherNet/IP port, as shown in the following table. (There may be additional delays due to the other devices in the network, such as switching hubs.)

Baud rate	Delay time	
100Base-TX	Command	0.0118 ms
	Response	(Number of words transferred × 0.0013) + 0.0118 ms
10Base-T	Command	0.0157 ms
	Response	(Number of words transferred × 0.0019) + 0.0157 ms

Receive Processing

Command	0.704 ms
Response	(Number of words being transferred × 0.003) + 0.704 ms

CPU Bus Unit Service Cycle (Remote Node)

The following table shows the CPU Bus Unit service cycle, which depends on the CPU Unit's CPU processing mode setting.

CPU execution mode	Processing time details	
Normal Mode (See note.)	One CPU Unit cycle time	
Priority peripheral servicing	EtherNet/IP Unit or built-in EtherNet/IP port is given priority.	Time slice instruction execution time
	EtherNet/IP Unit or built-in EtherNet/IP port is not given priority.	One CPU Unit cycle time
Parallel processing with synchronous memory access	One CPU Unit cycle time	
Parallel processing with asynchronous memory access	0.2 ms + peripheral servicing time (1 ms max. for peripheral servicing of each Special I/O Unit, CPU Bus Unit, peripheral port, RS-232C port, and Inner Board)	

Note CJ2/CJ3 CPU Units support only Normal Mode.

For details, refer to the *CPU Unit's Operation Manual*.

CPU Bus Unit Service Processing Time (Remote Node)

The following table shows the CPU Bus Unit service processing time, which depends on the CPU Unit's CPU processing mode setting.

CPU execution mode	Processing time details	
Normal Mode (See note.)	4% of CPU Unit cycle time (10% for CJ2/CJ3 CPU Units)	
Priority peripheral servicing	EtherNet/IP Unit or built-in EtherNet/IP port is given priority.	Time slice peripheral servicing execution time
	EtherNet/IP Unit or built-in EtherNet/IP port is not given priority.	Set peripheral servicing time (Default: 4% of CPU Unit cycle time)

CPU execution mode	Processing time details
Parallel processing with synchronous memory access	4% of CPU Unit cycle time
Parallel processing with asynchronous memory access	1 ms max.

Note CJ2/CJ3 CPU Units support only Normal Mode.

For details, refer to the *CPU Unit's Operation Manual*.

CPU Bus Unit Service Cycle (Local Node, 2)

The following table shows the CPU Bus Unit service cycle, which depends on the CPU Unit's CPU processing mode setting.

CPU execution mode	Processing time details	
Normal Mode (See note.)	One CPU Unit cycle time	
Priority peripheral servicing	EtherNet/IP Unit or built-in EtherNet/IP port is given priority.	Time slice instruction execution time
	EtherNet/IP Unit or built-in EtherNet/IP port is not given priority.	One CPU Unit cycle time
Parallel processing with synchronous memory access	One CPU Unit cycle time	
Parallel processing with asynchronous memory access	0.2 ms + peripheral servicing time (1 ms max. for peripheral servicing of each Special I/O Unit, CPU Bus Unit, peripheral port, RS-232C port, and Inner Board)	

Note CJ2/CJ3 CPU Units support only Normal Mode.

For details, refer to the *CPU Unit's Operation Manual*.

CPU Bus Unit Service Processing Time (Local Node, 2)

The following table shows the CPU Bus Unit service processing time, which depends on the CPU Unit's CPU processing mode setting.

CPU execution mode	Processing time details	
Normal Mode (See note.)	4% of CPU Unit cycle time (10% for CJ2/CJ3 CPU Units)	
Priority peripheral servicing	EtherNet/IP Unit or built-in EtherNet/IP port is given priority.	Time slice peripheral servicing execution time
	EtherNet/IP Unit or built-in EtherNet/IP port is not given priority.	Set peripheral servicing time (Default: 4% of CPU Unit cycle time)
Parallel processing with synchronous memory access	4% of CPU Unit cycle time	
Parallel processing with asynchronous memory access	1 ms max.	

Note CJ2/CJ3 CPU Units support only Normal Mode.

For details, refer to the *CPU Unit's Operation Manual*.

Note Depending on the actual operating environment, the transmission time may be longer than the one calculated with the equations given here. The following factors can cause longer transmission times: other traffic on the network, window sizes of network nodes, other traffic at the EtherNet/IP Unit or built-in EtherNet/IP port itself (e.g., simultaneous tag data link communications), and the system configuration.

Example Calculation

In this example, RECV(098) is used to receive 256 words of data from another PLC. The maximum transmission delay is calculated based on the following operating conditions.

- Local node's CPU cycle time: 10 ms
- Local node's CPU execution mode: Normal
- Local node's CPU peripheral servicing time: Default (4%)
- Remote node's CPU cycle time: 15 ms
- Remote node's CPU execution mode: Normal
- Remote node's CPU peripheral servicing time: Default (4%)
- Baud rate: 100Base-TX

Item	Calculated value
CPU Bus Unit service cycle (local node, 1)	10 ms
CPU Bus Unit service processing time (local node, 1)	0.4 ms
Send processing (command)	0.550 ms ≅ 0.5 ms
Transmission delay (command)	0.0118 ms ≅ 0.1 ms
Receive processing (command)	0.704 ms ≅ 0.7 ms
CPU Bus Unit service cycle (remote node)	15 ms
CPU Bus Unit service processing time (remote node)	0.6 ms
Send processing (command)	(256 × 0.002) + 0.550 = 1.062 ≅ 1.1 ms
Transmission delay (command)	(256 × 0.0013) + 0.0118 = 0.3446 ≅ 0.3 ms
Receive processing (command)	(256 × 0.003) + 0.704 = 1.472 ≅ 1.5 ms
CPU Bus Unit service cycle (local node, 2)	10 ms
CPU Bus Unit service processing time (local node, 2)	0.4 ms
Maximum transmission delay	10 + 0.4 + 0.5 + 0.1 + 0.7 + 15 + 0.6 + 1.1 + 0.3 + 1.5 + 10 + 0.4 = 40.6 ms

SECTION 11
FTP Server

This section describes the functions provided by the FTP server.

11-1 Overview and Specifications 346
11-1-1 Overview 346
11-1-2 Specifications 347
11-2 FTP Server Function Details 347
11-2-1 File Types 347
11-2-2 Connecting to the FTP Server 348
11-3 Using the FTP Server Function 349
11-3-1 Procedure 349
11-3-2 List of Settings Required for the FTP Server Function 350
11-4 FTP Server Application Example 351
11-5 Using FTP Commands 353
11-5-1 Table of Commands 353
11-5-2 Using the Commands 353
11-5-3 Error Messages and FTP Status 358
11-6 Checking FTP Status 359
11-6-1 FTP Status Flag 359
11-7 Using File Memory 360
11-7-1 File Memory 360
11-7-2 File Types 360
11-7-3 Initializing File Memory 362
11-7-4 I/O Memory Data Format 362
11-8 FTP File Transfer Time 365
11-9 Host Computer Application Example 366

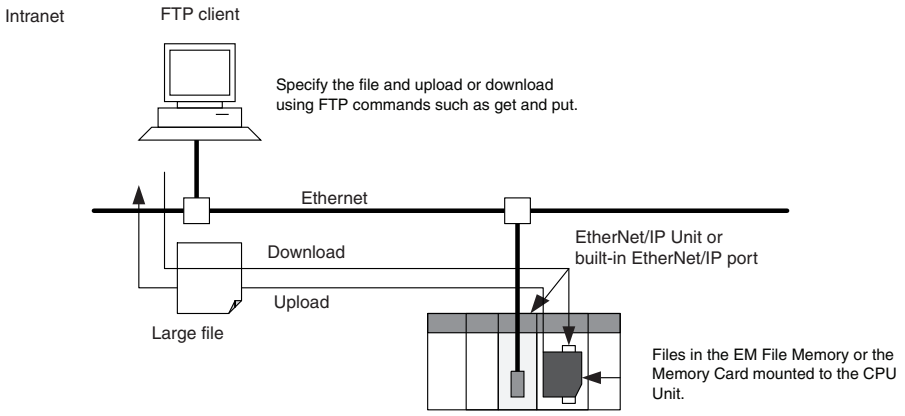
11-1 Overview and Specifications

11-1-1 Overview

The EtherNet/IP Unit or built-in EtherNet/IP port has a built-in FTP (File Transfer Protocol) server function, so other computers on the Ethernet can read or write (upload/download) large files in the EM file memory by executing FTP commands from the FTP client software.

For EtherNet/IP Units or built-in EtherNet/IP ports excluding CS1W/CJ1W-EIP21S, whether or not the FTP server can be used depends on the unit version.

Model	Unit version	FTP server
CS1W/CJ1W-EIP21S CJ3M-EIP21S (CJ3M-CPU3☐)	Ver.1.0 or later	Can be used
CS1W/CJ1W-EIP21 CJ2B-EIP21 (CJ2M-CPU6☐-EIP) CJ2M-EIP21 (CJ2M-CPU3☐)	Ver.2.0 or later	Can be used
	Ver.1.0	Cannot be used



Note Only one FTP client can connect at the same time.

Note Do not perform a simple backup operation in CS/CJ-series CPU Units while executing an FTP command from the FTP client software.

11-1-2 Specifications

Item		Specification	
		CS1W/CJ1W-EIP21 CJ2H-CPU6□-EIP CJ2M-CPU3□	**CS1W/CJ1W-EIP21S CJ3M-CPU3□**
Use of FTP		Default: Use FTP	Default: Not Use FTP
Executable commands		`open`: Connects the specified host FTP server. `user`: Specifies user name for the remote FTP server. `ls`: Displays the Memory Card file names. `dir`: Displays the Memory Card file names and details. `rename`: Changes a file name. `mkdir`: Creates a new directory in the working directory in the remote host. `rmdir`: Deletes a new directory from the working directory in the remote host. `cd`: Changes the Ethernet Unit work directory to the specified directory. `pwd`: Displays the Ethernet Unit work directory. `type`: Specifies the data type of transferred files. `get`: Transfers the specified file from the Memory Card to the local host. `mget`: Transfers multiple files from the Memory Card to the local host. `put`: Transfers the specified local file to the Memory Card. `mput`: Transfers multiple local files to the Memory Card. `delete`: Deletes the specified file from the Memory Card. `mdelete`: Deletes multiple files from the Memory Card. `close`: Disconnects the FTP server. `bye`: Closes the FTP (client). `quit`: Closes the FTP (client).	
Protection		FTP login name and password	
	FTP login name length	0 to 12 characters	1 to 16 characters
	Default FTP login name	CONFIDENTIAL	No
	Password length	0 to 8 characters	8 to 16 characters
Protocol		FTP (port number: 20/TCP, 21/TCP)*1	
Number of connections		1	

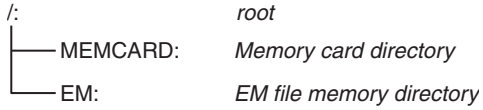
*1 The port numbers can be changed.

Note The PLC, however, is unable to read or write files at other nodes using FTP because the EtherNet/IP Unit or built-in EtherNet/IP port does not support FTP client functions.

11-2 FTP Server Function Details

11-2-1 File Types

The file system in the CPU Unit that can be accessed by the EtherNet/IP Unit or built-in EtherNet/IP port includes files in any Memory Card mounted in the CPU Unit and files in the EM file memory. The directory tree is shown below.



A connection will be initially made to the root directory.

Note
1. The date of the MEMCARD directory displayed for ls or dir commands in the root directory will be the date of the file system volume label.
2. The login date will be displayed for EM files and for MEMCARD if a volume label has not been created.

11-2-2 Connecting to the FTP Server

The host computer must connect to the FTP server before the FTP server functions can be used. The login name and password set in the Unit Setup will be used when connecting.

The operation when the login name and password are not set depends on the Unit model number.

Unit model number	Operation
CS1W/CJ1W-EIP21S CJ3M-CPU3☐	Login is not allowed.
CS1W/CJ1W-EIP21 CJ2H-CPU6☐-EIP CJ2M-CPU3☐	Using the login name *CONFIDENTIAL* allows for login without password check.

The FTP server in the EtherNet/IP Unit or built-in EtherNet/IP port can connect to only one client at a time. If a client attempts to connect when the FTP server is in use, a message will be returned and connection will be refused.

Login Name and Password Setting

In the Unit Setup (CPU Bus System Setup), set the login name and password in the FTP Tab Page.

If this setting is omitted, the CS1W/CJ1W-EIP21, CJ2H-CPU6☐-EIP or CJ2M-CPU3☐ will operate as shown below.

The default login name for FTP is “CONFIDENTIAL” and no password is set for the default login, so login is possible by simply entering “CONFIDENTIAL” as the login name.

Login Messages

Status	Message
Normal connection	`220 xxx.xx.xx.xx yyyyyyyyyy FTP server (FTP Version z.zz) ready.` `xxx.xx.xx.xx:` IP address of EtherNet/IP Unit or built-in EtherNet/IP port `yyyyyyyyyy:` EtherNet/IP Unit or built-in EtherNet/IP port model number (e.g., CS1W-EIP21) `z.zz:` Firmware version of EtherNet/IP Unit or built-in EtherNet/IP port
FTP server busy	`221 FTP server busy, Goodbye.`

Setting Restrictions

The following restrictions apply to login names and passwords.

- The login name and password must consist of alphanumeric characters, hyphens, and/or underscores. They are case sensitive.
- For the length of the login name and password, refer to *11-1-2 Specifications*.

- Always set a password when setting a new login name. The login name will not be valid unless a password is set for it.
- For CS1W/CJ1W-EIP21, CJ2H-CPU6□-EIP or CJ2M-CPU3□, if a login name is not set or contains illegal characters, the default login name, CONFIDENTIAL, must be used. In this case, no password is required and any password that is set will be ignored.

FTP File Transfer Mode

FTP has two file transfer modes: ASCII mode and binary mode. Before starting to transfer files, use the `type` command (specifies the data type of transferred files) to select the required mode.

Always select binary mode for binary files (extensions .IOM, .STD, or .OBJ) in the CS/CJ-series file memory and other program files (with extensions such as .CXP).

11-3 Using the FTP Server Function

11-3-1 Procedure

1,2,3...

1. Make the basic settings.
   Refer to *Initial Settings* on page 44.
2. With the CX-Programmer online, right-click the EtherNet/IP Unit or built-in EtherNet/IP port in the IO Table Dialog Box of the CX-Programmer, and select ***Edit - Unit Setup***. Set the following on the FTP Tab Page of the Edit Parameters Dialog Box.
   - Use of FTP
   - FTP login name
   - FTP password
   - Port number

Note CS1W/CJ1W-EIP21, CJ2H-CPU6□-EIP or CJ2M-CPU3□, you can omit these settings. In this case, using the login name *CONFIDENTIAL* allows for login without password check.

3. Select ***Transfer to PLC*** from the PLC Menu and click the **Yes** Button. The setting data will be transferred to the CPU Bus Unit System Setup Area in the CPU Unit.
4. When reading from and writing to the Memory Card:
   Mount the Memory Card into the CPU Unit.
5. Connect the EtherNet/IP Unit or built-in EtherNet/IP port using the FTP client software.
6. Enter the FTP login name and password set in the Unit Setup and log into the EtherNet/IP Unit or built-in EtherNet/IP port.

   Note Once logged in, the ftp commands can be used, such as cd (Change Directory), and get (Obtain File).
7. Search in the following directories for the required file in the Memory Card mounted to the CPU Unit or the EM File Memory.

File memory type	Directory
Memory Card	\MEMCARD
EM File Memory	\EM

8. Download the files.
9. Exit the connection.

Note The EtherNet/IP Unit or built-in EtherNet/IP port will be restarted when the settings data is transferred to the CPU Bus Unit System Setup Area, so that the new settings are read and become effective. Verify that it is safe for the EtherNet/IP Unit or built-in EtherNet/IP port to restart before transferring the settings data.

11-3-2 List of Settings Required for the FTP Server Function

Make the following settings for the unit setup when the server function is used.

CX-Programmer tab	Settings	Setting conditions
FTP	Login	User-set (when the default, CONFIDENTIAL, is not used)
	Password	User-set
	Port No.	Rarely required (when the default, 21, is not used)

In the CX-Programmer, set the above settings in the FTP Tab Page of the Edit Parameters Dialog Box.

Refer to *Using FTP* in *3-11 Other Parameters* for information on these settings.

11-4 FTP Server Application Example

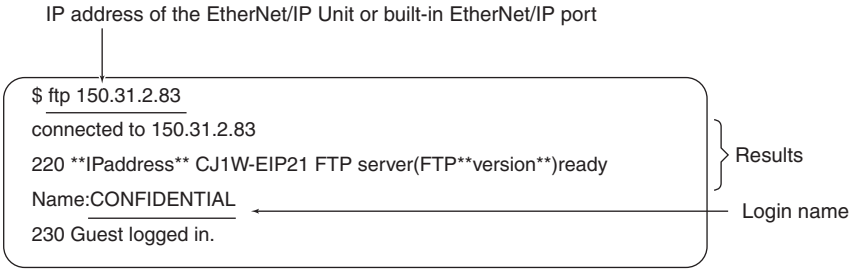
Here, an example of using the FTP server with a CJ1W-EIP21 is shown.

The following procedure shows how to use the FTP server by connection with the default login name, CONFIDENTIAL. No password is required.

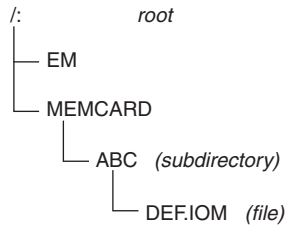
Note The login name and a password must be set in the CPU Bus Setup for the Ethernet Unit in the CPU Unit to use any login name other than CONFIDENTIAL.

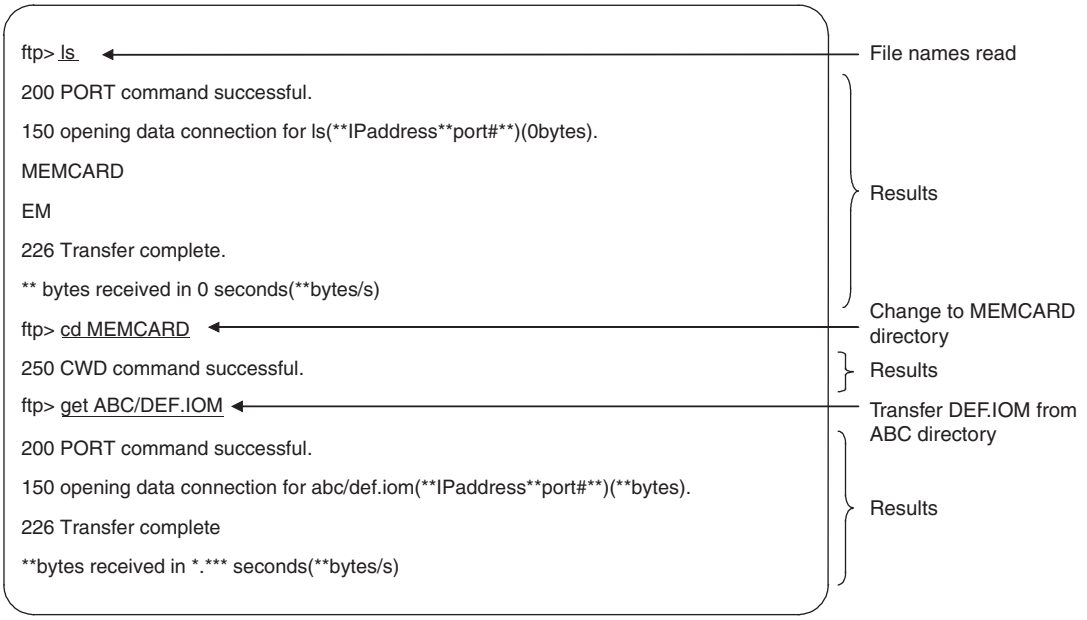
1,2,3...

1. Make sure that a Memory Card is inserted in the CPU Unit and turn ON the power supply to the PLC. If EM File Memory is to be used, create the EM File Memory.
2. Connect to the FTP server from a computer on the Ethernet by entering the text that is underlined in the following diagram.



3. Enter FTP commands (underlined in the following diagram) to read and write files. The following directory tree is used in this example.


/: root
EM
MEMCARD
ABC (subdirectory)
DEF.IOM (file)


ftp> ls
File names read
200 PORT command successful.
150 opening data connection for ls(**IPaddress**port#**)(0bytes).
MEMCARD
EM
226 Transfer complete.
** bytes received in 0 seconds(**bytes/s)
Results
ftp> cd MEMCARD
Change to MEMCARD directory
250 CWD command successful.
Results
ftp> get ABC/DEF.IOM
Transfer DEF.IOM from ABC directory
200 PORT command successful.
150 opening data connection for abc/def.iom(**IPaddress**port#**)(**bytes).
226 Transfer complete
bytes received in *.* seconds(**bytes/s)
Results

11-5 Using FTP Commands

This section describes the FTP commands which the host computer (FTP client) can send to the FTP server of the EtherNet/IP Unit or built-in EtherNet/IP port. The descriptions should also apply to most UNIX workstations, but slight differences may arise. Refer to your workstation's operation manuals for details.

11-5-1 Table of Commands

The FTP commands which can be sent to the EtherNet/IP Unit or built-in EtherNet/IP port are listed in the following table.

Command	Description
`open`	Connects the specified host FTP server.
`user`	Specifies user name for the remote FTP server.
`ls`	Displays the Memory Card file names.
`dir`	Displays the Memory Card file names and details.
`rename`	Changes a file name.
`mkdir`	Creates a new directory in the working directory in the remote host.
`rmdir`	Deletes a new directory from the working directory in the remote host.
`cd`	Changes the Ethernet Unit work directory to the specified directory.
`pwd`	Displays the Ethernet Unit work directory.
`type`	Specifies the data type of transferred files.
`get`	Transfers the specified file from the Memory Card to the local host.
`mget`	Transfers multiple files from the Memory Card to the local host.
`put`	Transfers the specified local file to the Memory Card.
`mput`	Transfers multiple local files to the Memory Card.
`delete`	Deletes the specified file from the Memory Card.
`mdelete`	Deletes multiple files from the Memory Card.
`close`	Disconnects the FTP server.
`bye`	Closes the FTP (client).
`quit`	Closes the FTP (client).

- The EtherNet/IP Unit or built-in EtherNet/IP port is considered to be the remote host and the host computer (FTP client) is considered to be the local host.
- A remote file is a file on the Memory Card or in EM File Memory in the CPU Unit. A local file is one in the host computer (FTP client).
- The parent directory is the directory one above the working directory.

11-5-2 Using the Commands

open

Format

`open [`*`IP_address`* `or` *`host_name_of_FTP_server`*`]`

Function

Connects the FTP server. Normally when the FTP client is booted, the FTP server IP address is specified to execute this command automatically.

user

Format

```
user [user_name]
```

Function

Specifies the user name. Specify the FTP login name set in the EtherNet/IP Unit or built-in EtherNet/IP port system setup. Following this, when asked to enter a password, enter the FTP password set in the system setup.

The user name is automatically requested immediately after connection to the FTP server.

Refer to *11-2-2 Connecting to the FTP Server* for information on the operation when the login name and password are not set.

ls

Format

```
ls [-l] [REMOTE_FILE_NAME [local_file_name]]
```

Function

Displays the remote host (Memory Card or EM File Memory) file names.

Set the switch [-l] to display not only the file names but the creation date and size as well. If the switch is not set, only the file names will be displayed.

You can specify a file name in the Memory Card or EM File Memory if desired.

If a local file name is specified, the file information will be stored in the specified file in the host computer.

dir

Format

```
dir [REMOTE_FILE_NAME [local_file_name]]
```

Function

Displays the file names, date created, and size of the files in the remote host (Memory Card or EM File Memory). It displays the same information as command [ls -l].

Specify a file name in the Memory Card or EM File Memory as the remote file name.

If a local file name is specified, the file information is stored in the specified file in the host computer.

rename

Format

```
rename CURRENT_FILE_NAME NEW_FILE_NAME
```

Function

Changes the specified current file name to the specified new file name.

`rename` can be used only to change the file name. It cannot be used to move the file to a different directory.

mkdir

Format

```
mkdir DIRECTORY_NAME
```

Function

Creates a directory of the specified name at the remote host (Memory Card or EM File Memory).

An error will occur if a file or directory of the same name already exists in the working directory.

rmdir

Format

```
rmdir DIRECTORY_NAME
```

Function

Deletes the directory of the specified name from the remote host (Memory Card or EM File Memory).

The directory must be empty to delete it.

An error will occur if the specified directory does not exist or is empty.

pwd

Format

```
pwd
```

Function

Displays the remote host's (Ethernet Unit) current work directory.

cd

Format

```
cd [directory_name]
```

Function

Changes the remote host (Ethernet Unit) work directory to the specified remote directory.

The files in the Memory Card are contained in the MEMCARD directory under the root directory (/). The files in EM File Memory are contained in the EM directory under the root directory (/). The root directory (/) is the directory used when logging into the EtherNet/IP Unit or built-in EtherNet/IP port. No MEM-CARD directory will exist if a Memory Card is not inserted in the PLC or if the Memory Card power indicator is not lit. No EM directory will exist if EM File Memory does not exist.

type

Format

```
type data_type
```

Function

Specifies the file data type. The following data types are supported:

ascii: Files are transferred as ASCII data
binary (image): Files are transferred as binary data.

All files are treated by the PLC as binary files. Before reading or writing any files, always use the `type` command to set the file type to binary. File contents cannot be guaranteed if transferred as ASCII data.

The default file type is ASCII.

get

Format

`get` *FILE_NAME* [*receive_file_name*]

Function

Transfers the specified remote file from the Memory Card or EM File Memory to the local host.

A receive file name can be used to specify the name of the file in the local host.

mget

Format

`mget` *FILE_NAME*

Function

Allows the use of a wildcard character (*) to transfer multiple remote files from the Memory Card or EM File Memory to the local host.

put

Format

`put` *file_name* [*DESTINATION_FILE_NAME*]

Function

Transfers the specified local file to the remote host (Memory Card or EM File Memory).

A destination file name can be used to specify the name the file is stored under in the Memory Card or EM File Memory.

Any existing file with the same name in the remote host (Memory Card or EM File Memory) will be overwritten by the contents of the transferred file.

If an error occurs during file transfer, the file being transferred will be deleted and the transmission will end in an error.

mput

Format

`mput` *FILE_NAME*

Function

Allows the use of a wildcard character (*) to transfer multiple local files to the remote host (Memory Card or EM File Memory).

Any existing file with the same name in the remote host (Memory Card or EM File Memory) will be overwritten by the contents of the transferred file.

If an error occurs during file transfer, the file being transferred will be deleted and the transmission of that file will end in an error. However, mput execution will continue and remaining files will be transferred.

delete

Format

`delete` *FILE_NAME*

Function

Deletes the specified remote file from the Memory Card or EM File Memory.

mdelete

Format

```
mdelete FILE_NAME
```

Function

Allows the use of a wildcard character (*) to delete multiple remote files from the Memory Card or EM File Memory.

close

Format

```
close
```

Function

Disconnects the FTP server of the EtherNet/IP Unit or built-in EtherNet/IP port.

bye

Format

```
bye
```

Function

Ends the FTP (client).

quit

Format

```
quit
```

Function

Ends the FTP (client).

11-5-3 Error Messages and FTP Status

Error Messages

The error messages returned by the EtherNet/IP Unit or built-in EtherNet/IP port are listed in the following table.

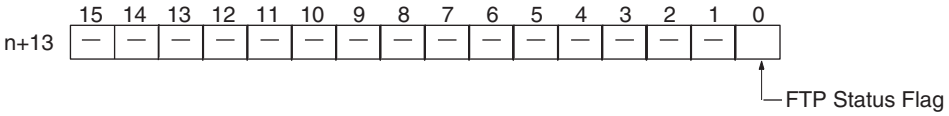
Message	Meaning
PPP is a directory.	The path name indicated at PPP is a directory.
PPP is not a directory.	The path name indicated at PPP is not a directory.
Another unit has access authority (FINS error 0 x 3001).	Another Unit currently has the access right.
Bad sequence of commands.	The RNFR command has not been executed.
Can't create data socket (X.X.X.X, YY).	A socket cannot be created.
Cannot access to device (FINS error 0 x 250F).	A file device error has occurred.
Cannot get memory blocks.	A message memory block cannot be allocated.
Command format error (FINS error 0 x 1003).	The command format is incorrect.
Connect error.	A connection error has occurred.
Directories of old and new paths are not same.	The directories before and after changing the name are different.
Directory name length exceeded max. size.	The directory name is too long.
Directory not empty (FINS error 0 x 2108).	The directory must be empty to delete it.
Fatal error (FINS error 0 x 1101).	A parameter error has occurred.
Fatal error (FINS error 0 x 1103).	
File or directory already exists.	The specified file or directory name already exists.
File or directory already exists (FINS error 0 x 2107).	
File or directory name illegal.	The file or directory name is incorrect.
File or directory name illegal (FINS error 0 x 110C).	
File read error (FINS error 0 x 1104).	An error occurs when reading the file.
File read error (FINS error 0 x 110B).	
File write error (FINS error 0 x 2106).	An error occurs when reading the file.
File write error (FINS error 0 x 2107).	
FINS error MRES 0 x XX: SRES 0 x XX.	Some other FINS error has occurred.
Length of directory name too long.	The path name of the directory is too long.
No space to create entry (FINS error 0 x 2103).	There are too many files to create a new one.
No such device (FINS error 0 x 2301).	The file device cannot be found.
No such file or directory.	The specified file or directory does not exist.
No such file or directory (FINS error 0 x 2006).	
No such file or directory (FINS error 0 x 2106).	
Not enough memory.	The communications buffers are full.
Not enough space in the system. (FINS error 1104).	The file device is full.
PLC communication error (timeout).	File access timed out.
Socket canceled.	The socket was canceled.
Socket error NN.	A socket bind error occurred. The error code will be given at NN.
Socket receive error NN.	A data reception error occurred. The error code will be given at NN.
Socket send error NN.	A data send error occurred. The error code will be given at NN.
Timeout (900 seconds): closing control connection.	The connection was closed because the client did not respond for 15 minutes.
Too many open files.	Too many sockets have been created.
Write access denied.	Writing is not possible.
Write access denied. (FINS error 0 x 2101).	

PPP: Path name
XXX: IP address
YY: Port number
MM: FINS error code
NN: Socket error code

11-6 Checking FTP Status

11-6-1 FTP Status Flag

The current status of the FTP server can be obtained from the service status in the words allocated to the EtherNet/IP Unit in the CPU Bus Unit Area in the CIO Area. The word containing the FTP Status Flag can be computed as follows: CIO 1500 + (25 x unit number) + 13



Status of bit 00	Meaning
1	FTP server busy (a user is connected)
0	FTP server free

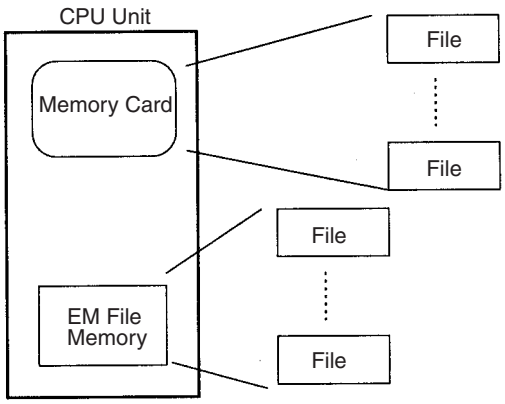
Note

1. File operations for files on the Memory Card are performed during FTP communications. Do not remove the Memory Card or turn OFF power to the PLC while FTP is being used.
2. When using File Memory Instruction from the program in the CPU Unit, program exclusive control using the FTP Status Flag so that the same data is not manipulated simultaneously by more than one instruction.

11-7 Using File Memory

There are two media that can be used to store files in memory for CS/CJ-series PLCs:

- Memory Cards
- EM File Memory



11-7-1 File Memory

Media	Memory type	Capacity	Model	File data recognized by CPU Unit
CS/CJ-series Memory Cards	Flash memory	2 GByte	HMC-SD292/293 (See note.)	• Complete user program • Specified portions of I/O Memory • Parameter area data (e.g. PLC Setup)
		4 GByte	HMC-SD492/493 (See note.)	
		16 GByte	HMC-SD1A2/1A3 (See note.)	
		128 MByte	HMC-EF183	
		256 MByte	HMC-EF283	
		512 MByte	HMC-EF583	
EM File Memory	RAM	Max. capacity of EM Area in CPU Unit	All EM Area banks from specified bank in I/O Memory (specified in PLC Setup)	

Note The HMC-SD□□□ is supported by the CJ3 CPU Unit.

11-7-2 File Types

■ **File Names**

Files are distinguished by assigning file names and extensions. The following characters can be used in file names and extensions:

Alphanumeric characters: A to Z and 0 to 9. (Names converted to all-caps)
! & $ # ’ [ ] - ^ ( ) _

The following characters cannot be used in files names and extensions:

, . / ? * ” : ; < > = + *(spaces)*

File names are not case sensitive and will be converted to all-caps in the PLC file system. File names can be up to 8 character long with 3-character extensions. An error will occur if a file name or extension is too long. The first period (.) in a file name will be taken as the delimiter between the file name and extension. Extensions are determined by the file type.

■ **Directories**

Up to five levels of directories (including root as the first level) can be created as file storage locations. A maximum of 65 characters can be used in directory names.

File Names Handled by CPU Unit

The files described in the following table can be read or written by the CPU Unit.

File type		File name	Extension	Contents	Description
Data file		********	.IOM	Specified ranges of I/O Memory	• Contains word (16-bit) data from a starting word through an end word in one memory area. • The following areas can be used: CIO, HR, WR, AR, DM, and EM.
Program file		********	.OBJ	Complete user program	• Contains all the programs for cyclic tasks and interrupt tasks, as well as task information for one CPU Unit.
Parameter area file		********	.STD	• PLC Setup • Registered I/O tables • Routing tables • CPU Bus Unit Setup and other setup data	• Contains all of the parameter data for one CPU Unit. • There is no need for the user to distinguish the various types of data contained in the file. • The file can be automatically read to or written from the CPU Unit simply by specifying the extension (.STD)
Files transferred at startup	Data files	AUTOEXEC	.IOM	I/O Memory data for the specified number of words starting from D20000	• There does not necessarily need to be a data file in the Memory Card when the automatic file transfer function is used at startup. • The AUTOEXEC.IOM file always contains DM Area data starting at D20000. • All data in the file will be transferred to memory starting at D20000 at startup.
	Program files	AUTOEXEC	.OBJ	Complete user program	• There must be a program file in the Memory Card when the automatic file transfer function is used at startup. • Contains all the programs for cyclic tasks and interrupt tasks, as well as task information for one CPU Unit.
	Parameter area file	AUTOEXEC	.STD	• PLC Setup • Registered I/O tables • Routing tables • CPU Bus Unit Setup and other setup data	• There must be a parameter file in the Memory Card when the automatic file transfer function is used at startup. • Contains all of the parameter data for one CPU Unit. • There is no need for the user to distinguish the various types of data contained in the file. • All parameters in the file will be automatically transferred to specified locations in memory at startup.

Note

1. Refer to information on file memory in the *CS/CJ-series Programmable Controllers Operation Manual* (W339).
2. All files transferred automatically at startup must have the name AUTOEXEC.

11-7-3 Initializing File Memory

Memory	Initialization method
Memory Cards	1. Insert the Memory Card into the CPU Unit. 2. Initialize the Memory Card from a Programming Device (Programming Consoles included).
EM File Memory	1. Specify in the PLC Setup the first bank to convert to file memory. 2. Initialize EM File Memory from the CX-Programmer.

11-7-4 I/O Memory Data Format

■ IOM Format

The IOM format is a data format used for binary data specified by the ladder instructions, READ DATA FILE (FREAD) and WRITE DATA FILE (FWRIT), in the CPU Unit.

If five words of data from the I/O memory (1234 hexadecimal, 5678 hexadecimal, 9ABC hexadecimal, etc.) is contained in an attached file in IOM format, the data will be stored in the attached file as shown in the following diagram.

Example: Binary data format with a delimiter after every 10 fields.

I/O memory

	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
+0	1234	5678	9ABC	DEF0	1234	5678	9ABC	DEF0	1234	5678
+10	9ABC	DEF0	1234	5678	9ABC	DEF0	1234	5678	9ABC	DEF0

.IOM file contents

XX	XX	…	XX	12	34	56	78	9A	BC	DE	F0	12	34	…

48 bytes
(Reserved by the system.)

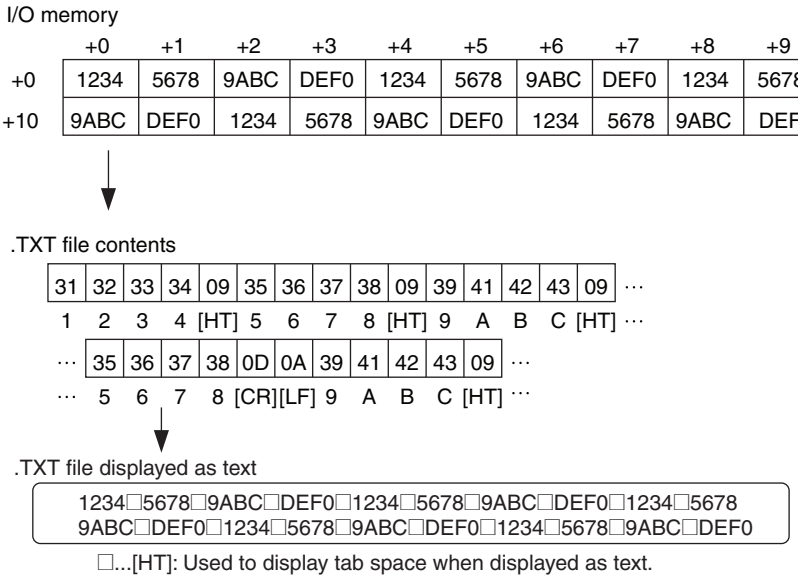
■ TXT Format

The TXT format is a data format (using tab delimiters) specified by the ladder instructions, READ DATA FILE (FREAD) and WRITE DATA FILE (FWRIT), in the CPU Unit. The format is configured according to the specified FREAD and FWRIT parameters, as follows:

Data format	Use of CRs and CR position
• Words without delimiters	• No CRs
• Double words without delimiters	• CR after every 10 fields.
• Words delimited by tabs.	• CR after each field.
• Double words delimited by tabs	• CR after every 2 fields.
	• CR after every 4 fields.
	• CR after every 5 fields.
	• CR after every 16 fields.

If data from the I/O memory (1234 hexadecimal, 5678 hexadecimal, 9ABC hexadecimal, etc.) is contained in an attached file in TXT format, the data will be converted into ASCII format in words or double-words. The words are delimited by inserting tabs ([HT]: 09), and carriage returns (CR) after specified fields ([CR][LF]: 0D0A).

Example:Data format using words delimited by tabs and CRs after every 10 fields.



□...[HT]: Used to display tab space when displayed as text.

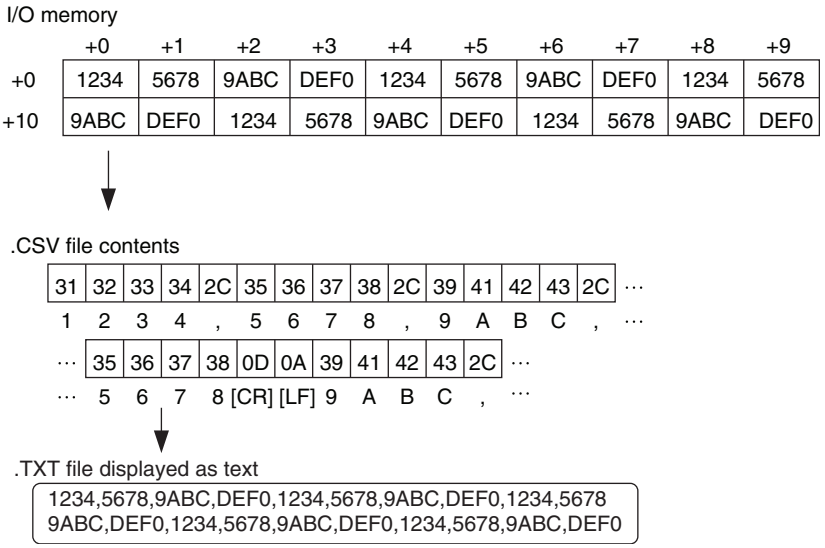
■ CSV Format

The CSV format is a data format (using comma delimiters) that is specified by ladder instructions, READ DATA FILE (FREAD) and WRITE DATA FILE (FWRIT), in the CPU Unit. The CSV format is configured according to the specified FREAD and FWRIT parameters, as follows:

Data format	Use of CRs and CR position
Words delimited by commas. Double words delimited by commas.	• No CRs • CR after every 10 fields. • CR after each field. • CR after every 2 fields. • CR after every 4 fields. • CR after every 5 fields. • CR after every 16 fields.

If word data from the I/O memory (1234 hexadecimal, 5678 hexadecimal, up to DEF0 hexadecimal) is contained in an attached file in CSV format, the word data will be converted into ASCII format in word or double-word units. The words are delimited by inserting comma delimiters (',':2C), and CRs after specified fields ([CR][LF]: 0D0A).

Example:Data format using words delimited by commas with CRs after every 10 fields.



Note FREAD will not be able to read the last byte in a file that has been written to the Memory Card if the file contains an odd number of bytes. Add 00 hexadecimal to the end of the file if necessary to write an even number of bytes to the Memory Card.

Note The UM and DM Areas contain binary data. Set the data type to binary using the `type` command before reading or writing files using FTP. (Refer to *type* on page 355.)

Note For details on how to use File Memory Instructions, refer to the *CS/CJ Series Instructions Reference Manual* (W474).

11-8 FTP File Transfer Time

File transfers using FTP can require 30 or 40 minutes depending on the capacity of the file. Approximate file transfer time are provided in the following table for reference.

All times are in seconds unless otherwise specified.

■ **CS1 CPU Units, CJ1 CPU Units, and CP1H CPU Units**

File system		Memory Card		EM File Memory	
CPU Unit status	Operating mode	PROGRAM	RUN	PROGRAM	RUN
	Cycle time	---	20 ms	---	20 ms
Transfers using `put`	1 KB	0.7 s	6.0 s	0.4 s	2.9 s
	30 KB	4.5 s	38.3 s	2.5 s	21.5 s
	60 KB	7.4 s	72.1 s	5.0 s	44.7 s
	120 KB	14.4 s	141.4 s	11.0 s	120.8 s
Transfers using `get`	1 KB	0.3 s	1.4 s	0.2 s	0.8 s
	30 KB	2.8 s	19.3 s	1.9 s	11.4 s
	60 KB	4.9 s	37.6 s	3.8 s	26.7 s
	120 KB	9.6 s	75.7 s	8.6 s	68.2 s

■ **CS1-H CPU Units, CJ1-H CPU Units, CJ1-R CPU Units, CJ2-H CPU Units, and CJ2M/CJ3M CPU Units**

File system		Memory Card		EM File Memory	
CPU Unit status	Operating mode	PROGRAM	RUN	PROGRAM	RUN
	Cycle time	---	20 ms	---	20 ms
Transfers using `put`	1 KB	0.5 s	2.7 s	0.2 s	0.6 s
	30 KB	1.8 s	11.6 s	0.7 s	6.6 s
	60 KB	3.2 s	21.1 s	1.5 s	14.0 s
	120 KB	6.2 s	40.2 s	3.6 s	32.5 s
Transfers using `get`	1 KB	0.2 s	0.3 s	0.2 s	0.2 s
	30 KB	1.7 s	4.8 s	1.0 s	4.1 s
	60 KB	2.5 s	9.4 s	2.3 s	9.7 s
	120 KB	4.9 s	18.8 s	4.9 s	27.0 s

Note

1. The above times assume that the Fixed Peripheral Servicing Time in the PLC Setup is set to the 4% value.
2. If the Fixed Peripheral Servicing Time in the PLC Setup is increased, FTP files will be transferred faster.

11-9 Host Computer Application Example

The following procedure provides an example of FTP operations from a host computer. In this example, the following assumptions are made.

- The IP address of the EtherNet/IP Unit or built-in EtherNet/IP port is registered in /etc/hosts on the host name as [cs1].
- The default FTP login name is being used (CONFIDENTIAL).
- A processing results data file called RESULT.IOM already exists on the Memory Card in the CPU Unit.
- A processing instructions data file called PLAN.IOM already exists on the workstation.

The following procedure transfers the processing results file RESULT.IOM from the Memory Card in the CPU Unit to the workstation and then the processing instructions file PLAN.IOM is transferred from the workstation to the Memory Card in the CPU Unit.

Underlined text is keyed in from the FTP client. The workstation prompt is indicated as $ and the cursor is indicated as ■.

1,2,3... 1. Start FTP and connect to the EtherNet/IP Unit or built-in EtherNet/IP port.

```
$ ftp cs1   ⋯   FTP started.
connected to cs1
220 **IPaddress** CS1W-ETN21 FTP server(FTP**version**)ready
Name(cs1:root): ■
```

2. Enter the login name.

```
Name(cs1:root):CONFIDENTIAL   ⋯   Login name
230 Guest logged in.
ftp> ■
```

3. Make sure the Memory Card is inserted. The MEMCARD directory will be displayed if there is a Memory Card in the CPU Unit.

```
ftp> ls   ⋯   Make sure the Memory Card is inserted.
200 PORT command successful.
150 opening data connection for ls(**IPaddress**port#**)(0 bytes).
MEMCARD
226 Transfer complete.
15 bytes received in 0 seconds(**bytes/s)
ftp> ■
```

4. Change to the MEMCARD directory.

```
ftp> cd MEMCARD  ⋯  Change to MEMCARD directory.
250 CWD command successful.
ftp> ■
```

5. Change data type to binary.

```
ftp> type binary  ⋯  Binary data type set.
200 Type set to I.
ftp> ■
```

6. Transfer the file RESULT.IOM to the workstation.

```
ftp> get RESULT.IOM  ⋯  File read.
200 PORT command successful.
150 opening data connection for result.iom (**IPaddress**port#**) (**bytes).
226 Transfer complete.
** bytes received in *.*** seconds (**bytes/s)
ftp> ■
```

7. Write the file PLAN.IOM to the Memory Card.

```
ftp> put PLAN.IOM  ⋯  File written
200 PORT command successful.
150 opening data connection for plan.iom (**IPaddress**port#**).
226 Transfer complete.
** bytes received in *.** seconds (**bytes/s)
ftp> ■
```

8. End FTP.

```
ftp> bye  ⋯  FTP ended.
221 Goodbye.
$ ■
```

SECTION 12
Automatic Clock Adjustment Function

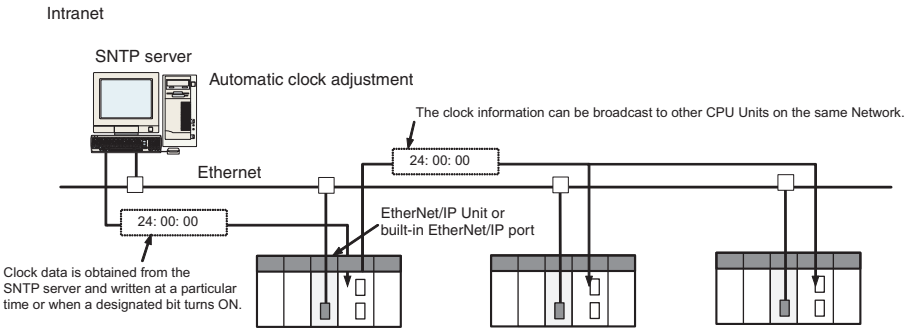
This section provides an overview of the automatic clock adjustment function, including details on specifications, required settings, operations from CX-Programmer, and troubleshooting.

12-1 Automatic Clock Adjustment 370
12-1-1 Overview 370
12-1-2 Specifications 371
12-2 Using the Automatic Clock Adjustment Function 371
12-2-1 Procedure 371
12-2-2 Settings Required for Automatic Clock Adjustment Function . 372
12-2-3 Auto Adjust Time 373
12-3 Automatic Clock Adjustment Switch 374
12-4 Automatic Clock Adjustment Error Processing 374
12-4-1 Automatic Clock Adjustment (SNTP) Errors 374
12-4-2 Error Log Error Codes for the Automatic Clock Adjustment Function 374

12-1 Automatic Clock Adjustment

12-1-1 Overview

The EtherNet/IP Unit or built-in EtherNet/IP port can obtain the clock information from the SNTP server (see note 1) at a particular time or when a designated bit turns ON and then refresh the internal clock information of the CPU Unit to which it is mounted (referred to as the local CPU Unit).



12-1-2 Specifications

Item	Specification	
Protocol	SNTP	
Port number	123 (UDP) Can also be set from the CX-Programmer in the Unit Setup.	
Adjustment timing	Automatic (fixed time) and manual (manual only cannot be set)	
Access to SNTP server	Writes the clock information from the SNTP server to the local CPU Unit.	Obtains the clock information from the SNTP server set up on the Network, and applies the information obtained to the local CPU Unit.
Refresh timing	When the automatic clock adjustment switch is turned from OFF to ON and at a specified time.	

12-2 Using the Automatic Clock Adjustment Function

12-2-1 Procedure

1,2,3...

1. Make the basic settings.
   Refer to *Initial Settings* on page 44.
2. With the CX-Programmer online, right-click the EtherNet/IP Unit or built-in EtherNet/IP port in the IO Table Dialog Box of the CX-Programmer, and select ***Edit - Unit Setup*** Set the following on the Auto Adjust Time Tab Page of the Edit Parameters Dialog Box.
   - SNTP server specification (required)
   - Access to the SNTP server is enabled when writing clock information from the SNTP server to the local CPU Unit when the Automatic Clock Adjustment Switch is turned from OFF to ON and at a set automatic adjustment time.
   - Automatic clock adjustment setting.
3. To perform automatic clock adjustment manually, turn the Automatic Clock Adjustment Switch from OFF to ON. (The Automatic Clock Adjustment Switch is word n bit 05 in the words allocated in the CPU Bus Unit Area, where n = CIO 1500 + (25 × unit number.)
4. Select ***Transfer to PLC*** from the PLC Menu and click the **Yes** Button. The Unit Setup (CPU Bus System Setup) will be transferred to the CPU Unit (the setting data will be transferred to the CPU Bus Unit System Setup Area).

12-2-2 Settings Required for Automatic Clock Adjustment Function

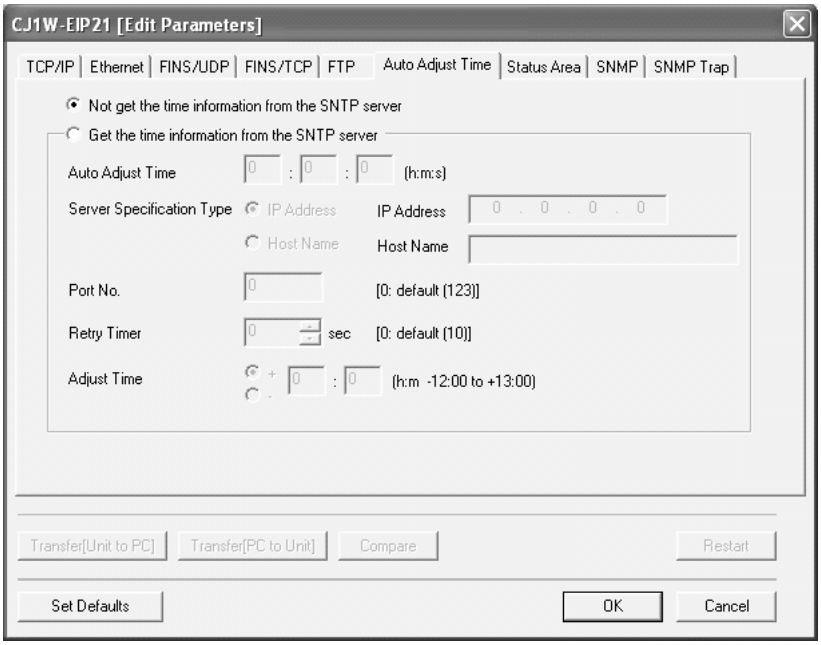
The following settings must be set in the Unit Setup when using the automatic clock adjustment function.

CX-Programmer tab	Settings	Setting conditions	Reference
Auto Adjust Time	Server Specification Type	Required.	*12-2-3 Auto Adjust Time* on page 373
	IP Address	One or the other is required, depending on the *Server specification type* setting.	
	Host Name		
	Port No.	Rarely required. (Change when a setting other than the default setting of 123 is required.)	
	Get the time information from the SNTP server	Required.	
	Auto Adjust Time	Optional	
	Retry Timer	Optional (Change when the default setting of 10 seconds is unacceptable.)	
	Adjust Time	Optional	
DNS (See note.)	IP Address	Required.	*3-8 TCP/IP and Link Settings* on page 66
	Port No.	Rarely required. (Change when a setting other than the default setting of 53 is required.)	
	Retry Timer	Optional (Change when the default setting of 10 seconds is unacceptable.)	

Note When the *Server specification type* field in Auto Adjust Time Tab is set to *Host name*.

12-2-3 Auto Adjust Time

The contents in the CPU Bus Unit System Setup that are set for using the automatic clock adjustment function are shown in the CX-Programmer's Edit Parameters Dialog Box.



Item	Contents	Default
Get the time information from the SNTP server	Enable to set the CPU Unit's clock to the time at the SNTP server's clock. The clock can be changed only for the CPU Unit to which the EtherNet/IP Unit or built-in EtherNet/IP port is mounted.	Not selected (disabled)
Auto Adjust Time	Set the time at which the SNTP server is to be accessed to synchronize the clocks. When the time that is set here arrives, the SNTP server is accessed and the CPU Unit clock is adjusted to match the SNTP server clock.	0:0:0
Server Specification Type	Select whether the SNTP server used for automatic clock adjustment is to be specified by IP address or by host domain name (i.e., by host name).	IP Address
IP Address	Set the IP address for the SNTP server that is to be used for automatic clock adjustment. This setting is enabled only when server specification by IP address has been selected.	0.0.0.0
Host Name	Set the host domain name (i.e., the host name) for the SNTP server that is to be used for automatic clock adjustment. This setting is enabled only when server specification by host name has been selected.	None
Port No.	Set the port number for connecting to the SNTP server that is to be used for automatic clock adjustment. This setting does not normally need to be changed.	0 (Number 123 is used.)

Item	Contents	Default
Retry Timer	Set the time to elapse before retrying when a connection to the SNTP server fails. This setting does not normally need to be changed.	0 (10 s)
Adjust Time	This sets in the CPU Unit's clock data the time difference made up from the SNTP server's clock data. To use the clock data from the SNTP server just as it is, input 0.	+0:0

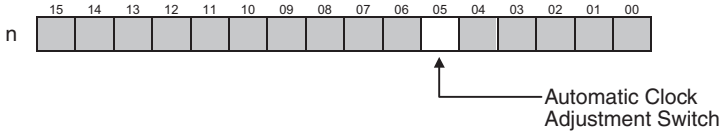
12-3 Automatic Clock Adjustment Switch

The Automatic Clock Adjustment Switch is allocated in the CIO Area as shown below. The first word n of the CIO Area is calculated using the following equation.

n = CIO 1500 + (25 × unit number)

Automatic Clock Adjustment Switch (Bit 05 of n)

The Unit control bit is shown in the following diagram.



When the Automatic Clock Adjustment Switch turns from OFF to ON, the EtherNet/IP Unit or built-in EtherNet/IP port obtains the clock data from the SNTP server on the network, and applies it to the local CPU Unit. After applying the data, the switch automatically turns OFF again.

12-4 Automatic Clock Adjustment Error Processing

12-4-1 Automatic Clock Adjustment (SNTP) Errors

The following table shows the main causes and remedies for errors that occur in the automatic clock adjustment function (SNTP).

Cause	Correction
SNTP, DNS server address not set	Reset each server address (IP address or host name).
SNTP, DNS server communications timeout	Inspect the communications path (EtherNet/IP Unit or built-in EtherNet/IP port, cable connections, hub, router, server), and correct the situation that is causing the error.
CPU Unit internal clock could not be set	The automatic clock adjustment function is not supported by certain CPU Units (models, lot numbers) if they are in RUN or MONITOR mode.

12-4-2 Error Log Error Codes for the Automatic Clock Adjustment Function

When an error occurs while the EtherNet/IP Unit or built-in EtherNet/IP port is operating, the error code, detailed error code, and time the error occurred are saved in the error log. The following table provides a list of the error codes.

The error log can be read by sending FINS commands to the EtherNet/IP Unit or built-in EtherNet/IP port.

Error code	Meaning	Detailed error code		Correction	EEPROM
		1st byte	2nd byte		
03C1	Server setting error	00H: DNS 03H: SNTP 04H: FTP 06H: BOOTP 07H: SNMP 08H: SNMP Trap 09H: FINS/UDP 0AH: FINS/TCP	01: IP address 02: Host name 03: Port number 04: Other parameters	Set the server settings correctly based on the information in the detailed error code.	---
03C4	Server connection error	00H: DNS 03H: SNTP 04H: FTP 06H: BOOTP 07H: SNMP 08H: SNMP Trap	01: Specified host does not exist 02: No service at specified host 03: Timeout 04: Closed unilaterally by host 05: Cannot connect because account information does not match 06: Host name resolution error 07: Transmission error 08: Reception error 09: Other error 0AH: Error in obtained IP address	Take either of the following measures. • Correct the settings for each server. • Inspect the communications path (EtherNet/IP Unit or built-in EtherNet/IP port), cable connections, hub, router, server), and correct the situation that is causing the error.	---
03C6	Clock data write error	0001: Clock data could not be refreshed because of a CPU Unit error.		Clear the CPU Unit error.	---
		0002: Clock data could not be refreshed because the CPU Unit could not write clock data in that operation mode.		The automatic clock adjustment function is not supported by certain CPU Units (models, lot numbers). (See notes 2 to 4.)	---

Note (1) For details on other error log information, refer to *SECTION 16 Modbus Client Function*.

(2) An error will occur in the following CPU Units when the automatic clock adjustment function is executed under the conditions shown in the table.

CPU Unit	Conditions
CPU Units manufactured on or before January 31, 2003 (lot numbers 030131 or earlier): CJ1G-CPU□□H CJ1H-CPU□□H CS1G-CPU□□H CS1H-CPU□□H	When the CPU execution mode is set to other than normal mode (priority peripheral servicing mode, parallel processing with synchronous memory access mode, or parallel processing with asynchronous memory access mode). AND When the CPU Unit operating mode is set to RUN or MONITOR mode.

(3) The manufacturing date can be determined from the lot number on the side or top corner of the CPU Unit.

(4) The lot numbers are as follows:
YYMMDD, in which YY indicates the last two digits of the year, MM the month, and DD the day.

(5) For the CS1W/CJ1W-EIP21, CJ2H-CPU6□-EIP, and CJ2M-CPU3□, automatic adjustment will become no longer possible from February 7, 2036, due to the specifications of the SNTP protocol. With the EtherNet/IP Unit (built-in port), this function will no longer operate from February 7, 2036 (not displayed as error information).

SECTION 13
Security Functions

This section describes the security functions provided by CS1W/CJ1W-EIP21S EtherNet/IP Units.

13-1 Overview of Security Functions 378
13-1-1 List of Security Functions 378
13-2 Secure Communications 380
13-2-1 Function Overview 380
13-2-2 Function Details 380
13-3 User Authentication 385
13-3-1 Function Overview 385
13-3-2 Function Details 385
13-4 Opening and Closing the Port 403
13-4-1 Function Overview 403
13-4-2 Function Details 403
13-4-3 Protocols for Sending Automatically 407
13-5 IP Packet Filtering 408
13-5-1 Function Overview 408
13-5-2 Function Details 408
13-6 Operation Log 415
13-6-1 Function Overview 415
13-6-2 Function Details 415
13-7 General Security Use Cases 424
13-7-1 Use Cases. 424
13-7-2 Case 1: Permitting Packet Reception for Specific Protocols. . 424
13-7-3 Case 2: Permitting Packet Reception from Specific Source IP Addresses. 425
13-8 Protective Measures to Prevent Security Threats 427

13-1 Overview of Security Functions

This section provides an overview of security functions provided by CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ EtherNet/IP Units.

13-1-1 List of Security Functions

CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ EtherNet/IP Units provide a set of security functions that are intended to protect user assets from network access.

These functions protect user programs and various data stored in the CPU Unit.

The functions can also be used to restrict operations from Support Software in order to prevent malfunction.

Function name	Function overview	Reference
Secure communications *1	Ensure the confidentiality and integrity of communications lines that provide access from Support Software to critical data in the CPU Unit.	*13-2 Secure Communications*
User authentication *1	Permits only the specified users to perform online operations from Support Software and restricts the online operations based on the operation authority set for each user.	*13-3 User Authentication*
Opening and closing the port	Blocks and allows packets to pass through the TCP/UDP ports assigned to individual communications functions according to the settings.	*13-4 Opening and Closing the Port*
IP packet filtering	Selectively permits packets that EtherNet/IP ports to receive to pass through the filter according to the preset conditions.	*13-5 IP Packet Filtering*
Operation log *1	Records important operations and results of users who connect online using secure communications, along with information on the date and time, computer's IP address, and user name.	*13-6 Operation Log*

*1 When connected to the CP1H CPU Units, the CX-Programmer and PLC backup tools cannot use the corresponding functions.

Refer to *13-7 General Security Use Cases* for the configuration example and settings for each use case.

Supported EtherNet/IP Units

EtherNet/IP Units
CS1W-EIP21S, CJ1W-EIP21S, CJ3M-CPU☐

Supported Support Software

The following Support Software is supported.

Support Software	Version	
	CS1W-EIP21S CJ1W-EIP21S	CJ3M-CPU3☐
CX-Programmer	Ver. 9.81 or higher	Ver. 9.90 or higher
PLC Backup Tool	Ver. 1.03 or higher	Ver. 1.06 or higher
EIP21S User Management Tool*1	Ver. 1.0 or higher	Ver. 1.0 or higher

*1 If the OS of your PC is earlier than Windows 10, you cannot either install the EIP21S User Management Tool or select Secure Comm in the CX-Programmer and the PLC Backup Tool.
If the Windows 10 version is earlier than 1803, you cannot either go online by Secure Comm or use the function derived from Secure Comm.

In this section, the above Supported Software is mentioned by name without version information.

Supported CPU Units

The following CPU Units are supported.

CPU Units
CJ3 CPU Units (CJ3M-CPU☐☐)
CJ2 CPU Units*1 (CJ2H-CPU☐☐, CJ2H-CPU☐☐-EIP, CJ2M-CPU☐☐)
CJ1G-P CPU Unit (CJ1G-CPU4☐P)
CS1-H CPU Units (CS1G/H-CPU☐☐H)
CS1D Duplex System CPU Units (CS1D-CPU☐☐HA/H, CS1D-CPU☐☐SA/S, CS1D-CPU☐☐P)
CP1H CPU Units (CP1H-X40D☐-☐, CP1H-XA40D☐-☐, CP1H-Y20DT-D)

*1 The built-in EtherNet/IP ports of CJ2H-CPU6☐-EIP/CJ2M-CPU3☐ CPU Units do not support connections using secure communications.

Note There are no restrictions on security functions due to the unit versions of the CPU Units.

13-2 Secure Communications

This section describes the secure communications function.

Note To improve security, we recommend installing the CX-One on a computer installed with a supported version of Microsoft Windows OS.

13-2-1 Function Overview

Secure communications ensure the confidentiality and integrity of communications lines that provide access from Support Software to critical data in the CPU Unit for improved system's security performance.

The secure communications function is intended for applications where Support Software must be connected to the CPU Unit via an unreliable network such as Internet connections.

This means that you cannot use secure communications when connecting Support Software to the CPU Unit via a USB or peripheral port.

To use secure communications, you must save the user authentication settings to the EtherNet/IP Unit or built-in EtherNet/IP port in advance using the EIP21S User Management Tool.

Note

(1) If the OS of your PC is earlier than Windows 10, you cannot either install the EIP21S User Management Tool or select Secure Comm in the CX-Programmer and the PLC Backup Tool.
If the Windows 10 version is earlier than 1803, you cannot either go online by Secure Comm or use the function derived from Secure Comm.

(2) When connected to the CP1H CPU Units, the CX-Programmer and PLC backup tools cannot use the corresponding functions.

13-2-2 Function Details

Settings

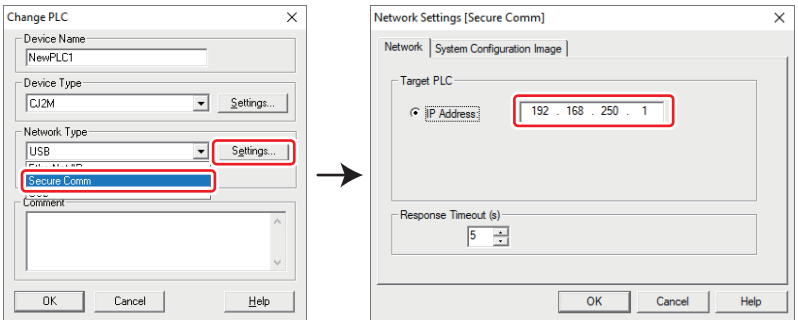
CX-Programmer

Make the following settings in the Change PLC Dialog Box.

Setting	Description (See note 1.)
Device Type	Select the type of the CPU Unit to connect to.
Network Type	• Select *Secure Comm*. • Click the **Settings** Button and enter the IP address of the EtherNet/IP Unit or built-in EtherNet/IP port to connect to in *IP Address* in *Target PLC*.

Note

(1) Even if you select CJ2H-CPU6□-EIP/CJ2M-CPU3□ in *Device Type*, you can select *Secure Comm* in *Network Type*. However, this will not allow you to connect online with the Unit even if you set the IP address of its built-in EtherNet/IP port because of a communications error in the Support Software.

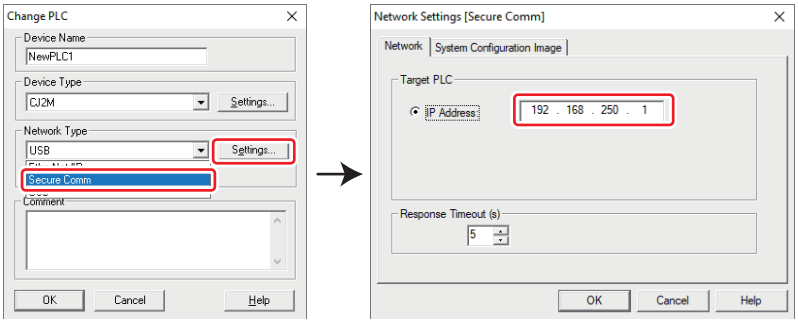


PLC Backup Tool

Make the following settings in the Change PLC Dialog Box of the PLC Backup Tool.

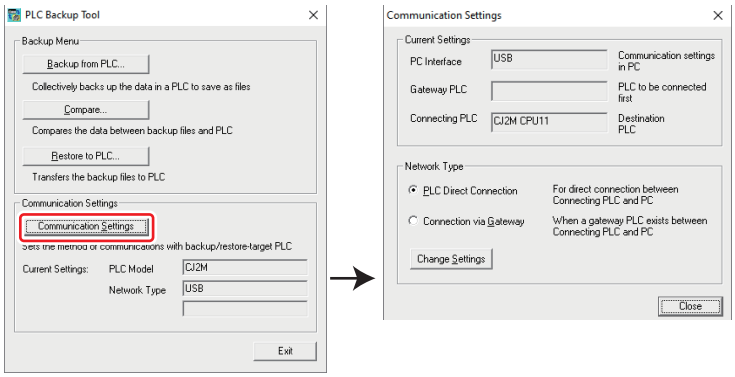
Setting	Description (See note 1.)
Device Type	Select the type of the CPU Unit to connect to.
Network Type	• Select *Secure Comm*. • Click the **Settings** Button and enter the IP address of the EtherNet/IP Unit or built-in EtherNet/IP port to connect to in *IP Address* in *Target PLC*.

Note (1) Even if you select CJ2H-CPU6□-EIP/CJ2M-CPU3□ in *Device Type*, you can select *Secure Comm* in *Network Type*. However, this will not allow you to connect online with the Unit even if you set the IP address of its built-in EtherNet/IP port because of a communications error in the Support Software.

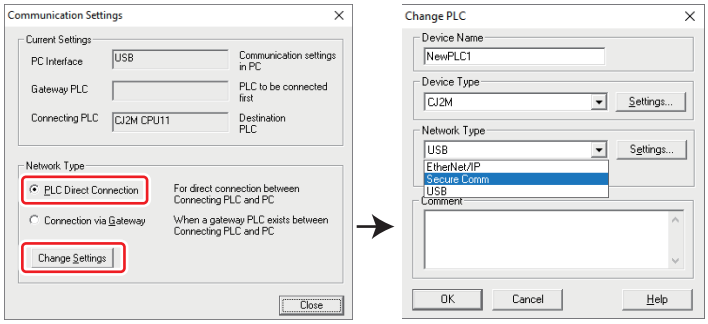


To open the Change PLC Dialog Box of the PLC Backup Tool, follow the steps below.

1,2,3... 1. Click the **Communication Settings** Button in the PLC Backup Tool Dialog Box to open the Communication Settings Dialog Box.



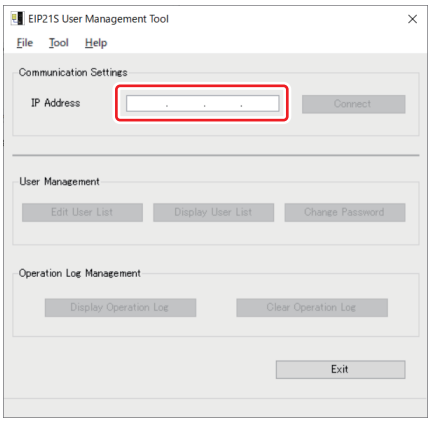
2. Click the **Change Settings** Button with the *PLC Direct Connection* Option selected in the Communication Settings Dialog Box.



Note If you select the *Connect via Gateway* Option instead of *PLC Direct Connection* in the Communication Settings Dialog Box, you cannot select *Secure Comm*.

EIP21S User Management Tool

In the *Communication Settings* group in the EIP21S User Management Tool Dialog Box, enter the IP address of the EtherNet/IP Unit or built-in EtherNet/IP port to connect to in *IP Address*.



Note To use secure communications, you must save the user authentication settings of the users who are permitted to connect, such as the user names and passwords, in the EtherNet/IP Unit or built-in EtherNet/IP port in advance. Refer to *13-3 User Authentication* for information on the user authentication settings.

Procedure

CX-Programmer

With the settings made as described in *Settings*, select ***Work Online*** from the PLC Menu to connect online.

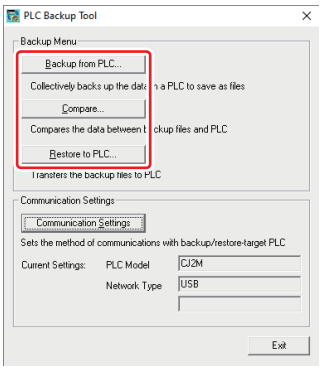
Refer to the *CX-Programmer Operation Manual* (Cat. No. W446) for information on how to connect online.

After this, you will be subject to user authentication and, if successful, go online with the EtherNet/IP Unit. Refer to *13-3 User Authentication* for information on user authentication.

Note The secure communications function does not provide the automatic online connection feature.

PLC Backup Tool

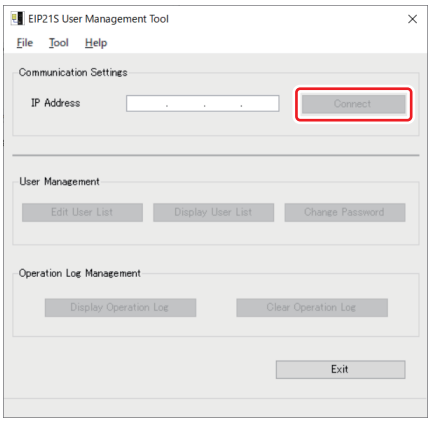
With the settings made as described in *Settings*, select one of the *Backup Menu* buttons in the PLC Backup Tool to connect online.



After this, you will be subject to user authentication and, if successful, go online with the EtherNet/IP Unit. Refer to *13-3 User Authentication* for information on user authentication.

EIP21S User Management Tool

With the settings made as described in *Settings* above, click the **Connect** Button in the *Communication Settings* group to connect online.



After this, you will be subject to user authentication and, if successful, go online with the EtherNet/IP Unit. Refer to *13-3 User Authentication* for information on user authentication.

When online, the *IP Address* setting in the *Communication Settings* group will be grayed out.

Specifications

Conditions for Communications Using Secure Comm

The following are conditions under which communications using Secure Comm are possible.

A. The connected CPU Unit has a EtherNet/IP Unit or built-in EtherNet/IP port that belongs to an Ethernet network.

B. One of the following Support Software is used to make connection settings for secure communications.
CX-Programmer
PLC Backup Tool
EIP21S User Management Tool

C. User authentication settings are stored in the connected EtherNet/IP Unit or built-in EtherNet/IP port.

The following is an example of conditions under which communications using Secure Comm are not possible.

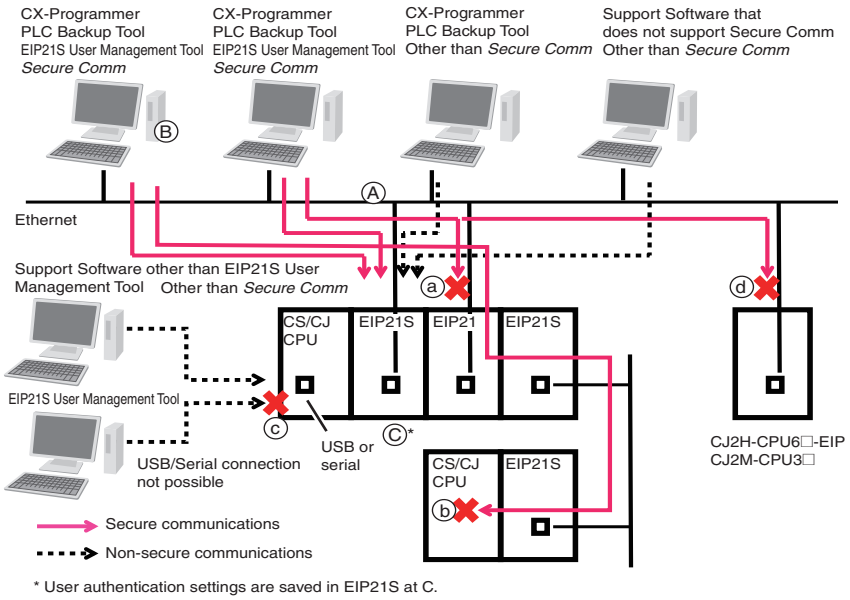
a. The connection destination is an EtherNet/IP Unit other than CS1W/CJ1W-EIP21S,CJ3M-CPU3☐, or an Ethernet Unit.

b. The connection destination is located in a different network (beyond the allowable level of transparency).

c. The connection destination has a USB, peripheral, or serial port.

d. The connection destination is a CJ2H-CPU6☐-EIP/CJ2M-CPU3☐ CPU Unit with a built-in EtherNet/IP port.

Note For the EIP21S User Management Tool, if the OS of your PC is a Windows 10 version of earlier than 1803, you cannot either go online by Secure Comm or use the function derived from Secure Comm.



* User authentication settings are saved in EIP21S at C.

Number of Simultaneous Connections for Secure Communications

The secure communications function allows for connecting up to 64 nodes simultaneously to a EtherNet/IP Unit or built-in EtherNet/IP port.

If you attempt to connect online with more than the maximum number of nodes, a communications error will occur in the Support Software.

The number of nodes here means the number of the connected IP addresses.

13-3 User Authentication

This section describes the user authentication function.

13-3-1 Function Overview

User authentication permits only the specified users to perform online operations from Support Software and restricts the online operations based on the operation authority set for each user.

This improves the security performance of the system.

This function is available only when the EtherNet/IP Unit is connected using the secure communications function.

Note

(1) Secure Comm will not allow you to connect online with the CPU Unit due to an authentication failure if the user name and password do not match. Make a note of the user name and password. If you forget them, follow the troubleshooting procedure to clear the authentication settings. Note that this will restore the factory default settings.
Refer to *What to Do If You Forget Administrator Account Information* for information on the troubleshooting procedure.

(2) When connected to the CP1H CPU Units, the CX-Programmer and PLC backup tools cannot use the corresponding functions.

13-3-2 Function Details

When using the secure communications function from Support Software to connect online with the CPU Unit, you will be asked to enter your user name and password. If the user name and password match the preset ones, the authentication is successful and you will go online. If the authentication fails, you will go offline.

The user name and password used for the last online connection are not stored anywhere in the Support Software.

If the CX-Programmer or EIP21S User Management Tool is online and has not been operated for a certain period of time, the Support Software will interrupt the communications and generate a communications error. For details, refer to *User Authentication Timeout*.

On the other hand, the PLC Backup Tool requires an online connection every time you perform backup, comparison, or restore operation. It goes offline automatically when the operation is completed. For this reason, the PLC Backup Tool does not monitor the time during which it is not operated online.

Users are assigned one of the following types of operation authority: Administrator, Designer, or Operator. Each user is allowed to operate the CPU Unit online within the range of the assigned authority. Refer to *Operation Authority* for details on the operation authority.

The user name, password, operation authority, and other user authentication settings are stored in the EtherNet/IP Unit or built-in EtherNet/IP port. They are not stored in the CX-Programmer or other Support Software. This enables users to establish online connections according to the settings stored in individual EtherNet/IP Unit or built-in EtherNet/IP port, independent of the computers that they use.

Use the EIP21S User Management Tool to make the user authentication settings. For details on the operation, refer to the information that can be accessed from the Help menu of the EIP21S User Management Tool.

Note The user registration of the administrator, addition and deletion of users, and change of operation authority must be performed by a person responsible for the management of the target PLC system.

Settings

After the user authentication settings are configured, user authentication can be performed.

User Authentication Setting

■ First Administrator Registration

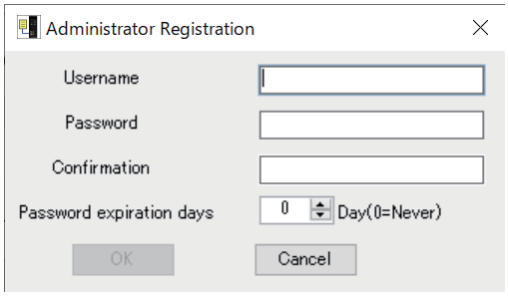
This operation is performed by a person responsible for management of the target PLC system.

EIP21S EtherNet/IP Units are shipped from the factory with the user authentication settings initialized. Therefore, when connecting online for the first time, first register the administrator using the EIP21S User Management Tool, and then register other users.

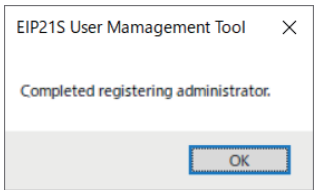
With the user authentication settings initialized, you cannot connect the CX-Programmer and PLC Backup Tool online using secure communications.

1,2,3...

1. Using the EIP21S User Management Tool, connect online to the CEtherNet/IP Unit or built-in EtherNet/IP port.
   Enter the IP address of the Unit to connect to in *IP Address* in the *Communication Settings* group, and click the **Connect** Button.
   The Administrator Registration Dialog Box is displayed.



2. Enter the administrator's user name, password, and password expiration days and click the **OK** Button.
   A notification dialog box will be displayed to notify you of the completion of the administrator registration.



Click the **OK** Button. You are now offline.

3. With the user name and password registered in step 2, connect online to the EtherNet/IP Unit as the administrator.
   You are now online.

4. Register user data for other users.

■ **User Management**

This operation is performed by the administrator using the EIP21S User Management Tool.

The administrator can add or delete accounts, change the type of authority, or reset a lost or leaked password.

For adding and deleting accounts, changing user names, changing passwords, changing permissions, and other operations, refer to *User Authentication Using the EIP21S User Management Tool*.

■ **Password Change**

This operation is performed by individual users using the EIP21S User Management Tool.

The initial password for each user has been set by the administrator at the time of user registration. If necessary, each user should connect online with the EtherNet/IP Unit using his or her own account and change the password.

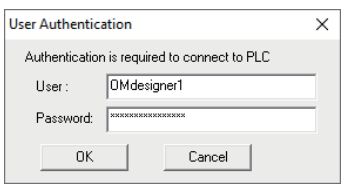
For details on the operation, refer to the information that can be accessed from the Help menu of the EIP21S User Management Tool.

Procedure

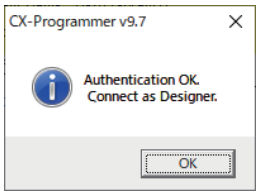
User Authentication Using the CX-Programmer or PLC Backup Tool

1,2,3...

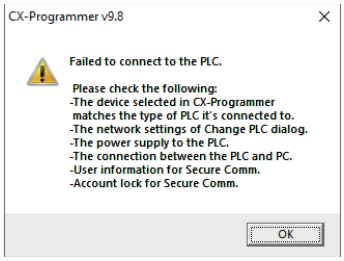
1. Connect the Support Software online.
2. Enter your user name and password.



If the authentication is successful, your operation authority will be displayed with authentication OK.



If the authentication fails, an authentication failure message will be displayed.

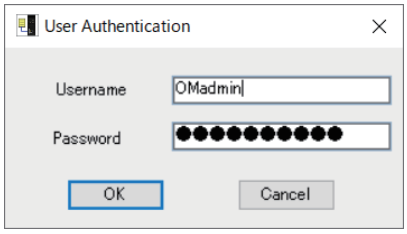


Refer to the *CX-Programmer Operation Manual* (Cat. No. W446) for details on how to connect the Support Software online.

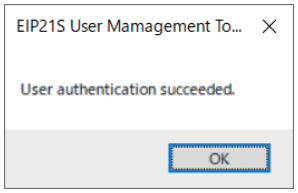
User Authentication Using the EIP21S User Management Tool

1,2,3...

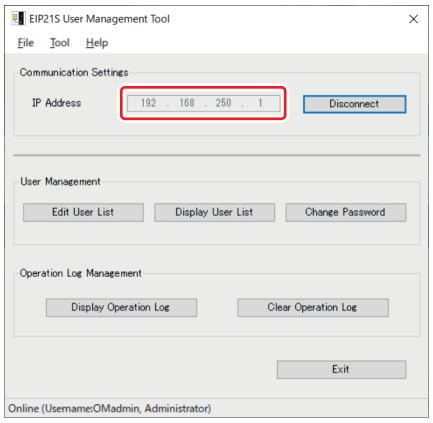
1. Connect the Support Software online.
2. Enter your user name and password.



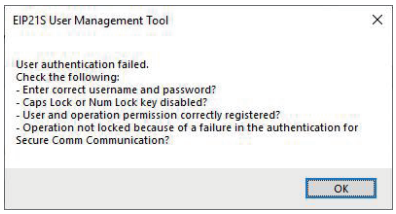
If the authentication is successful, a notification dialog box will be displayed to notify you of the success of the user authentication.



Click the **OK** Button. The *IP Address* setting in the *Communication Settings* group will be grayed out.



If the authentication fails, after the following message box, the User Authentication Dialog Box will be displayed again to prompt for re-authentication.

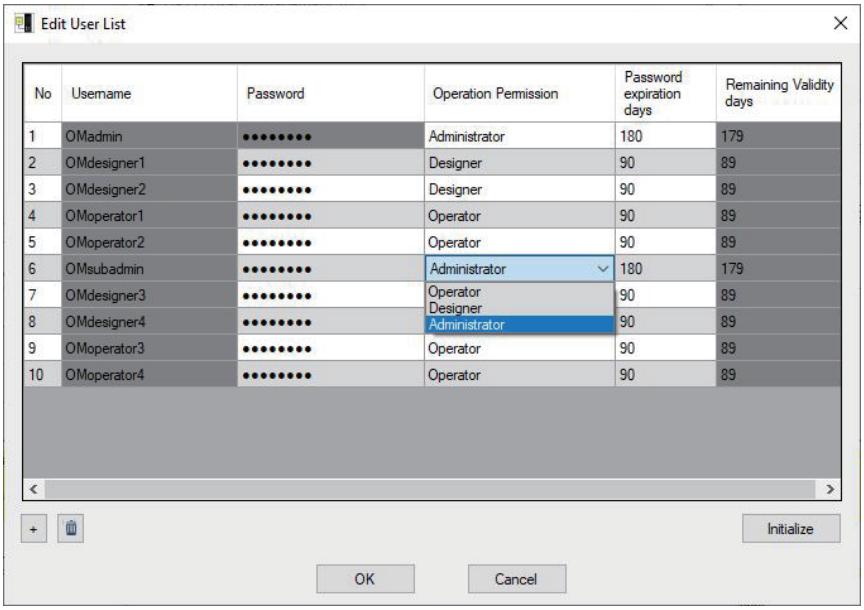


Editing and Checking the User Authentication Settings

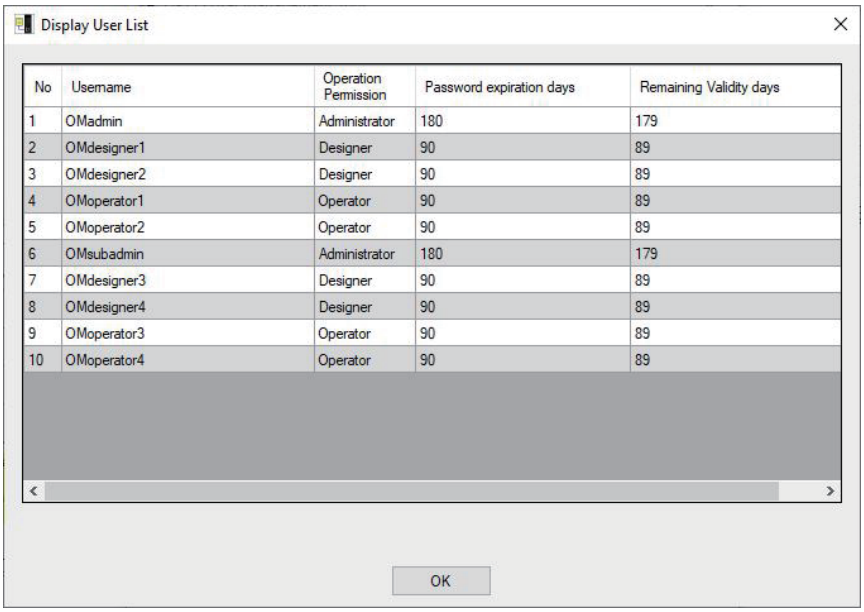
Using the EIP21S User Management Tool, connect online to the EtherNet/IP Unit or built-in EtherNet/IP port.

The following dialog boxes are used.

Edit User List Dialog Box



Display User List Dialog Box



The remaining number of password expiration days is displayed in **Remaining Validity days**.

The number 0 shows that it will expire within 24 hours.

The number -1 shows that it has expired.

For details on the operation, refer to the information that can be accessed from the Help menu of the EIP21S User Management Tool.

Adding Accounts

This operation is performed by users who have the Administrator operation authority in the Edit User List Dialog Box of the EIP21S User Management Tool.

After completing the settings, click the **OK** Button to transfer the settings to the EtherNet/IP Unit or built-in EtherNet/IP port that is online. The settings will be reflected immediately and enabled after completion of the transfer.

Deleting Accounts

This operation is performed by users who have the Administrator operation authority in the Edit User List Dialog Box of the EIP21S User Management Tool.

After completing the settings, click the **OK** Button to transfer the settings to the EtherNet/IP Unit or built-in EtherNet/IP port that is online. The settings will be reflected immediately and enabled after completion of the transfer.

When a user is online, another user who has the administration authority may delete the account of that user.

In this case, a communications error will occur in the Support Software used by the user whose account was deleted. To connect online to the EtherNet/IP Unit again, the user must use an account different from the deleted account, or add a new account.

Note that you cannot delete your own account online in the Edit User List Dialog Box. To delete the account, you must ask someone who has the Administrator operation authority.

Checking Accounts

This operation is performed by users who have the Administrator or Designer operation authority in the Display User List Dialog Box of the EIP21S User Management Tool.

In this dialog box, they can check the user names, operation authority, and password expiration days of all the accounts registered in the EtherNet/IP Units or built-in EtherNet/IP ports that are online.

This allows the designer to know who has the Administrator operation authority and ask him or her to add or delete users.

The administrator can use the information of all listed users to determine whether or not accounts are required for them, and review the information as needed.

Changing User Names

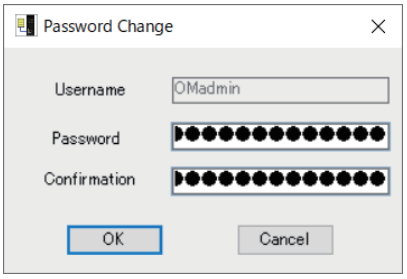
The EIP21S User Management Tool does not allow you to change the user name of your account.

To change the user name, you must delete the existing account and then add a new one.

Changing Passwords

All users are allowed to change their own passwords in the Password Change Dialog Box of the EIP21S User Management Tool.

Password Change Dialog Box



After completing the settings, click the **OK** Button. The changes are reflected immediately and enabled. Then, the EIP21S User Management Tool changes from online to offline.

This function allows users to change the initial passwords set by the administrator.

Note If you enter the same password as the current one for a new password, an error will occur. Enter a different password.

It is also possible to change the passwords of multiple users at once. This operation is performed by users who have the Administrator operation authority in the Edit User List Dialog Box of the EIP21S User Management Tool.

After completing the settings, click the **OK** Button to transfer the settings to the EtherNet/IP Unit or built-in EtherNet/IP port that is online. The settings will be reflected immediately and enabled after completion of the transfer.

This function allows the administrator to change the password of a certain user, or set the initial passwords for all users.

When a user is online, another user who has the Administrator operation authority may change the password of that user.

In this case, a communications error will occur in the Support Software used by the user whose password was changed. To connect online to the EtherNet/IP Unit again, the user must use the changed password.

Note that you cannot change the password of your own account online in the Edit User List Dialog Box. To change your own password, use the Password Change Dialog Box.

Changing Authority

This operation is performed by users who have the Administrator operation authority in the Edit User List Dialog Box of the EIP21S User Management Tool.

After completing the settings, click the **OK** Button to transfer the settings to the EtherNet/IP Unit or built-in EtherNet/IP port that is online. The settings will be reflected immediately and enabled after completion of the transfer.

When a user is online, another user who has the Administrator operation authority may change the operation authority of that user.

In this case, the user whose operation authority was changed remains online and has the operation authority before the change in the Support Software. The user will have the operation authority after the change when he or she connects online again.

Note that you cannot change the operation authority of your own account online in the Edit User List Dialog Box. To change the operation authority, you must ask someone who has the Administrator operation authority.

Setting of Password Expiration Days

This operation is performed by users who have the Administrator operation authority in the Edit User List Dialog Box of the EIP21S User Management Tool.

After completing the settings, click the **OK** Button to transfer the settings to the EtherNet/IP Unit or built-in EtherNet/IP port that is online. The settings will be reflected immediately and enabled after completion of the transfer.

However, even if the password expiration days have passed when the user is online, the status will stay online.

Initializing User Authentication Settings

This operation is performed by users who have the Administrator operation authority in the Edit User List Dialog Box of the EIP21S User Management Tool.

If this operation is performed, the user authentication settings for all users, including the administrator, stored in the EtherNet/IP Unit or built-in EtherNet/IP port that is online will be deleted and the Unit will be reset to the defaults.

When a user is online, another user who has the Administrator operation authority may initialize the user authentication settings.

In this case, a communications error will occur in the Support Software used by the user who is online.

Specifications

User Authentication Setting

The user authentication settings are as shown below.

Use the EIP21S User Management Tool to make the user authentication settings.

EtherNet/IP Unit or built-in EtherNet/IP port stores the user authentication settings in its own nonvolatile memory.

Up to 64 users can be registered.

Setting	Setting range
Username	Number of characters: 1 to 16, blank (NULL) by default in EIP21S User Management Tool Dialog Box
	Available characters: Single-byte alphanumeric, case-sensitive
Password	Number of characters: 8 to 32, blank (NULL) by default in EIP21S User Management Tool Dialog Box
	Available characters: Single-byte alphanumeric, case-sensitive
Operation Permission	Select one of the following types of authority (*Administrator* by default) *Administrator*, *Designer*, *Operator*
Password expiration days*1	Set 0 to 999 0: Indefinite period 1 to 999: Expiration days

*1 The password validity period is a period until the days of password expiration setting passes after the last password update date.

Switching Users

You cannot switch from one account to another while the Support Software remains online.

To switch your account while the Support Software online, you need to once go offline.

Password Expiration Days

If the remaining expiration days are less than 15 days, the Support Software will prompt you to change the password when you go online and will become online.

If you go online when the password expiration days have passed, the Support Software will make notification as follows:

■ **For EIP21S User Management Tool**

It displays the Password Change Dialog Box.

If the user changes the password, it will become online.

If the user presses **Cancel** in the Password Change Dialog Box, it will become offline.

■ **For Support Software other than EIP21S User Management Tool**

It displays the dialog box notifying that the password expiration days have passed and becomes offline.

Performing the following operation will update the last password update date to the time of the CPU Units when that operation is done.

a. The administrator changes and transfers the password in the Edit User List Dialog Box.

b. The user changes and transfers the password in the Password Change Dialog Box.

c. Restoring the backup file including the user authentication settings

Note: It is the user of the changed password in the case of a or b and all the users included in the backup file in the case of c that the last password update date is updated for.

Note In order to use the password expiration days properly, set the CPU Unit's clock.
In the following cases, the password expiration days may be shorter than the set days.

- The time of the CPU Unit's clock was changed.
- The battery of the CPU Units was exhausted.
- Battery-free operation is used for the CPU Units.
- The CPU Units were left for 5 minutes or more in a battery-less and a none-nergized state (at an ambient temperature of 25°C).

Note For CJ3/CJ2 CPU Units, if the battery is discharged or the unit is operated without a battery, timekeeping starts from 00:00:00 on January 1, 2000, after the built-in capacitor discharges.

Simultaneous Online

You can use multiple accounts at the same time to go online with a single EtherNet/IP Unit or built-in EtherNet/IP port

Also, you can use the same account to establish multiple online connections from Support Software running on multiple computers.

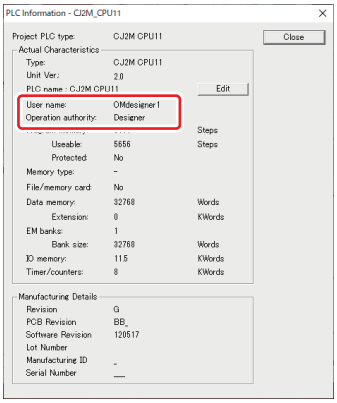
The maximum number of computers (IP addresses) that can be online simultaneously is 64.

Refer to *13-2 Secure Communications* for information on the number of simultaneous connections.

Displaying Online Users

With the CX-Programmer, an online user can check the user name and operation authority of his or her own account in the PLC Information Dialog Box.

However, this user cannot check the account information on users who are online using other accounts.



Locking Account

If you enter a wrong password 5 times in a row in user authentication with a user name and password, "Online connection failed" is recorded in the operation log and that account is locked for 10 minutes. If you try to go online with the locked account, the Support Software will display the dialog box notifying that the account is locked and will become offline.

If the account is locked when a certain user is online, the Support Software that is online with that account will encounter a communications error. To place the Support Software online again, once go offline, and then wait for the account to be unlocked, or connect that online with another account.

For the EtherNet/IP Unit or built-in EtherNet/IP port, cycling the power supply or restarting it will reset the number of login failures and unlock the account.

If the administrator changes the password for a locked account, the account will be unlocked.

What to Do If You Forget Administrator Account Information

If you forget the user ID or password of your administrator account, ask someone who has the Administrator operation authority to check the account information.

If there is no one who has the Administrator operation authority, you must initialize the EtherNet/IP Unit or built-in EtherNet/IP port to the defaults.

In this case, you will end up redoing all settings of the Unit, including user authentication settings, from scratch since they have been lost due to initialization. Keep the administrator account information strictly confidential.

The following methods are available to initialize your EtherNet/IP Unit to the defaults. Method A is recommended for security reasons.

A. Initialize the Unit from the Support Software connected to the USB, peripheral, or serial port of the CPU Unit.

B. Initialize the Unit from the Support Software connected via Ethernet without using secure communications.

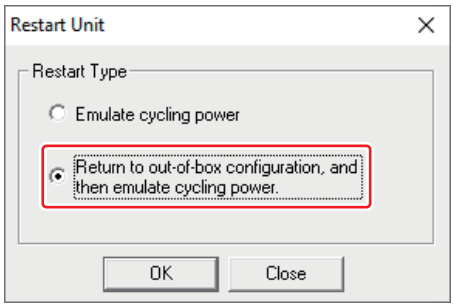
In either case, you must restart the Unit after initializing the Unit to the defaults.

To restart the EtherNet/IP Unit after restoring the factory default settings with the CX-Programmer, follow the steps below.

1,2,3...

1. Click the **Restart** Button in the Edit Parameters Dialog Box and, in a confirmation dialog box for restart, click the **Yes** Button.
   The Restart Unit Dialog Box is displayed.

2. Select *Return to out-of-box configuration, and then emulate cycling power*. and click the **OK** Button.



Note

(1) Be aware that the above Method B is for connection via a network that does not use secure communications or user authentication. For this reason, use it only in a network installed with security measures other than the security functions provided by EtherNet/IP Unit or built-in EtherNet/IP port, such as a firewall.

(2) Depending on the settings of opening and closing the port or IP packet filtering, your connection attempts may fail. Determine the settings for EtherNet/IP Unit or built-in EtherNet/IP port in consideration of such cases. Refer to *13-4 Opening and Closing the Port* and *13-5 IP Packet Filtering* for details on these functions.

Error Detection for User Authentication Settings

If saving the user authentication settings to non-volatile memory fails due to a power interruption or malfunction caused by external noise, at the next power ON, the user will be notified of the fact that the saving has failed.

The notification method is as follows.

- The Unit registers the error code in the error log and displays the error code on the 7-segment display. (Refer to *SECTION 16 Modbus Client Function*.)
- The error is reflected in the status of the flags in the allocated CIO area words. (Refer to *Unit Status 2 (EtherNet/IP Unit to CPU Unit) (n + 11)* in *4-2-2 Details of the Allocated CIO Area Words*.)
- Error message is displayed when the EIP21S User Management Tool is connected online.

If saving the user authentication settings fails, the EtherNet/IP Unit or built-in EtherNet/IP port operates on the assumption the user authentication settings are the defaults. In this case, redo the user authentication setting procedure from the first administrator registration.

Operation Authority

Each user is allowed to operate the CPU Unit online within the range of the assigned authority.

Be sure to assign one of the following types of operation authority to each user.

Type	Authority overview
Administrator	The administrator can add and delete users and change their operation authority using the EIP21S User Management Tool. For the CX-Programmer and the PLC Backup Tool, this user can perform the same operations as the designer.
Designer	The designer can check the user list and change his or her own password using the EIP21S User Management Tool. This user can perform almost all operations of the CX-Programmer and all operations of the PLC Backup Tool.
Operator	The operator can change his or her own password using the EIP21S User Management Tool. Among the operations of the CX-Programmer, this user can get data from the PLC. However, this user cannot write data to the PLC.

Note

There are no restrictions on operations due to operation authority when users are offline.
When secure communications are not used, there is no distinction among the types of operation authority.

Refer to the following authority list for the operation authority for individual online operations.

Operation Authority List for CX-Programmer

■ **CX-Programmer**

Function				Authority		
				Administrator	Designer	Operator
Work Online				Permitted	Permitted	Permitted
Auto Online (See note 1.)				Not permitted	Not permitted	Not permitted
Changing Operating Mode				Permitted	Permitted	Not permitted
Monitor (Monitoring, Differential Monitor, Pause)				Permitted	Permitted	Permitted
Force (On, Off, Cancel, Cancel All Forces)				Permitted	Permitted	Permitted
Set (On, Off, Value)				Permitted	Permitted	Permitted
Transfer	To PLC			Permitted	Permitted	Not permitted
	From PLC			Permitted	Permitted	Permitted (See note 2.)
	Compare with PLC			Permitted	Permitted	Permitted (See note 2.)
	Task Transfer to PLC			Permitted	Permitted	Not permitted
	Task Transfer from PLC			Permitted	Permitted	Permitted (See note 2.)
	Compare task with PLC			Permitted	Permitted	Permitted (See note 2.)
Protection	Set Password			Permitted	Permitted	Not permitted
	Release Password			Permitted	Permitted	Not permitted
Online Edit	Ladder Task		Changing program	Permitted	Permitted	Not permitted
			Changing set timer/ counter value	Permitted	Permitted	Not permitted
	ST Task		Changing program	Permitted	Permitted	Not permitted
	SFC Task	SFC Chart	Changing program	Permitted	Permitted	Not permitted
		Action	Changing program	Permitted	Permitted	Not permitted
		Transition	Changing program	Permitted	Permitted	Not permitted
	Function Block		Changing program	Permitted	Permitted	Not permitted
	Transfer FB Source			Permitted	Permitted	Not permitted
	Transfer SFC Source			Permitted	Permitted	Not permitted
Release Access Rights				Permitted	Permitted	Not permitted
Release FB/SFC/ST Online Edit Access Rights				Permitted	Permitted	Not permitted
Clear All Memory Areas				Permitted	Permitted	Not permitted
Data Trace				Permitted	Permitted	Permitted
Time Chart Monitoring				Permitted	Permitted	Permitted
Information Reading PLC Information				Permitted	Permitted	Permitted
Information Reading PLC Manufacturing Details				Permitted	Permitted	Permitted
Information Changing PLC name (See note 3.)				Permitted	Permitted	Not permitted
Reading/Resetting Cycle Time				Permitted	Permitted	Permitted
Monitoring Synchronous Operation Status (See note 4.)				Permitted	Permitted	Permitted
Set file encryption (See note 5.)				Permitted	Permitted	Not permitted
Disable file encryption setting (See note 5.)				Permitted	Permitted	Not permitted
Read operation log (See note 5.)				Permitted	Not permitted	Not permitted
Clear operation log (See note 5.)				Permitted	Not permitted	Not permitted
Export operation log (See note 5.)				Permitted	Not permitted	Not permitted
Read Extended FINS write access log (See note 5.)				Permitted	Not permitted	Not permitted
Clear Extended FINS write access log (See note 5.)				Permitted	Not permitted	Not permitted
Export Extended FINS write access log (See note 5.)				Permitted	Not permitted	Not permitted

Note (1) Not available for PLCs connected via *Secure Comm* (not supported for security reasons).
(2) Not available when UM protection is enabled (because UM protection cannot be released in advance).
(3) CJ2/CJ3 CPU only.
(4) CJ2H version.1.1 and later only.
(5) CJ3 CPU only.

■ **I/O Table**

Function			Authority		
			Administrator	Designer	Operator
Transfer to PLC	IO Table		Permitted	Permitted	Not permitted
	SIO Unit Parameters		Permitted	Permitted	Not permitted
Transfer from the PLC	IO Table		Permitted	Permitted	Permitted
	SIO Unit Parameters		Permitted	Permitted	Permitted
Compare with PLC			Permitted	Permitted	Permitted
Create			Permitted	Permitted	Not permitted
Verify Registered/Actual IO Table			Permitted	Permitted	Permitted
Delete			Permitted	Permitted	Not permitted
Unit Profile information			Permitted	Permitted	Permitted
Dip Switch information			Permitted	Permitted	Permitted
Online Add Unit/Hot Swap (See note 1.)			Permitted	Permitted	Permitted
Start Special Application	Start with Settings Inherited		Not permitted	Not permitted	Not permitted
	Start only		Permitted	Permitted	Permitted
Unit Setup	EIP21S Unit CJ3M-CPU built-in EtherNet/IP	Transfer [PC to Unit]	Permitted	Permitted	Not permitted
		Transfer [Unit to PC]	Permitted	Permitted	Permitted
		Compare	Permitted	Permitted	Permitted
		Restart	Permitted	Permitted	Not permitted
		Unit Manufacturing information	Permitted	Permitted	Permitted
		Unit Error Log	Permitted	Permitted	Permitted
	Other Units	Transfer [PC to Unit]	Permitted	Permitted	Permitted
		Transfer [Unit to PC]	Permitted	Permitted	Permitted
		Compare	Permitted	Permitted	Permitted
		Restart	Permitted	Permitted	Permitted
		Unit Manufacturing information	Permitted	Permitted	Permitted
		Unit Error Log	Permitted	Permitted	Permitted

Note (1) CS1D only.

■ **PLC Setup**

Function	Authority		
	Administrator	Designer	Operator
Transfer to PLC	Permitted	Permitted	Not permitted
Transfer from PLC	Permitted	Permitted	Permitted
Verify	Permitted	Permitted	Permitted

■ **Memory Card**

Function		Authority		
		Administrator	**Designer**	**Operator**
Format		Permitted	Permitted	Permitted
Program Area	Transfer [Area to Memory Card]	Permitted	Permitted	Permitted
	Transfer [Memory Card to Area]	Permitted	Permitted	Not permitted
CPU Bus Unit Area	Transfer [Area to Memory Card]	Permitted	Permitted	Permitted
	Transfer [Memory Card to Area]	Permitted	Permitted	Not permitted
IO Table Area	Transfer [Area to Memory Card]	Permitted	Permitted	Permitted
	Transfer [Memory Card to Area]	Permitted	Permitted	Not permitted
PLC Setup Area	Transfer [Area to Memory Card]	Permitted	Permitted	Permitted
	Transfer [Memory Card to Area]	Permitted	Permitted	Not permitted
Peripheral Device Area	Transfer [Area to Memory Card]	Permitted	Permitted	Permitted
	Transfer [Memory Card to Area]	Permitted	Permitted	Not permitted
Routing Table Area	Transfer [Area to Memory Card]	Permitted	Permitted	Permitted
	Transfer [Memory Card to Area]	Permitted	Permitted	Not permitted
IO Memory Area	Transfer [Area to Memory Card]	Permitted	Permitted	Permitted
	Transfer [Memory Card to Area]	Permitted	Permitted	Permitted

■ **Error Log**

Function	Authority		
	Administrator	**Designer**	**Operator**
Reading Error Log	Permitted	Permitted	Permitted
Clear All Memory Areas	Permitted	Permitted	Not permitted

■ **PLC Clock**

Function	Authority		
	Administrator	**Designer**	**Operator**
Obtaining time of PLC	Permitted	Permitted	Permitted
Synchronize Clock	Permitted	Permitted	Not permitted
Set PLC Clock	Permitted	Permitted	Not permitted

■ **PLC Memory**

Function			Authority		
			Administrator	**Designer**	**Operator**
Memory Tab	Transfer To PLC		Permitted	Permitted	Permitted
	Transfer From PLC		Permitted	Permitted	Permitted
	Compare With PLC		Permitted	Permitted	Permitted
	Monitor		Permitted	Permitted	Permitted
	Force On/Off		Permitted	Permitted	Permitted
	Set On/Off		Permitted	Permitted	Permitted
Address Tab	Force On/Off		Permitted	Permitted	Permitted
	Set Value		Permitted	Permitted	Permitted
	Forced Status	Scan Force Status	Permitted	Permitted	Permitted
		Clear all Forced Addresses	Permitted	Permitted	Permitted

Operation Authority List for EIP21S User Management Tool

Function			Authority		
			Administrator	**Designer**	**Operator**
Connect (After user registration)			Permitted	Permitted	Permitted
Display User List			Permitted	Permitted	Not permitted
Account operation (User's own account)	Add		Conditionally permitted (See note 1.)	Not permitted	Not permitted
	Delete		Not permitted	Not permitted	Not permitted
	Change	User name	Not permitted	Not permitted	Not permitted
		Authority	Not permitted	Not permitted	Not permitted
		Password	Permitted	Permitted	Permitted
		Password expiration setting	Permitted	Not permitted	Not permitted
Account operation (Other user's account)	Add		Permitted	Not permitted	Not permitted
	Delete		Permitted	Not permitted	Not permitted
	Change	User name	Not permitted	Not permitted	Not permitted
		Authority	Permitted	Not permitted	Not permitted
		Password	Permitted	Not permitted	Not permitted
		Password expiration setting	Permitted	Not permitted	Not permitted
Initialize User List			Permitted	Not permitted	Not permitted
Display Operation Log			Permitted	Not permitted	Not permitted
Export Operation Log			Permitted	Not permitted	Not permitted
Clear Operation Log			Permitted	Not permitted	Not permitted

Note (1) Available for unregistered users only.

Operation Authority List for PLC Backup Tool

Function	Authority		
	Administrator	**Designer**	**Operator**
Backup from PLC	Permitted	Permitted	Permitted
Restore to PLC	Permitted	Permitted	Not permitted
Compare with PLC	Permitted	Permitted	Permitted

User Authentication Timeout

If the CX-Programmer or EIP21S User Management Tool is online and has been in a no-operation state for a certain period of time, a user authentication timeout will occur. At this time, the Support Software will interrupt communications and then generate a communications error. In this case, once go offline and then connect the Support Software online again.

"No-operation state" refers to the state in which no key, mouse button, and mouse wheel operations are performed for the window of the Support Software, regardless of whether it is active or not. In the case of the CX-Programmer, operations are monitored not only for the main window but also for the IO Table Dialog Box, and Unit Setup and other tab pages. If a timeout occurs while a transfer processing dialog box is displayed after execution of a transfer, it will not be detected as a user authentication timeout until the user closes the transfer processing dialog box when the transfer processing is completed.

Note The PLC Backup Tool requires an online connection every time you perform backup, comparison, or restore operation. It goes offline automatically when the operation is completed. For this reason, the PLC Backup Tool does not monitor the time during which it is not operated online.

Settings

Set the timeout observation interval in the Environment Settings Dialog Box of the EIP21S User Management Tool when offline.

These settings, stored in the computer on which the EIP21S User Management Tool is installed, are common for all accounts. They must be set by a user who has Windows administrator rights.

The specifications of the settings are as shown below.

Setting	Setting condition	Setting range
Observe user authentication timeout	Optional	Select the check box/Clear the check box
Timeout observation interval	**Observe user authentication timeout** is selected	Default: 10 min Setting range: 1 to 360 min

For details on the operation, refer to the information that can be accessed from the Help menu of the EIP21S User Management Tool.

Checking the Connection Status

When the CX-Programmer is online with multiple CPU Units, the connection status of each CPU Unit is displayed in the project tree in the main window.

13-4 Opening and Closing the Port

This section describes the function of opening and closing the port.

13-4-1 Function Overview

Opening and closing the port is a function that blocks and allows packets to pass through the TCP/UDP ports assigned to individual communications functions according to the settings.

By setting any communications functions that you will not use to *Not use*, you can reduce the number of entry points for external attacks to improve the security performance of the system.

Note Set all communications functions that you will or may use to *Use*.
This function enables or disables the communications functions for a node based on the settings. For example, when *Use CIP message server* is not set, the tag data link for that node will not work.

13-4-2 Function Details

The table below shows whether or not it is possible to use TCP/UDP and other communications functions.

For details, refer to *3-11 Other Parameters*.

CS1/CJ1W-EIP21S or CJ3M-CPU3□

Communications functions	Type	Default Port number	Default value	Open and close the port	How to open and close the port
Tag Data Link (Class1)	UDP	2222	Open	Possible	Set by Use CIP message server on the CIP Communication Settings Tab Page in the Edit Parameters dialog box. Close: Unchecked Open: Checked
CIP Message Communication (Class3, UCMM)	TCP/ UDP	44818	Open	Possible	
DNS	UDP	53	Close	Possible	Set on the TCP/IP Tab Page in the Edit Parameters dialog box. Close: Not use DNS Open: Use DNS
Secure Comm	TCP	443	Open	Not possible	Closing is not possible.
SSH/SFTP	TCP	22	Close	Not possible	Opening is not possible.
FINS/UDP	TCP	9600	Close	Possible	Set on the FINS/UDP Tab Page in the Edit Parameters dialog box. Close: Not use FINS/ UDP Open: Use FINS/UDP

Communications functions	Type	Default Port number	Default value	Open and close the port	How to open and close the port
FINS/TCP	TCP/ UDP	9600	Close	Possible	Set on the FINS/TCP Tab Page in the Edit Parameters dialog box. Close: Not use FINS/ TCP Open: Use FINS/TCP
Modbus Server (See note.)	TCP	502	Close	Possible	Set on the Modbus Server Tab Page in the Edit Parameters dialog box. Close: Not use TCP Service Open: Use TCP Service
	UDP				Set on the Modbus Server Tab Page in the Edit Parameters dialog box. Close: Not use UDP Service Open: Use UDP Service
FTP	UDP	20, 21	Close	Possible	Set on the FTP Tab Page in the Edit Parameters dialog box. Close: Not use FTP Open: Use FTP
SNTP	UDP	123	Close	Possible	Set on the Auto Adjust Time Tab Page in the Edit Parameters dialog box. Close: Not use Auto Adjust Time Open: Use Auto Adjust Time
SNMP	UDP	161	Close	Possible	Set on the SNMP Tab Page in the Edit Parameters dialog box. Close: Not use SNMP Open: Use SNMP
SNTP Trap	UDP	162	Close	Possible	Set on the SNMP Tab Page in the Edit Parameters dialog box. Close: Not use SNMP Open: Use SNMP

Note Modbus Server is supported by the CJ3M-CPU3□.

CS1W/CJ1W-EIP21, CJ2H-CPU6□-EIP or CJ2M-CPU3□

Communications functions	Type	Default Port number	Default value	Open and close the port	How to open and close the port
Tag Data Link (Class1)	UDP	2222	Open	Not possible	Closing is not possible.
CIP Message Communication (Class3, UCMM)	TCP/ UDP	44818	Open	Not possible	
DNS	UDP	53	Close	Possible	Set on the TCP/IP Tab Page in the Edit Parameters dialog box. Close: Not use DNS Open: Use DNS
FINS/UDP	UDP	9600	Close	Not possible	Closing is not possible.
FINS/TCP	TCP	9600	Close	Not possible	Closing is not possible.
FTP	TCP	20, 21	Open	Possible	Set on the FTP Tab Page in the Edit Parameters dialog box. Close: Not use FTP Open: Use FTP
SNTP	UDP	123	Close	Possible	Set on the Auto Adjust Time Tab Page in the Edit Parameters dialog box. Close: Not use Auto Adjust Time Open: Use Auto Adjust Time
SNMP	UDP	161	Close	Possible	Set on the SNMP Tab Page in the Edit Parameters dialog box. Close: Not use SNMP Open: Use SNMP
SNTP Trap	UDP	162	Close	Possible	Set on the SNMP Tab Page in the Edit Parameters dialog box. Close: Not use SNMP Open: Use SNMP

Note (1) Default settings and other specifications differ between CS1W/CJ1W-EIP21S or CJ3M-CPU3□ and other models. Refer to *Using FTP* and *SECTION 11 FTP Server* for details.

Specifications

The following shows the impact when CIP message server (tag data links and CIP message communications), FINS/UDP, and FINS/TCP are set to not be used.

CIP Message Server

Set *Use CIP message server* to use tag data links and Explicit messages.

Setting	Operation
Use CIP message server (default)	• Tag data links and Explicit messages can be used. • Support Software or NS/NA series programmable terminals can connect to the CPU when the Network Type is *EtherNet/IP*.
Not use CIP message server	• Tag data links and Explicit messages cannot be used. • Support Software or NS/NA series programmable terminals cannot connect to the CPU when the Network Type is *EtherNet/IP*.

Note When tag data link settings exist and *Use CIP message server* is not set for a node, the behavior of the function will be as follows.

When set for local node		When set for remote node	
Originator	**Target**	**Originator**	**Target**
A verification error (target nonexistent) will occur. 7-segment display: d5 Error code: Not recorded.	No error will be detected.	A verification error (target nonexistent) will occur. 7-segment display: d5 Error code: Not recorded.	No error will be detected.

When *Use CIP message server* is not set for a node, a CIP message-related error will occur as shown below.

CMND/CMND2 (using FINS command 2810)

When set for instruction execution node	When set for remote node or relay node
No error will be detected.	The instruction ends normally. However, the response to the CIP message is as follows. General Status: 01 hex Additional Status: 0204 hex

CMND/CMND2 (using FINS command 2801), EXPLT, EGATR

When set for instruction execution node	When set for remote node
No error will be detected.	The instruction ends normally. However, the response to the CIP message is as follows. General Status: 01 hex Additional Status: 0204 hex

FINS/UDP and FINS/TCP

Service	Setting	Operation
FINS/UDP	Not use (default)	The Configuration Support Software CX-One cannot connect via *Ethernet* or *FinsGateway* (when FinsGateway is set to use UDP service). NS/NA/NB-series programmable terminals cannot connect to the CPU via *Ethernet*. When both FINS/UDP and FINS/TCP are set to *Not use*, executing the SEND, RECV, CMND, SEND2, RECV2, or CMND2 instruction results in an abnormal completion. (See note 2.)
	Use	FINS/UDP services can be used.
FINS/TCP	Not use (default)	The Configuration Support Software CX-One cannot connect to *Ethernet (FINS/TCP)* or *FinsGateway* (when FinsGateway is set to use TCP service). When both FINS/UDP and FINS/TCP are set to *Not use*, executing the SEND, RECV, CMND, SEND2, RECV2, or CMND2 instruction results in an abnormal completion. (See note 2.)
	Use	FINS/TCP Services can be used.

Note The behavior of the instruction differs depending on the *response required/not required* setting in its control data.
If response not required, the instruction will be normally completed.
If response required, the instruction will be completed abnormally. The completion code is 0205 hex (Timeout error: No response returned from remote node. Monitoring timer timed out.).

13-4-3 Protocols for Sending Automatically

The services that automatically send EtherNet frames regardless of whether the port is open or closed are as follows.

Protocol	Description
ARP	Sends ARP frames to detect duplicate IP addresses.
LLDP	Sends LLDP frames to search for adjacent devices. This can be turned OFF with a setting. (The default is ON.)

13-5 IP Packet Filtering

This section describes the IP packet filtering function.

13-5-1 Function Overview

IP packet filtering selectively permits packets that EtherNet/IP ports receive to pass through the filter according to the preset conditions. This improves the security performance of the system.

Note Register all devices and conditions for which to permit packet reception in the IP Packet Filter column.
If the IP packet filter settings do not match the specifications of the PLC system, or if the settings are incorrect, the devices may not either communicate or connect to Support Software. Therefore, we recommend using only the use cases described in *13-7 General Security Use Cases*.
Alternatively, ask someone who fully understands the network specifications of the PLC system and has knowledge of Ethernet to perform setup and management according to *Appendix J Security Use Cases*.
The network specifications here refer to the IP addresses of the devices and the TCP/UDP port numbers used for communications.

13-5-2 Function Details

In the IP Packet Filter Tab Page of the Edit Parameters Dialog Box for the EtherNet/IP Unit or built-in EtherNet/IP port in the CX-Programmer, set whether or not to use packet filtering and the filter conditions for packets permitted to pass through the filter.

Note Enabling the IP packet filter settings prevents the Unit from communicating with devices via the target EtherNet/IP port. Be careful of the settings.

The settings in the IP packet filter table are retained when you change from *Use IP Packet Filter* to *Not use IP Packet Filter* in the CX-Programmer. The settings in the IP packet filter table are transferred to the built-in EtherNet/IP Unit regardless of the setting of whether or not to use the function.

The IP packet filter function supports stateful inspection. Therefore, the EtherNet/IP Unit or built-in EtherNet/IP port can receive responses from the remote node without filter conditions added to the IP packet filter table when it makes a request to a remote node as a client.

The protocols supported by stateful inspection are TCP, UDP, and ICMP.

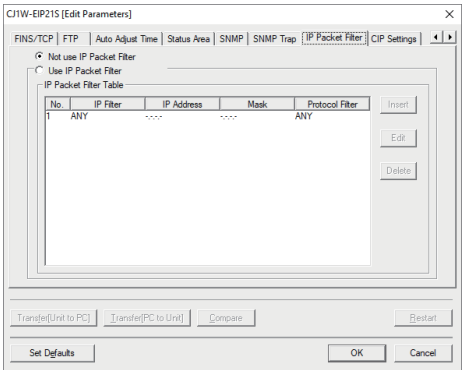
Note The DNS/SNTP function is not supported by IP packet filtering. This is because it is a client function that opens ports during use and closes them at completion.

Settings

Set this in the IP Packet Filter Tab Page of the Edit Parameters Dialog Box for the EtherNet/IP Unit or built-in EtherNet/IP port in the CX-Programmer.

The settings will be reflected and enabled when the Unit is restarted after completion of the transfer.

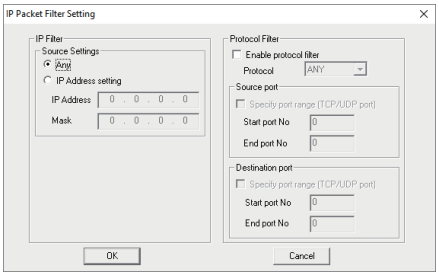
IP Packet Filter Tab Page



Setting	Description	Default
IP Packet Filter	Select whether or not to use the IP packet filter. Not use IP Packet Filter (default) Use IP Packet Filter	Not use IP Packet Filter
IP Packet Filter Table	Set the conditions for IP packets for which to permit reception. You can edit the conditions when *Use IP Packet Filter* is selected. A maximum of 32 conditions can be registered.	Registration of 1 condition (to receive ANY IP address and protocol)

IP Packet Filter Table

Select the *Use IP Packet Filter* Option in the IP Packet Filter Tab Page and then click the **Insert** Button to display the table.



Setting			Description	Default
IP Filter			Set the conditions for filtering by source IP address.	---
	Source Settings		Set the source IP address specification method. Any IP Address setting	Any
		IP Address	When the IP address specification method is *IP Address setting*, set the source IP address.	0.0.0.0
		Mask	When the IP address specification method is *IP Address setting*, set the mask for the source IP address.	0.0.0.0

Setting	Description	Default
Protocol Filter	Set the conditions for filtering by protocol.	
Refer to *Appendix I IP Packet Filter Settings*.		

■ **How the IP Filter Settings Work**

The IP filter settings permits packet reception at the set IP address(es).

If *Any* is set in *Source Settings*, packet reception is permitted for all IP addresses.

If *IP Address setting* is set in *Source Settings*, packet reception is permitted for the IP address specified in the lower-level settings: *IP Address* and *Mask*.

For *IP Address*, set the bits set for the mask in *Mask* and the following bits to *0*s.

Example of setting

- To permit one IP address
  Set the IP address at which to permit reception in *IP Address* and *255.255.255.255* in *Mask*.
  For example, to permit reception at 192.168.250.100, set *192.168.250.100* in I*P Address* and *255.255.255.255* in *Mask*.
- To permit multiple IP addresses
  Set the IP address at which to permit reception in *IP Address* and *Mask*.
  For example, to permit reception at 192.168.***.***, set *192.168.0.0* in *IP Address and 255.255.0.0* in *Mask*.

■ **How the Protocol Filter Settings Work**

Refer to *Appendix I IP Packet Filter Settings*.

Settings for Various Use Scenarios

The IP packet filter table settings to use the IP packet filter are shown for each device or function that you will use.

Settings for Connecting Support Software

The settings for using Support Software are as shown in the table below.

Support Software	Connection method	Applicable protocol	*Protocol Filter* settings			
			Protocol	*Destination Port* settings		
				Range specification	Start port No.	End port No.
Configuration Support Software CX-One	The *Network Type* used for connection is *Secure Comm*.	HTTPS	TCP	Use	443	443
	The *Network Type* used for connection is *Ethernet(FINS/TCP)*.	FINS	TCP		9600 (See note 1.)	9600 (See note 1.)
	The *Network Type* used for connection is *Ethernet*.	FINS	UDP		9600 (See note 1.)	9600 (See note 1.)
	The *Network Type* used for connection is *EtherNet/IP*.	CIP	TCP		44818	44818
		ICMP	ICMP	Not use	---	---
Network Configurator	*Ethernet I/F* is selected as the interface.	CIP	TCP	Use	44818	44818
		CIP	UDP		44818	44818
		ICMP	ICMP	Not use	---	---
EIP21S User Management Tool	No selection required (Only secure communications will be used.)	HTTPS	TCP	Use	443	443

Note (1) If you enter a port number value that is not the default in the FINS/UDP or FINS/TCP settings, the value will be set.

Settings for Using EtherNet/IP Communications

The settings for using EtherNet/IP communications are as follows.

Communications name	Applicable protocol	Condition	*Protocol Filter* settings			
			Protocol	*Destination Port* settings		
				Range specification	Start port No.	End port No.
EtherNet/IP messages	UCMM	Server	TCP	Use	44818	44818
	Class 3	Server	TCP		44818	44818
EtherNet/IP tag data links	Class 1	Originator	IGMP (See note 1.)	Not use	---	---
		Target	TCP	Use	44818	44818

Note (1) Set this to use Multicast.

Note If you use SYSMAC Gateway or CX-Compolet, in addition to the above settings, make settings to also permit ICMP.
The settings are as shown in the table below.

***Protocol Filter* settings**			
Protocol	***Destination Port* settings**		
	Range specification	**Start port No.**	**End port No.**
ICMP	Not use	---	---

Settings for Connecting OMRON Programmable Terminals

The settings for connecting OMRON Programmable Terminals are as shown in the table below.

■ **NA-series Programmable Terminals**

Connection method	**Applicable protocol**	***Protocol Filter* settings**			
		Protocol	***Destination Port* settings**		
			Range specification	**Start port No.**	**End port No.**
Connection via *EtherNet/IP*	CIP	TCP	Use	44818	44818
Connection via *Ethernet*	FINS	UDP		9600 (See note 1.)	9600 (See note 1.)

Note (1) If you enter a port number value that is not the default in the FINS/UDP settings, the value will be set.

■ **NB-series Programmable Terminals**

Connection method	**Applicable protocol**	***Protocol Filter* settings**			
		Protocol	***Destination Port* settings**		
			Range specification	**Start port No.**	**End port No.**
Connection via *Ethernet*	FINS	UDP	Use	9600 (See note 1.)	9600 (See note 1.)

Note (1) If you enter a port number value that is not the default in the FINS/UDP settings, the value will be set.

■ **NS-series Programmable Terminals**

Connection method	Applicable protocol	*Protocol Filter* settings			
		Protocol	*Destination Port* settings		
			Range specification	Start port No.	End port No.
Connection via *EtherNet/IP*	CIP	TCP	Use	44818	44818
Connection via *Ethernet*	FINS	UDP		9600 (See note 1.)	9600 (See note 1.)

Note (1) If you enter a port number value that is not the default in the FINS/UDP settings, the value will be set.

Settings for Using FINS Message Communications

The settings for using FINS message communications are as shown in the table below.

Connection method	Applicable protocol	*Protocol Filter* settings			
		Protocol	*Destination Port* settings		
			Range specification	Start port No.	End port No.
FINS/UDP	FINS	UDP	Use	9600 (See note 1.)	9600 (See note 1.)
FINS/TCP	FINS	TCP		9600 (See note 1.)	9600 (See note 1.)

Note (1) If you enter a port number value that is not the default in the FINS/UDP or FINS/TCP settings, the value will be set.

Settings for Using SNMP

The *Protocol Filter* and *Destination Port* settings for using SNMP are as follows.

Protocol Filter - *Protocol*: UDP

Destination Port

Range specification: Use

Start port No.: 161 (See note 1.)

End port No.: 162 (See note 1.)

Note (1) If you enter an SNMP/SNMP trap port number, the value will be set.

Settings for Using FTP Server

The *Protocol Filter* and *Destination Port* settings for using the FTP server function are as follows.

Protocol Filter - *Protocol*: TCP

Destination Port

Range specification: Use

Start port No.: 20 (See note 1.)

End port No.: 21 (See note 1.)

Note (1) If you enter an FTP port number, the value will be set.

Troubleshooting

If You Forget the IP Packet Filter Settings for the EtherNet/IP Unit or built-in EtherNet/IP port

If available, use the CX-Programmer that provides online connection to the EtherNet/IP Unit via Ethernet and check or change the IP packet filter settings.

If the Support Software is not available, you cannot connect to the EtherNet/IP Unit via Ethernet.

In this case, connect the CX-Programmer online and check or change the IP packet filter settings through the USB, peripheral, or serial port of the CPU Unit with the EtherNet/IP Unit mounted.

If Access from a Remote Node Fails

Follow the steps below to narrow down the cause and take corrective action.

Step	Item	Corrective action
1	Determine whether the cause is the IP packet filter settings.	• Set the EtherNet/IP Unit to *Not use IP Packet Filter* and check if it is possible to access the remote node. • If possible, the cause is the IP packet filter settings. Go to step 2. • If not possible, the cause may be other than the IP packet filter settings. Review the communications path, connection destination settings, etc.
2	Review the IP packet filter settings.	• Reset the IP address and port number settings for the devices and Support Software connected to the EtherNet/IP Unit or built-in EtherNet/IP port . • Monitor the communications line data and check if the source IP address, source port, and destination port are registered in the IP packet filter settings (only if possible).

13-6 Operation Log

This section describes the operation log function.

13-6-1 Function Overview

The operation log function records important operations and results of users who connect the Support Software online using secure communications, along with information on the date and time, computer's IP address, and user name.

This allows you to determine who did what operation and when. You can use it to prevent repudiation if a security problem occurs.

This function is available only when the EtherNet/IP Unit is connected using the secure communications function.

Note When connected to the CP1H CPU Units, the CX-Programmer and PLC backup tools cannot use the corresponding functions.

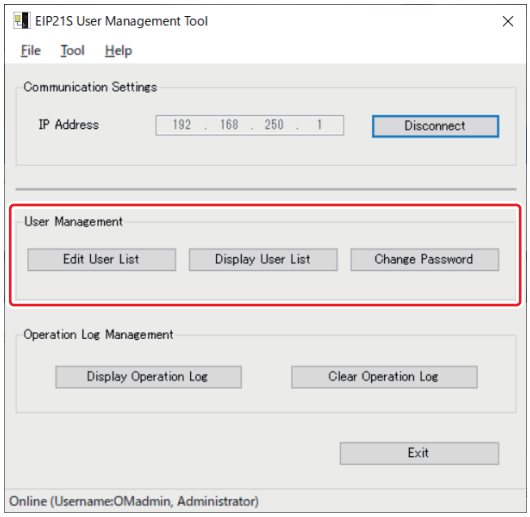
13-6-2 Function Details

Settings

The user authentication settings need to be configured to use the operation log function.

Procedure

1,2,3... 1. Connect the EIP21S User Management Tool online and authenticate with an account that has the Administrator operation authority.
In the EIP21S User Management Tool Dialog Box, the *IP Address* setting in the *Communication Settings* group will be grayed out.



Use the buttons in the *Operation Log Management* group in this dialog box to operate operation logs.

Refer to the following description for information on displaying, exporting, and clearing operation logs.

Specifications

A EtherNet/IP Unit or built-in EtherNet/IP port records operation logs in its own nonvolatile memory.

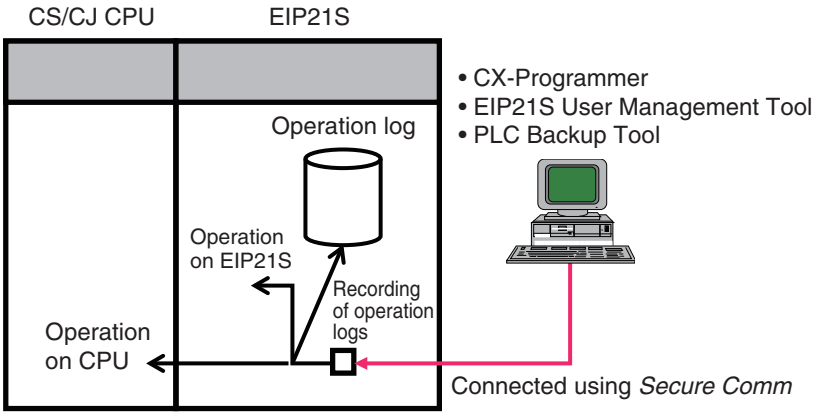
It has a capacity to record a maximum of 1,024 operation logs. If the number of operation logs exceeds 1,024, the oldest operation log will be overwritten with a new operation log.

Users with the Administrator operation authority can connect the EIP21S User Management Tool online, and display, export, and clear operation logs.

You can use the operation log function when Support Software with security functions is connected online using secure communications.

Refer to *Operation Log List* for information on logs recorded by the operation log function.

The operation log function cannot be used with CX-Programmer or PLC Backup Tool versions that do not support security functions.



Note The date time used for operation logs is the clock data in the CPU Unit. When the battery is discharged or during battery-less operation, the clock data become unstable after the internal capacitor is discharged. If clock data is required, install a battery and set the correct clock information in the CPU Unit using CX-Programmer or the "Automatic Clock Adjustment" function provided by the EtherNet/IP Unit.

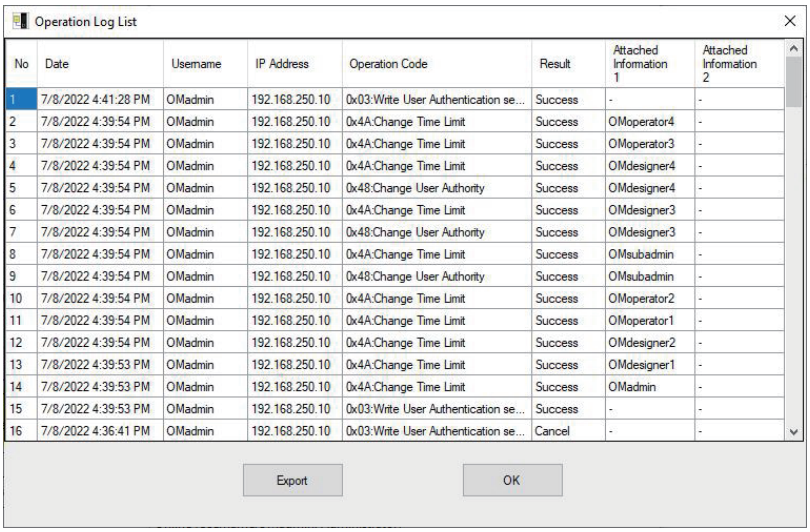
Displaying Operation Logs

Users with the Administrator operation authority can display operation logs.

As a user with the administrative authority, click the **Display Operation Log** Button in the *Operation Log Management* group in the EIP21S User Management Tool Dialog Box to display the operation log list.

By default, the operation log list is sorted by date and time. The date and time represents the PLC clock time obtained from the CPU Unit.

The numbers in the *No.* column represent the order in which the operation logs were recorded by the EtherNet/IP Unit or built-in EtherNet/IP port.

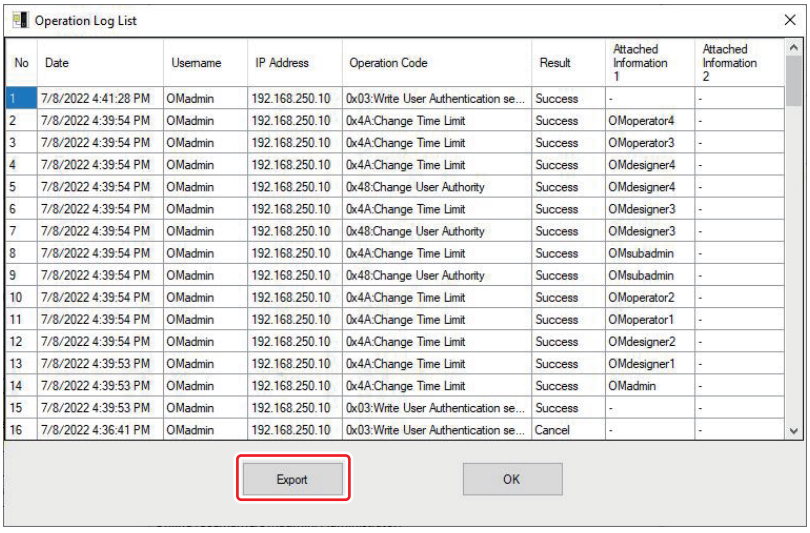


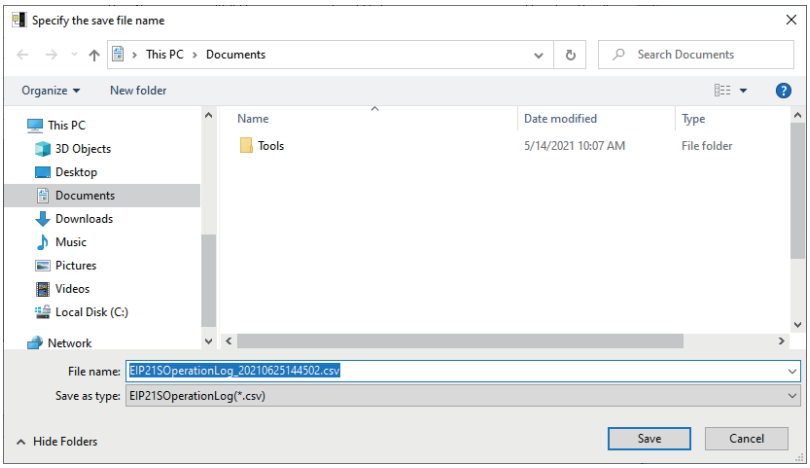
Note If you changes the PLC clock time from the CPU Unit, the order of registration of the operation logs will not match the order by PLC clock time.
To check the operation logs in the order of registration, sort the operation logs in the *No.* column.

Exporting Operation Logs

Users with the Administrator operation authority can export operation logs.

As a user with the administrative authority, click the **Export** Button, select the location to save the operation log file in the Operation Log List Dialog Box, and save it.





Default file name: EIP21SOperationLog_*Date(YYYYMMDDHHMMSS)*.csv

Default export destination: My Document folder
(Environment.SpecialFolder.MyDocument)

The specifications of the exported operation log file are as follows.

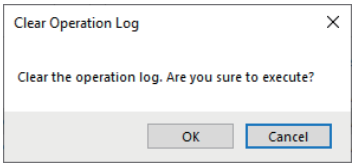
Setting	Specification
Output format	CSV (Comma-separated values)
Display order	Default display (Reverse chronological order of occurrence time)
Character code	UTF-8 with BOM
Language	English (independent of the language setting of the Support Software)

Clearing Operation Logs

Users with the Administrator operation authority can clear operation logs.

As a user with an administrative authority, click the **Clear Operation Log** Button in the *Operation Log Management* group in the EIP21S User Management Tool Dialog Box. Click the **OK** Button in the confirmation dialog box to clear all operation logs.

This registers *Clear Important Operation Log* in the operation log.



Note Initializing the EtherNet/IP Unit or built-in EtherNet/IP port to the defaults does not clear the operation logs.

Operation Log List

Important operations that will be recorded in operation logs are as listed below.

Software Name	Operation target (See note 6.)	Operation	Operation log			
			Log code (hex)	Operation	Result, IP address, Username (See note 1.)	Additional Information (See note 2.)
EIP21S User Management Tool	EIP21S	Registration of the first user	01	First user registration	a (See note 3.)	A
EIP21S User Management Tool CX-Programmer PLC Backup Tool	EIP21S	Online connection	02	Online Connection Started (See note 4.)	b (See note 8.)	A
		End online connection.	55	Online Disconnection (See note 4.)	b	A
EIP21S User Management Tool	EIP21S	Transfer user authentication settings.	03	Write User Authentication setting	a	A
		Get operation logs.	04	Acquire Important Operation Log	a	A
		Clear operation logs.	05	Clear Important Operation Log	a	A
		Add user account.	46	Add User	b	B
		Delete user account.	47	Delete User	b	B
		Change operation authority of account.	48	Change User Authority	b	B
		Change password of account.	49	Change User Password	b	B
		Change password expiration setting of account.	4A	Change Time Limit	b	B
		Initialize user authentication setting.	4B	Initialize User Setting	b	A
CX-Programmer PLC Backup Tool	CPU	Change to PROGRAM mode	0A	PLC Operation Mode (PROGRAM)	a	A
CX-Programmer	CPU	Change to MONITOR mode	0B	PLC Operation Mode (MONITOR)	a	A
		Change to RUN mode	0C	PLC Operation Mode (RUN)	a	A
		Transfer from computer to PLC	0D	Transfer to PLC	a	A
		Transfer from PLC to computer	0E	Transfer from PLC	a	A
		Comparison between computer and PLC	0F	Transfer (Comparison (PC and PLC))	a	A
		Transfer specified task from computer to PLC.	12	Partial Transfer (Transfer task to PLC)	a	A
		Transfer specified task from PLC to computer.	13	Partial Transfer (Transfer task from PLC)	a	A
		Compare specified tasks between computer and PLC.	14	Partial Transfer (Comparison (PC and PLC))	a	A
		Set read protection by password.	15	Read Protection (Set)	a	A
		Release read protection by password.	16	Read Protection (Release)	a	A

Software Name	Operation target (See note 6.)	Operation	Operation log			
			Log code (hex)	Operation	Result, IP address, Username (See note 1.)	Additional Information (See note 2.)
CX-Programmer	CPU	Force-release remote node (CX-Programmer or Communications Unit) access right.	18	Protect (Release Access Right)	a	A
		Clear all user program, I/O memory, and parameter area data in CPU Unit (CPU Unit status initialization).	19	Clear All PLC Memory	a	A
		Start online editing.	1A	Online Edit (Edit)	a	A
		Transfer changes in online editing. Change timer/ counter settings.	1B	Online Edit (Apply Changes)	a	A
		Undo online editing.	1C	Online Edit (Undo)	a	A
		Transfer FB source in online editing.	1D	Online Edit (Transfer FB Source)	a	A
		Transfer SFC/ST source in online editing.	1E	Online Edit (Transfer SFC/ST Source)	a	A
		Force-release online edit permissions to FB/SFC/ST.	1F	Online Edit (Forced Release Permissions to FB/SFC/ST)	a	A
		Change PLC name.	20	Change PLC Name	a	A
PLC Backup Tool	---	Back up data of all or only specified Units in PLC.	32	Backup	a	A
		Transfer backup files to all or only specified Units in PLC.	33	Restore	a	A
CX-Programmer (PLC Clock)	CPU	Set PLC clocks. Or adjust PLC's time to computer's time.	3C	Clock Synchronization	a	A
CX-Programmer (IO Table CS1W/CJ1W-EIP21S (Edit Parameters))	EIP21S	Transfer settings from EIP21S to computer.	3D	EIP21S Settings (Transfer from Unit)	a	A
		Transfer settings from the computer to EIP21S.	3E	EIP21S Settings (Transfer to Unit)	a	A
		Compare settings between EIP21S and computer.	3F	EIP21S Settings (Comparison)	a	A
		Restart the EIP21S.	40	EIP21S Settings (Restart) (See note 5.)	a	A
CX-Programmer (IO Table CS1W/CJ1W-EIP21S (Edit Parameters)), PLC Backup Tool	EIP21S	Change setting of IP address type of EIP21S.	4C	Change EIP21S Settings (IP Address Type)	b	C
		Change IP address setting of EIP21S.	4D	Change EIP21S Settings (IP Address)	b	D
		Change FINS/UDP setting of EIP21S.	4E	Change EIP21S Settings (FINS/UDP)	b	A
		Change FINS/TCP setting of EIP21S.	4F	Change EIP21S Settings (FINS/TCP)	b	A
		Change FTP setting of EIP21S.	50	Change EIP21S Settings (FTP)	b	A
		Change SNMP setting of EIP21S.	51	Change EIP21S Settings (SNMP)	b	E
		Change setting of IP packet filter of EIP21S.	52	Change EIP21S Settings (IP Packet Filter)	b	A
		Change CIP settings of EIP21S.	53	Change EIP21S Settings (CIP Communication)	b	A

Software Name	Operation target (See note 6.)	Operation	Operation log			
			Log code (hex)	Operation	Result, IP address, Username (See note 1.)	Additional Information (See note 2.)
CX-Programmer (Memory Card)	CPU	Transfer data from PLC to Memory Card.	41	Memory Card (Transfer to Memory Card/EM File)	a	A
		Transfer data from Memory Card to PLC.	42	Memory Card (Transfer to PLC)	a	A
CX-Programmer (PLC System Settings)	CPU	Transfer PLC system settings from computer to PLC.	43	PLC System Settings (Transfer to PLC)	a	A
		Transfer PLC system settings from PLC to computer.	44	PLC System Settings (Transfer from PLC)	a	A
		Compare PLC system settings between computer and PLC.	45	PLC System Settings (Comparison)	a	A
CX-Programmer	CPU (See note 7.)	Set file encryption.	58	File Encryption Settings	c	A
		Disable file encryption setting.	59	Disable File Encryption Setting.	c	A
		Clear operation log.	5A	Clear Operation Log	c	A
		Clear Extended FINS write access log.	5B	Clear Extended FINS Write Access Log	c	A
Network Configurator	EIP21S (See note 7.)	Start tag data link.	5C	Start Tag Data Link	e	A
CX-Programmer, Program, turn power supply ON		Turn power supply ON, or start tag data link by software switch operation.	5C	Start Tag Data Link	e	A
Network Configurator		Stop tag data link.	5D	Stop Tag Data Link	d	A
CX-Programmer, Program		Stop tag data link by software switch operation.	5D	Stop Tag Data Link	d	A
CX-Programmer (I/O table component (unit restart of CJ1W-EIP21S [Edit Parameters])), CX-Programmer (unit restart by AR), reset by Network Configurator, turn power supply ON	EIP21S (See note 7.)	Start EIP21S.	5E	Start EIP21S	e	A

Note (1) The contents of the result, IP address, and user columns are classified by symbol as follows:

Symbol	Result	IP address	Username
a	The result of the operation is recorded. 0: Normal exit (All operations completed successfully) 1: Abnormal exit (Other than Normal exit and Cancel) 2: Cancel (Operation canceled by user)	The IP address of the operated computer is recorded.	The user name of the user account with which the user performed the operation is recorded.
b	The result of the operation is recorded. 0: Normal exit (All operations completed successfully)		
c	0: Normal exit (All operations completed successfully) 1: Abnormal exit (All operations did not complete successfully)		EIP21S (See note 9.)
d	Normal exit (All operations completed successfully)	0.0.0.0	
e	0: Normal exit (All operations completed successfully) 1: Abnormal exit (All operations did not complete successfully)		

(2) Additional Information is classified by symbol as follows:

Symbol	Additional Information 1	Additional Information 2
A	None	None
B	This shows the user name of the operation target account.	None
C	This shows the setting of the changed IP address type. 01 hex: **Use the following address** 02 hex: **Get IP address from the BOOTP server** 03 hex: **Get IP address from the BOOTP server (1-Shot)**	None
D	When the setting of the changed IP address type is **Use the following address**, it shows the set value of that.	None
E	This shows the changed setting item. 01 hex: Setting other than **Authentication Check 1** and **Authentication Check 2** 02 hex: **Authentication Check 1** 03 hex: **Authentication Check 2**	None

(3) The user name registered at the first administrator registration will be recorded as an operation log.

(4) The registration timings for Online Connection Started and Online Disconnection are as follows:

Operation	Registration timing
Online Connection Started	When user authentication is completed.
Online Disconnection	When online connection ends.

(5) In the following cases, operation logs will not be recorded because communications between the EtherNet/IP Unit or built-in EtherNet/IP port and the Support Software are interrupted.
- You returned to out-of-box configuration, and then emulated cycling power.
- You changed and then transferred the IP address.

(6) The operation of CJ3M-CPU3□ built-in EtherNet/IP is also described as EIP21S.

(7) The CJ3M-CPU□□ only.

(8) This is “c” for the CJ3M-CPU3□.
If authentication fails five times in a row, “Abnormal exit” is recorded.

(9) “EIP21S” is registered to leave a record that an error was registered by the EtherNet/IP Unit.

13-7 General Security Use Cases

This section describes general security use cases and shows a configuration example and settings for each of them.

13-7-1 Use Cases

The following use cases are described.

Case	Use case	Function to use	Reference
1	Permitting packet reception for specific protocols	Opening and closing the port	*13-7-2*
2	Permitting packet reception from specific source IP addresses	IP packet filtering	*13-7-3*

Note Refer to *Appendix J Security Use Cases* for more advanced use cases.

13-7-2 Case 1: Permitting Packet Reception for Specific Protocols

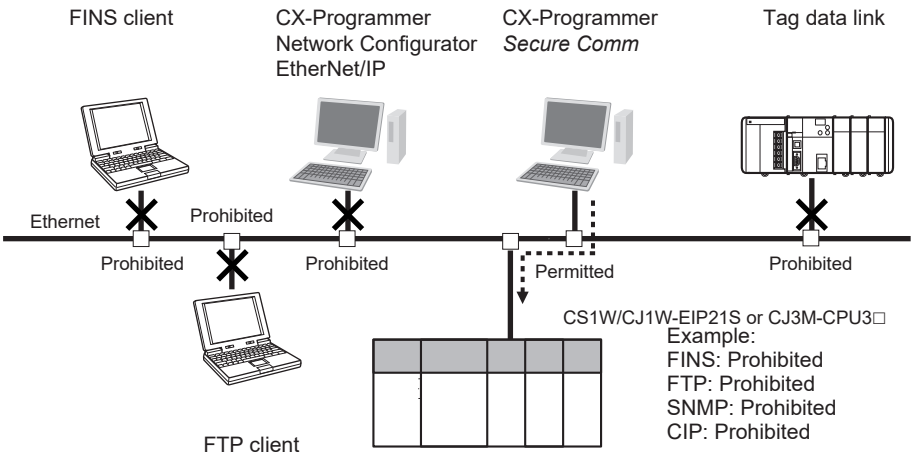
This use case is for permitting access from a specific protocol.

Use it to prohibit communications for protocols that are not used.

In this use case, the function of opening and closing the port is used.

Configuration Example

This configuration example permits Secure Comm communications with the Support Software, and prohibits communications from other protocols.



Settings for This Configuration Example

Make the settings as shown in the following table.

TCP/IP communications functions	Setting	Reference
CIP message server	Not use	*13-4 Opening and Closing the Port*
FINS/UDP	Not use	
FINS/TCP	Not use	
FTP server	Not use	*Using FTP* in *3-11 Other Parameters*
SNMP	Not use	*Using SNMP* in *3-11 Other Parameters*

13-7-3 Case 2: Permitting Packet Reception from Specific Source IP Addresses

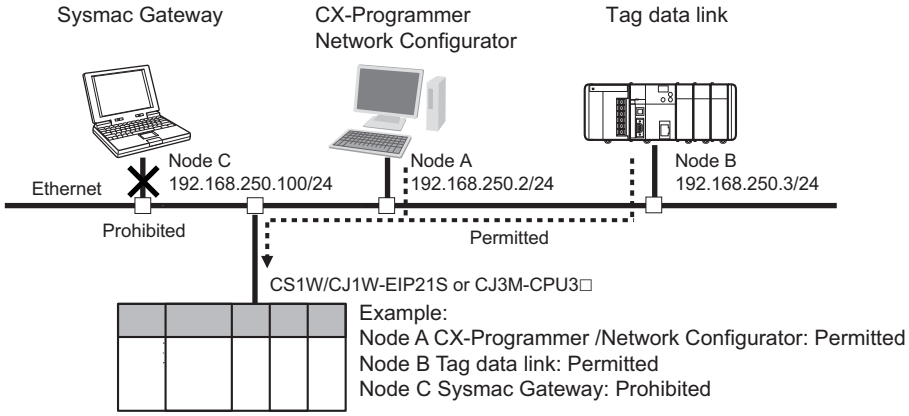
This use case is for permitting access from specific nodes.

Use it to prohibit connections from unauthorized nodes, such as computers brought into the site without permission.

In this use case, IP packet filtering is used.

Configuration Example

This configuration example permits only communications from specific computers and external devices, and prohibits communications from other client devices.



Settings for This Configuration Example

Make the settings in the IP Packet Filter Setting Dialog Box as shown in the following table.

Set the IP addresses of nodes A and B individually. Therefore, set *255.255.255.255* as the mask.

No.	IP Filter			Protocol Filter						
	Source Settings			Protocol Filter	Source port			Destination Port		
	Setting method	IP Address	Mask		Range specification	Start port No.	End port No.	Range specification	Start port No.	End port No.
1	IP address specification	192.168.250.2	255.255.255.255	Any	---	---	---	---	---	---
2	IP address specification	192.168.250.3	255.255.255.255	Any	---	---	---	---	---	---

Note

(1) Register the IP addresses of all external devices to use because communications from IP addresses that are not registered in the IP Packet Filter Setting are blocked.

(2) If you set the mask to other than 255.255.255.255, communications from multiple IP addresses will be permitted.
For example, the settings below permit communications from devices with IP addresses between 192.168.250.0 and 192.168.250.255.

No.	IP Filter			Protocol Filter						
	Source Settings			Protocol Filter	Source port			Destination Port		
	Setting method	IP Address	Mask		Range specification	Start port No.	End port No.	Range specification	Start port No.	End port No.
1	IP address specification	192.168.250.0	255.255.255.0	Any	---	---	---	---	---	---

13-8 Protective Measures to Prevent Security Threats

Using the security function of the EtherNet/IP Units or built-in EtherNet/IP ports is useful for preventing a network from security threats. To do so, you need to use the function of the Units properly.

This section describes the operational measures for using the security function of the Units properly.

Arranging Communications Devices to a Reliable Network

When you use services other than secure communications of the EtherNet/IP Units or built-in EtherNet/IP ports, arrange the communications devices, including the EtherNet/IP Units, in a reliable network.

If you use the other network, take appropriate measures such as using VPN.

Refer to *2-1-3 Communications Specifications* for the services supported by the EtherNet/IP Units or built-in EtherNet/IP ports.

Deleting Data before Discarding the Units

When you discard the EtherNet/IP Units or built-in EtherNet/IP ports and the CPU Units connecting them, delete the information inside the Units by the following methods to prevent information leakage.

Target	Description	Procedure
CJ1/CJ2/CS/ CP1H CPU Units	Clear all memory areas.	Refer to the *SYSMAC CX-Programmer Ver.9.□ Operation Manual* (Cat. No. W446).
CJ3 CPU Unit	Clear all memory areas, clear operation log, and clear Extended FINS write access log.	Refer to the *CJ-series CJ3 CPU Unit Hardware User's Manual* (Cat. No. W664).
CS1W/CJ1W-EIP21S CJ3M-CPU3□ Built-in EtheNet/IP function	Initialize them to the defaults.	Refer to *17-5 Unit Initialization*.

Putting a Physical Access Restriction to the Units

Implement measures that restrict anyone other than authorized personnel not to enter the place where the PLC system including the CPU Units and the CS1W/CJ1W-EIP21S is installed.

The measures include restricting such people not to enter that place and locking the entrance.

Putting an Access Restriction to the Network Configuration File and Managing the Configuration

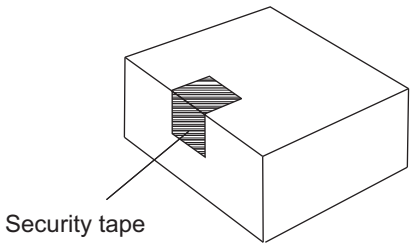
Implement measures that prevent anyone other than authorized personnel from obtaining or tampering the network configuration file that the Network Configurator creates.

The measures include keeping the network information file in an access-restricted place and managing the configuration of that.

Refer to *6-2-15 Saving the Network Configuration File* and *6-2-16 Reading a Network Configuration File* for the network information file.

Using Unpacked Items

For the EtherNet/IP Units or built-in EtherNet/IP ports and the CPU Units connecting them, use those with security tape unpeeled from the purchased item packaging boxes.



Note To prevent tampering, the product's item packaging boxes are sealed with tape that indicates that they have not been opened. Confirm that they have not been opened before use.

SECTION 14
Socket Services

This section describes the functionality provided by the Ethernet Unit via the socket services.

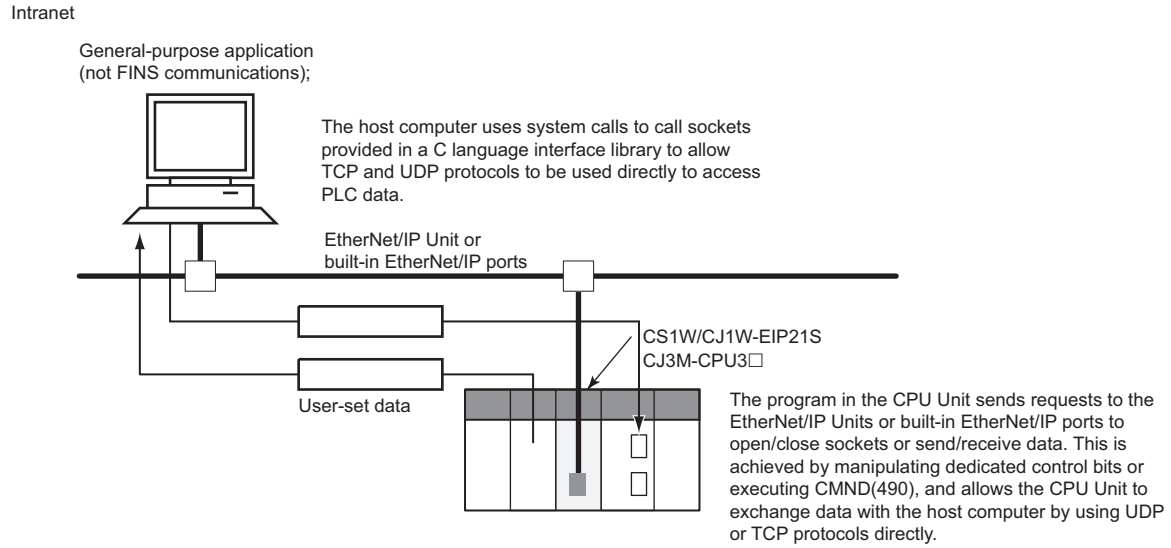
14-1 Overview of Socket Services 431
14-1-1 Overview 431
14-1-2 Using Socket Services with Socket Service Request Switches 432
14-1-3 Using Socket Services with CMND/CMND2 433
14-1-4 Specific Socket Service Functions 433
14-2 Overview of Socket Communications from Ethernet Units 434
14-2-1 What are Sockets? 434
14-2-2 Socket Port Numbers 434
14-3 Protocol Overview 435
14-3-1 Differences between TCP and UDP 435
14-3-2 Opening TCP Sockets 436
14-3-3 Fragmentation of Send Data 437
14-4 Socket Service Function Guide 438
14-4-1 Manipulating Dedicated Control Bits 438
14-4-2 Executing CMND 439
14-4-3 Settings Required for Socket Service Function 439
14-4-4 CIO Area Allocations 439
14-4-5 DM Area Allocations 440
14-5 Using Socket Services by Manipulating Dedicated Control Bits 442
14-5-1 Application Procedure 442
14-5-2 Socket Services and Socket Status 444
14-5-3 Socket Service Parameters 445
14-5-4 Parameters 447
14-5-5 Socket Service Request Switches 449
14-5-6 Response Codes 450
14-5-7 Timing Charts 455
14-5-8 TCP/IP Communications Programming Example (Using Socket Services by Manipulating Dedicated Control Bits) 457
14-5-9 UDP/IP Communications Programming Example (Using Socket Services by Manipulating Dedicated Control Bits) 461
14-6 Using Socket Services with CMND/CMND2 465
14-6-1 Using Socket Service 465
14-6-2 Socket Services and Socket Status 466
14-6-3 Basic FINS Command Format 467
14-6-4 Response Codes in the Command Response 468
14-6-5 Response Codes in the Results Storage Areas 468
14-6-6 Communications Timing Chart 468

14-6-7 Socket Service Timing Chart 469
14-6-8 TCP/IP Communications Programming Example (Using Socket Services with CMND) 470
14-6-9 UDP/IP Communications Programming Example (Using Socket Services with CMND) 478
14-7 Details on the Socket Service Using with Function Block 484
14-7-1 Table of Function Block 484
14-7-2 UDP/IP Communications Programming Example (Using Function Blocks) 484
14-8 Precautions in Using Socket Services 488
14-8-1 UDP and TCP Socket Services 488
14-8-2 UDP Socket Service 488
14-8-3 TCP Socket Service 488
14-8-4 Precautions in Using Socket Service Request Switches 489
14-8-5 Times Required for Sending and Receiving for Socket Services 490

14-1 Overview of Socket Services

14-1-1 Overview

The Socket services are used to exchange data between the PLC and general-purpose applications that do not support FINS message communications. The socket services can be used by CS/CJ-series PLCs through the user program by manipulating dedicated control bits (called Socket Service Request Switches) or by executing the CMND instruction.



The two methods of using the socket services are as follows:

- Dedicated Control Bits (Socket Service Request Switches)
  Requests can be made to a socket service by setting parameters and then merely manipulating specific Socket Service Request Switches.
- CMND(490)
  Requests can be made to a socket service by sending service request commands to the EtherNet/IP Unit or built-in EtherNet/IP port.

Note One of the main differences between using Socket Service Request Switches and using CMND(490) is in the number of sockets that can be connected simultaneously, as shown in the following table.

Protocol	Socket Service Request Switches	CMND (See note.)
UDP	Total of 8 sockets max.	8 sockets max.
TCP		8 sockets max.

Note The CMND2 instructions can also be used with the CJ2/CJ3 CPU Units.

The following built-in EtherNet/IP Units are supported.

EtherNet/IP Units or built-in EtherNet/IP ports
CS1W-EIP21S, CJ1W-EIP21S or CJ3M-CPU3□

Note (1) The CS1W/CJ1W-ETN21 Ethernet Unit, the EtherNet/IP Unit or built-in EtherNet/IP ports, and CJ3M-CPU3□ Unit both support the socket service functions.
Although the functions and specifications are almost the same, the addresses of the allocated CIO Area and DM Area words are different between the two.
To replace a Unit between the two in an application that uses this function, you must change the addresses of the allocated CIO Area and DM Area words.
For information on the EtherNet/IP Unit's allocated CIO Area and DM Area words, refer to *SECTION 4 Ethernet Unit Memory Allocations* in the *CS/CJ-series Ethernet Units Operation Manual Construction of Networks* (Cat. No. W420).

(2) A port for socket services is in the closed state unless a UDP or TCP port is specified and the open process is performed.

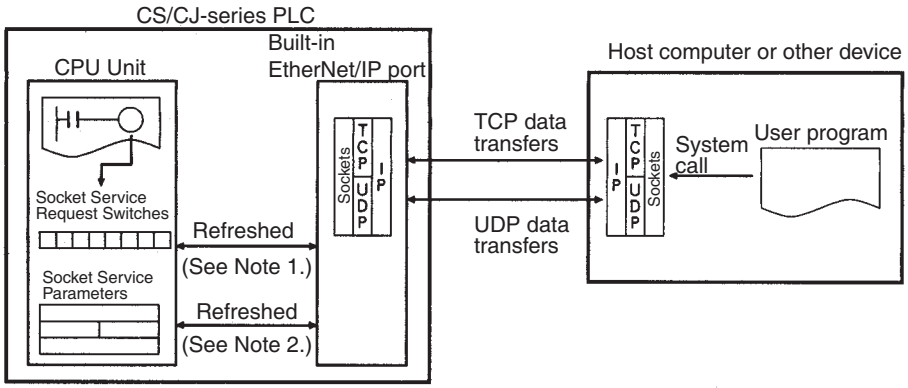
(3) Except for the CS1W/CJ1W-EIP21S or CJ3M-CPU3□ EtherNet/IP Units or built-in EtherNet/IP ports do not support the socket services.

14-1-2 Using Socket Services with Socket Service Request Switches

Socket services can be used by setting the parameters in a Socket Service Parameter Area in the CPU Bus Unit Area and then turning ON a Socket Service Request Switch.

When using Socket Service Request Switches, a maximum of 8 sockets can be opened simultaneously for the UDP and TCP combined. Also, the same socket number cannot be used simultaneously for both UDP and TCP. (There is only one Socket Service Parameter Area for each socket, i.e., the same area must be used for both UDP and TCP.)

An illustration of using Socket Service Request Switches to execute socket services is provided below.



Note

1. Socket Service Request Switches in the CPU Bus Unit Area in the CIO Area are used to send a service request from the CPU Unit to the EtherNet/IP Unit or built-in EtherNet/IP port.
2. The Socket Service Parameters in the CPU Bus Unit Area in the DM Area are used to specify the service being requested from the EtherNet/IP Unit or built-in EtherNet/IP port. The CPU Bus Unit Area in the DM Area is also used to receive results of processing from the EtherNet/IP Unit or built-in EtherNet/IP port to the CPU Unit.

After setting the required parameters in a Socket Service Parameter Area in the CPU Bus Unit Area in the DM Area, the Socket Service Request Switches can be used to request opening, sending, receiving, or closing for either the UDP or TCP protocol. When requesting a send, send data at the send/receive data addresses set in the parameter area is sent. When requesting a reception, data is received to the send/receive data addresses set in the parameter area.

14-1-3 Using Socket Services with CMND/CMND2

Service request commands can be sent to the EtherNet/IP Unit or built-in EtherNet/IP port by executing the CMND/CMND2 instruction in the ladder diagram.

Up to 16 sockets can be connected using CMND/CMND2: 8 UDP sockets and 8 TCP sockets.

The socket service request commands that can be used are listed in the following table. Refer to *Appendix E FINS Commands Addressed to EtherNet/IP Units or Built-in EtherNet/IP Ports* for details.

Command code		Name
MRC	SRC	
27	01	UDP OPEN REQUEST
	02	UDP RECEIVE REQUEST
	03	UDP SEND REQUEST
	04	UDP CLOSE REQUEST
	10	TCP PASSIVE OPEN REQUEST
	11	TCP ACTIVE OPEN REQUEST
	12	TCP RECEIVE REQUEST
	13	TCP SEND REQUEST
	14	TCP CLOSE REQUEST

Requests sent to the Ethernet Unit by sending commands through execution of CMND/CMND2, and when the Unit receives a command, it will return a response. The response does not, however, indicate that processing has been completed, and the status of the flags in the Socket Status Words allocated to the Unit must be used to determine when processing has been completed.

The results of processing will be stored in the words specified when CMND/CMND2 was executed once the requested processing has been completed.

14-1-4 Specific Socket Service Functions

The socket service functions listed in the following table can be executed either using Socket Service Request Switches or using CMND/CMND2.

Protocol	Socket service request
UDP	Open UDP socket
	Receive via UDP socket
	Send via UDP socket
	Close UDP socket
TCP	Open TCP socket, passive
	Open TCP socket, active
	Receive via TCP socket
	Send via TCP socket
	Close TCP socket

14-2 Overview of Socket Communications from Ethernet Units

14-2-1 What are Sockets?

Sockets are interfaces that allow TCP and UDP protocols to be used directly from the user program. With personal computers, socket are provided as C language interface libraries, etc., which allow TCP or UDP protocols to be programming using library functions. With UNIX computers, socket interfaces are supported in the form of system calls.

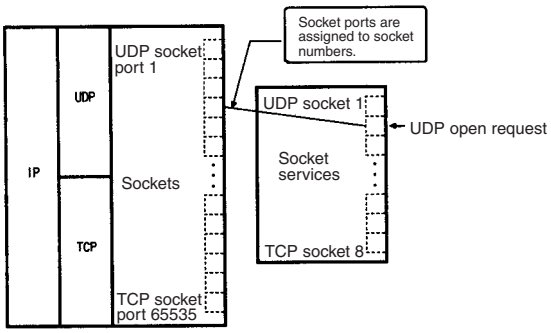
The CS/CJ-series PLCs support the socket service from the user program. The user program requests service functions either by manipulating Socket Service Request Switches in the CPU Bus Unit Area in the CIO Area or by sending FINS commands to the EtherNet/IP Unit or built-in EtherNet/IP port by executing CMND instruction in the ladder diagram.

Socket communications services can be used to transfer arbitrary data between a PLC and a host computer or between two PLCs. The Ethernet supports two socket services: a UDP socket service and a TCP socket service.

■ **Using Sockets with the EtherNet/IP Unit or built-in EtherNet/IP port**

The EtherNet/IP Unit or built-in EtherNet/IP port supports up to 16 simultaneous socket connections for the socket services, 8 each for UDP and TCP sockets.

Socket numbers 1 to 8 are assigned to sockets for both UDP and TCP sockets. Sockets are managed from the ladder-diagram program by assigning a socket port for each socket number. The socket port number is assigned when the socket is opened.



14-2-2 Socket Port Numbers

Port numbers are classified as follows in network communications.

Port number	Name	Usage
1 to 1023	System port (Well-known port)	Port for which purpose is predetermined
1024 to 49151	User port (Registered port)	Port used by specific application or service
49152 to 65535	Dynamic and/Private Ports	Port that users can freely use without restrictions

Therefore, for socket services, when using ports for purposes other than registered protocols, it is recommended to use ports 49152 to 65535. Also, port number 0 cannot be specified.

Furthermore, the built-in EtherNet/IP port uses TCP/UDP ports for some applications, so do not set a port number that will be a duplicate of any of their port numbers. For details on the TCP/UDP port numbers used by the EtherNet/IP Unit (built-in port), refer to *13-4 Opening and Closing the Port*.

14-3 Protocol Overview

14-3-1 Differences between TCP and UDP

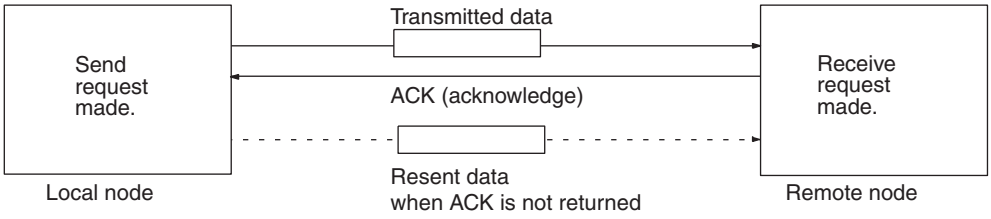
There are differences in the socket services between TCP and UDP.

■ TCP Communications

The following procedure is followed each time data is transmitted to ensure that the data arrives normally at the remote node:

1,2,3...

1. The remote node returns ACK when data is received normally.
2. The local node sends the next data after it receives ACK, or it resends the same data if ACK is not returned within the specified time.

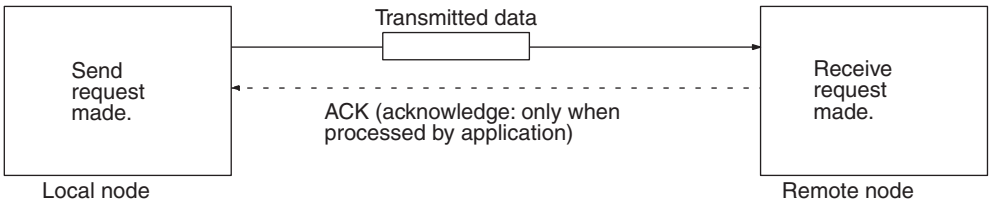


With the TCP protocol, the remote IP address and remote TCP port number are specified when an open request is made for a socket. When a send request is made, the number of bytes to send and the send data are specified. When a receive request is made, the number of bytes to receive is specified.

With the TCP protocol, communications with another remote device are not possible until the socket that was opened has been closed.

■ UDP Communications

Data is simply sent to the remote node. Unlike TCP, the reception of data is not checked and data is not resent. To increase communication reliability, data resends must be programmed by the user in user application.



With the UDP protocol, the remote IP address and remote UDP port number are not specified when an open request is made for a socket. When a send request is made, the remote IP address, the remote UDP port number, the number of bytes to send, and the send data are specified. When a receive request is made, the number of bytes to receive is specified. (The response data shows from which IP address and UDP port number the received data was sent.)

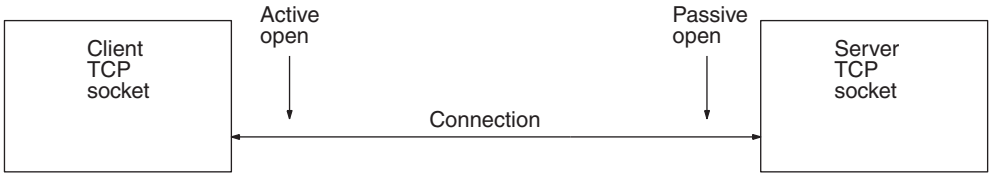
With the UDP protocol, communications with another remote device are possible even if the socket that was opened is not closed.

14-3-2 Opening TCP Sockets

To achieve highly reliable data communications, TCP establishes a virtual communications circuit between the two nodes before starting data transmissions. The virtual communications circuit is known as a “connection.”

■ **Passive OPEN and Active OPEN**

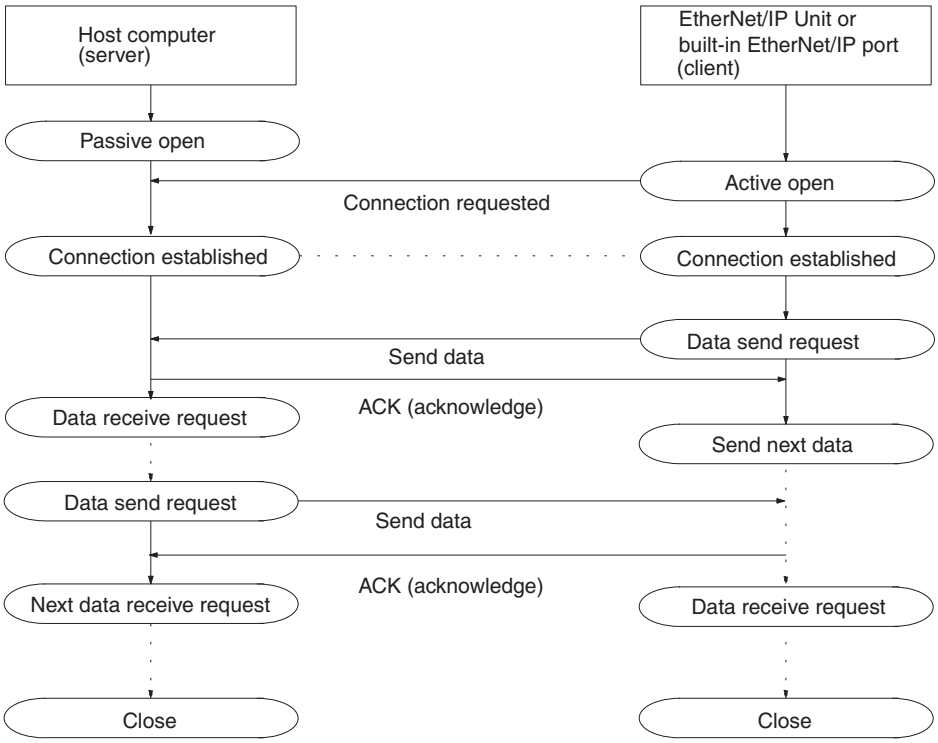
An open command is executed for a node to establish a connection. The open method differs depending on whether the node is a client or server. A passive open method is used to open the node as a server and the active open method is used to open the node as a client.



Note 1. When a connection is made between two nodes, the process at the node providing a service is called the server, and the process at the node requesting the service is called the client. The server is started first and waits for a service request from a client. The client requests to the server that a connection be opened and then transmits data. When the TCP protocol is used, however, the client–server relationship does not need to be programmed in the application because it is automatically handled by the protocol.

■ **TCP Communications Procedure**

When the EtherNet/IP Unit (built-in port) operates as a client and the host computer operates as a server to perform communication using TCP, processing proceeds according to the procedure shown in the chart below.



14-3-3 Fragmentation of Send Data

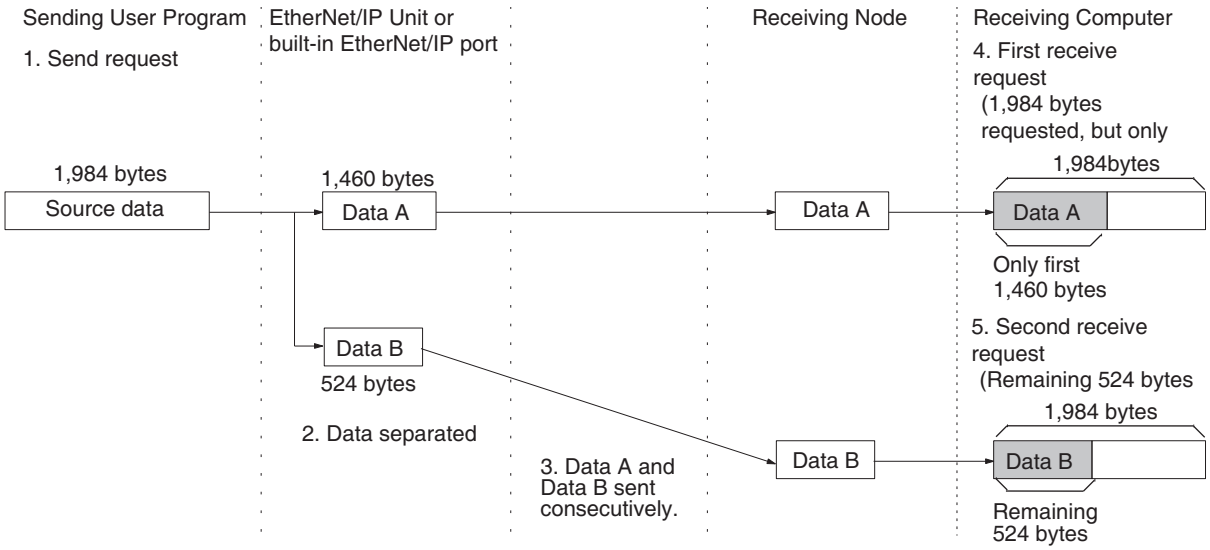
The EtherNet/IP Unit or built-in EtherNet/IP port fragments data for TCP transmission into units of 1,460 bytes and data for UDP transmission into units of 1,472 bytes. TCP requires one reception request to receive each unit of data. UDP, however, restores the original data before passing it to the user process, allowing all the data in a single transmission to be received with one reception request.

■ Cautions when Using TCP

An example of the fragmentation and transmission of data using the TCP is shown in the following illustration.

1,2,3...

1. The sending user program sends a request to send 1,984 bytes of data.
2. The EtherNet/IP Unit or built-in EtherNet/IP port fragments the send data into Data A with 1,460 bytes and Data B with 524 bytes.
3. Data A and Data B are sent consecutively.
4. The receiving user program sends a request to receive 1,984 bytes of data. However, only data A is sent in the first packet, and data B is not received.
5. Another receive request to receive data must be made before the remaining data, Data B, is received.



When using TCP protocol, the fragmented data is passed to the user program. Therefore, the receiving user program must be able to evaluate the end of the data transmission, and repeatedly send receive requests until all data has been received. The receive request is sent twice in the example shown above, but the data would be even more fragmented if a router was included in the communications path, and the number of receive requests would need to be increased accordingly.

When making the receive request, it is not necessary to specify the same data length as the sent data length. For example, if the length setting is shorter than the actual length of the data, all the data can be received by repeating the receive requests.

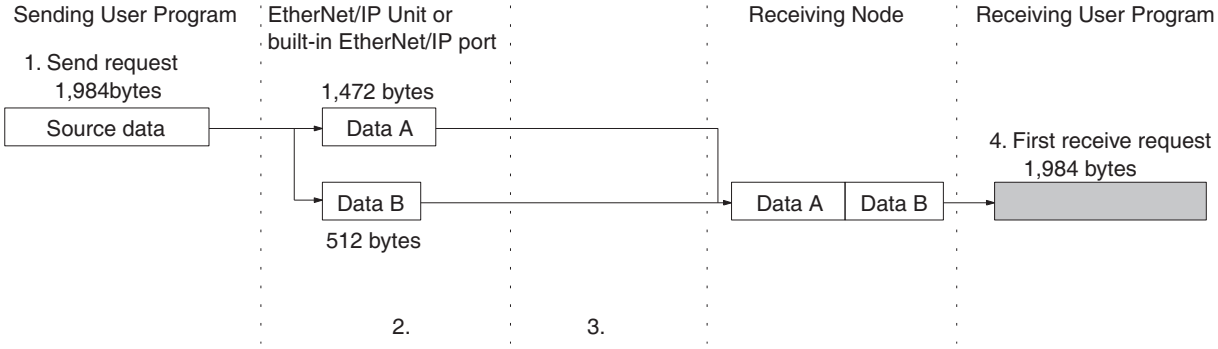
Note If communications are with a different segment and data is sent via the TCP protocol, data will be fragmented into units of 536 bytes.

■ **Cautions when Using UDP**

An example of fragmentation and transmission of data using the UDP is shown in the following illustration.

1,2,3...

1. The transmission user program sends a request to send 1,984 bytes of data.
2. The EtherNet/IP Unit or built-in EtherNet/IP port fragments the send data into Data A with 1,472 bytes and Data B with 512 bytes.
3. Data A and Data B are sent consecutively.
4. When the receiving user program sends a request to receive 1,984 bytes of data, Data A and Data B are linked to restore the original data, which is passed to the user program.



As shown above, the UDP protocol handles data communications as datagrams, so that the send data is restored to the original data before being passed to the user program. Consequently, if the data length in the receive request is set to the length of the send data, the entire data can be received using a single receive data request. However, if the data length in the receive data request is set smaller than the actual length of the data, all received data exceeding the set data length will be discarded.

14-4 Socket Service Function Guide

14-4-1 Manipulating Dedicated Control Bits

■ **Description**

The EtherNet/IP Unit's or built-in EtherNet/IP port's socket services are used by setting parameters and manipulating bits only.

■ **Point**

This method is used by setting the required parameters in the socket service parameter area allocated in the CPU Bus Unit words in the DM Area, and then turning ON the Socket Service Request Switches in memory.

■ **Number of available sockets**

A total of 16 sockets can be used, 8 UDP sockets + 8 TCP sockets.

Note To use the CS1W/CJ1W-EIP21S's socket services when tag data links are used on the CS1W/CJ1W-EIP21S, use the CMND instruction. Do not manipulate dedicated control bits.

14-4-2 Executing CMND

■ **Description**

The socket services are used by sending service request commands to the EtherNet/IP Unit or built-in EtherNet/IP port.

■ **Point**

A UDP or TCP socket service is requested by sending a FINS command to the Ethernet Unit by executing CMND from the CPU Unit.

■ **Number of available sockets**

- Knowledge of FINS commands is required.
- A total of 16 sockets can be used, 8 UDP sockets + 8 TCP sockets.

14-4-3 Settings Required for Socket Service Function

The following settings must be made in the Unit Setup when using socket services.

CX-Programmer Unit Setup Tab	Setting	Setting requirements	Page
TCP/IP	IP Address	Optional	*3-8 TCP/IP and Link Set-tings*
	Sub-net Mask	Optional	
	IP Router Table	Optional (Set when Ethernet Unit will communicate through the IP router with a socket on another IP network segment)	
	TCP/IP keep-alive	Optional (Change when the default setting of 5 min is unacceptable.)	
Status Area	Layout Type	Required Set this to *User defined*.	*3-11 Other Param-eters*
	Allocation Area	Required Set the first word of the user setting area to allocate.	

14-4-4 CIO Area Allocations

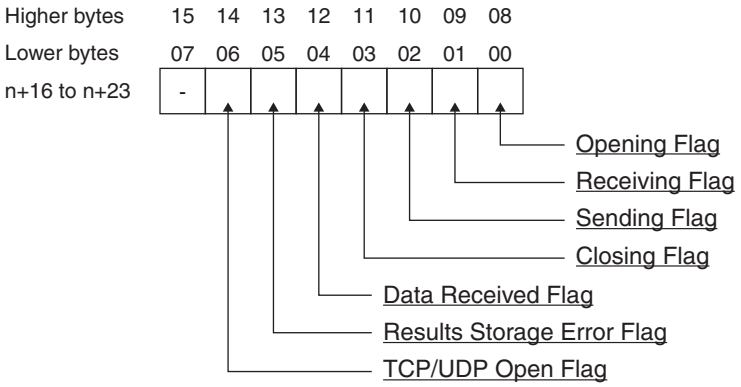
The following CIO Area words are allocated in the CPU Bus Unit Area in the CIO Area starting at word n+ 1. The value of n can be calculated from the unit number as follows:

Beginning word n = CIO 1500 + (25 x unit number)

■ **UDP/TCP Socket Status (Ethernet Unit to CPU Unit)**

The status of the UDP and TCP sockets is provided in the socket status words shown in the following diagram. There is a status word for each socket for both UDP and TCP.

Offset	Bit 15 – 8	7 – 0	Data direction
n+16	UDP Socket No. 2 Status	UDP Socket No. 1 Status	EtherNet/IP Unit → CPU Unit
n+17	UDP Socket No. 4 Status	UDP Socket No. 3 Status	
n+18	UDP Socket No. 6 Status	UDP Socket No. 5 Status	
n+19	UDP Socket No. 8 Status	UDP Socket No. 7 Status	
n+20	TCP Socket No. 2 Status	TCP Socket No. 1 Status	EtherNet/IP Unit → CPU Unit
n+21	TCP Socket No. 4 Status	TCP Socket No. 3 Status	
n+22	TCP Socket No. 6 Status	TCP Socket No. 5 Status	
n+23	TCP Socket No. 8 Status	TCP Socket No. 7 Status	



Bit	Switch	Status	Manipulated by	Unit operation
00/08	Opening Flag	ON	Unit	Turns ON when an open request is received.
		OFF		Turns OFF when open processing has been completed.
01/09	Receiving Flag	ON		Turns ON when a receive request is received. (Turns ON when receive request is received if high-speed option is disabled and remains OFF when high-speed processing is enabled.)
		OFF		Turns OFF when receive processing has been completed.
02/10	Sending Flag	ON		Turns ON when a send request is received. (Turns ON when send request is received if high-speed option is disabled and remains OFF when high-speed processing is enabled.)
		OFF		Turns OFF when send processing has been completed.
03/11	Closing Flag	ON		Turns ON when an close request is received.
		OFF		Turns OFF when close processing has been completed.
04/12	Data Received Flag	ON		Turns ON when data from a remote node has been received at an open TCP socket.
		OFF		Turns OFF when receive processing has been requested for an open TCP socket.
05/13	Results Storage Error Flag	ON		Turns ON if there is an error in the Results Storage Area specified for the socket service request command to the EtherNet/IP Unit or built-in EtherNet/IP port. Turns ON when either bits 0 to 3 or bits 8 to 11 complete changing from ON to OFF.
		OFF		Turns OFF when the next request is received.
06/14	TCP/UDP Open Flag	ON		Turns ON when UDP open processing has been completed or when a TCP connection is made.
		OFF		Turns OFF when close processing has been completed. (Will remain OFF when open processing ends in an error.)
07/15	(Not used)	-	-	-

14-4-5 DM Area Allocations

The following DM Area words are allocated in the CPU Bus Unit Area in the DM Area. The beginning word m is calculated by the following equation.

Beginning word m = D30000 + (100 x unit number)

■ Number of Bytes Received at TCP Socket (Ethernet Unit to CPU Unit)

The number of bytes of data saved in the reception buffer at the TCP socket is stored in the TCP Connection Status words. The Data Received Flag in the CIO Area turns ON/OFF in response to the status of these words. When the dedicated control bits (switches) are manipulated or the receive request is sent by executing the CMND(490) instruction, the values of these words are temporarily set to 0000 hexadecimal.

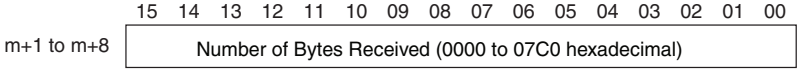
If any data remains in the reception buffer after the receive request processing is complete, the number of bytes is stored in the Number of Bytes Received at TCP Socket and the Data Received Flag turns ON again.

Depending on the timing of data reception, the number of received data bytes may be 0 even if the Data Received Flag turns ON. To prevent this, use flag control to receive data according to the sample programs.

Refer to the following sample programs.

- 14-7-8 TCP/IP Communications Programming Example (Using Socket Services by Manipulating Dedicated Control Bits)
- 14-8-8 TCP/IP Communications Programming Example (Using Socket Services with CMND(490))

Receive requests should be executed after confirming that the required data is contained in the number of bytes received.



Up to 4,096 bytes of data are stored in the reception buffer, but the value stored is within the range (maximum: 1,984 bytes) that can be set by manipulating the control bits or sending the receive request in the CMND(490) instruction.

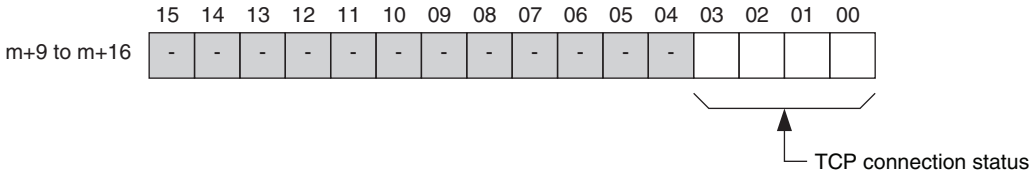
0000 hexadecimal: 0 bytes

07C0 hexadecimal: 1,984 bytes

■ TCP Connection Status (Ethernet Unit to CPU Unit)

The TCP Connection Status shows the status of a port that has been opened using the TCP socket. This port status is stored even after the port is closed, and remains until the socket is used to open the port again.

The TCP Connection Status Bits are not synchronized with the Socket Status words, however, so the status conversion timing is slightly different.



The status is shown in bits 0 to 3 (1-digit hexadecimal), as follows:

Number	Status	Meaning
00000000	CLOSED	Connection closed.
00000001	LISTEN	Waiting for connection.
00000002	SYN SENT	SYN sent in active status.
00000003	SYN RECEIVED	SYN received and sent.
00000004	ESTABLISHED	Already established.
00000005	CLOSE WAIT	FIN received and waiting for completion.
00000006	FIN WAIT1	Completed and FIN sent.
00000007	CLOSING	Completed and exchanged FIN. Awaiting ACK.
00000008	LAST ACK	FIN sent and completed. Awaiting ACK.
00000009	FIN WAIT2	Completed and ACK received. Awaiting FIN.
0000000A	TIME WAIT	After closing, pauses twice the maximum segment life (2MSL).

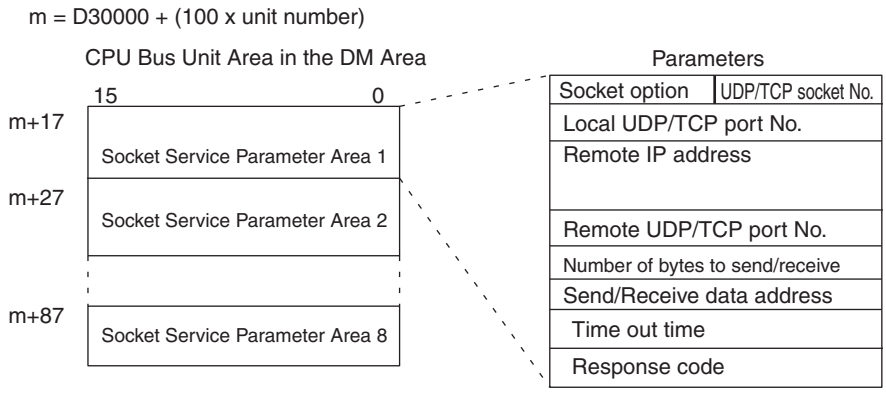
Note The CS1W/CJ1W-ETN21 Ethernet Unit, the ,EtherNet/IP Unit or built-in EtherNet/IP port, and CJ3M-CPU3□ both support the socket services using Socket Service Request Switches. However, the addresses of the allocated CIO areas and allocated DM areas differ between both of them.
To replace a Unit between the two in an application using this function, you must change the addresses of the allocated CIO Area words.
For information on the allocated CIO Area words, refer to *SECTION 4 Ethernet Unit Memory Allocations* in the *CS/CJ-series Ethernet Units Operation Manual Construction of Networks* (Cat. No. W420).

14-5 Using Socket Services by Manipulating Dedicated Control Bits

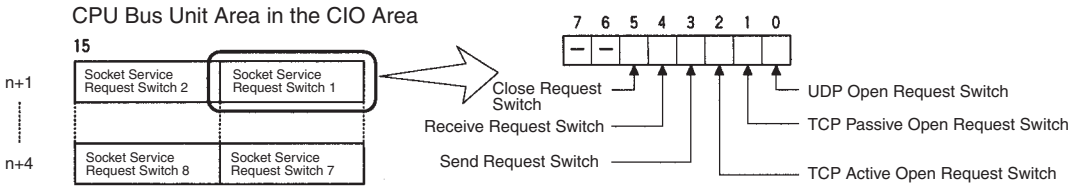
14-5-1 Application Procedure

Procedure

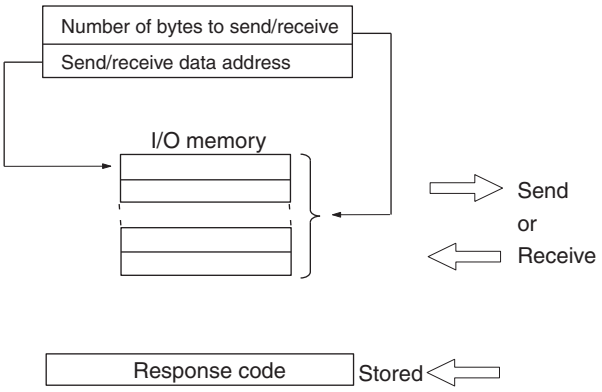
1,2,3... 1. Set the socket service parameters in the CPU Bus Unit Area in the DM Area.



2. Turn ON the Socket Service Request Switches in the CPU Bus Unit Area in the CIO Area.



3. When a send or receive request is made, the data will be automatically sent or received according to the send/receive data address in the Socket Service Parameter Area. When processing has been completed, a response code will be automatically stored in the Socket Service Parameters.



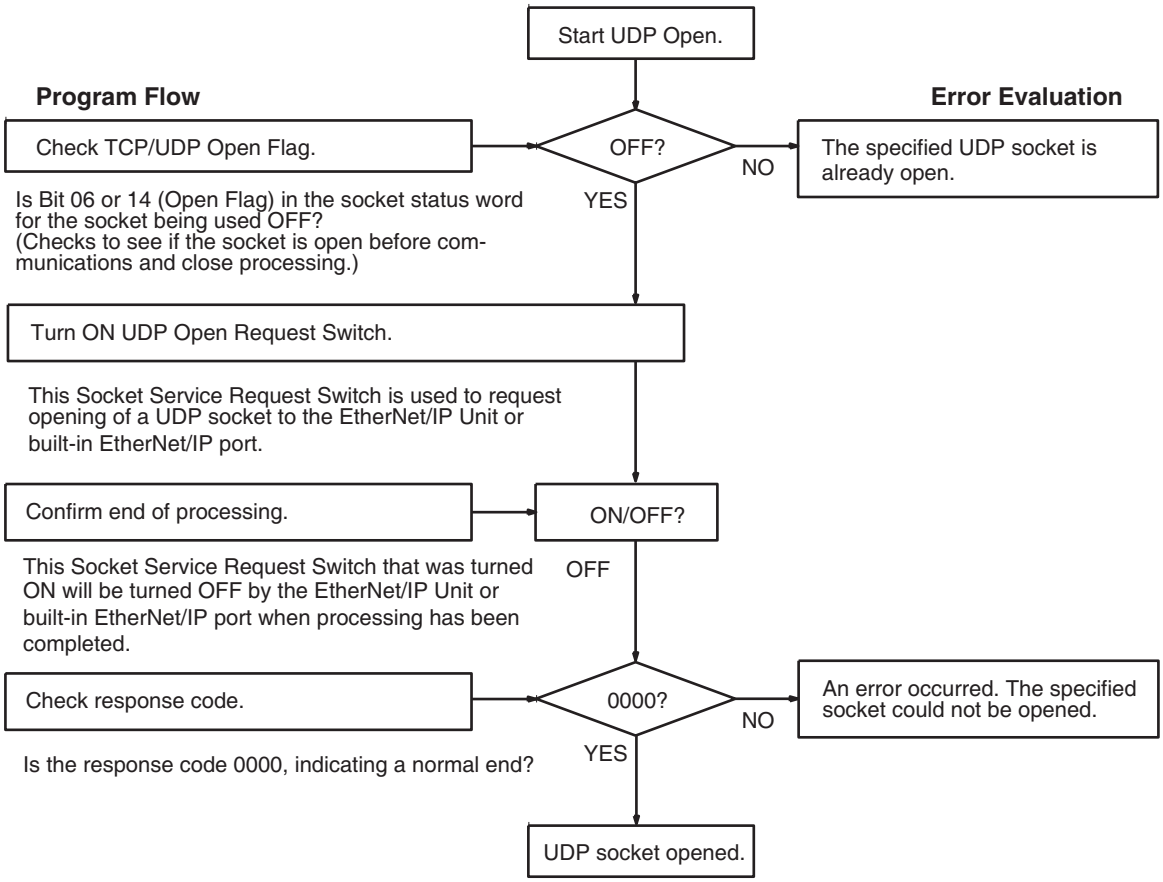
Precautions

A Socket Service Parameter Area cannot be used for other sockets once open processing has been successfully completed for it. Check the socket status before attempting to open a socket. TCP socket status is provided in words m+9 to m+16 in the DM Area for sockets 1 to 8.

The performance of sending and receiving has been improved using optional settings for the TCP or UDP socket services using specific bits. Also, a linger socket option can be used with the TCP socket services. Selecting this option enables immediate open processing using the same ports without having to wait (approximately 1 min.) until the port number opens after the socket closes.

14-5-2 Socket Services and Socket Status

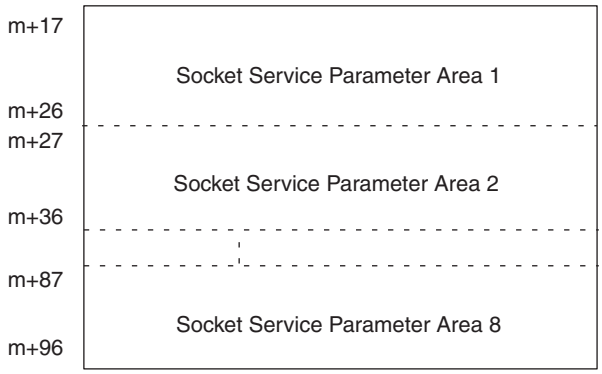
When using socket services, it is important to consider the timing of the status changes in the Socket Status Area. The diagram below shows a flowchart for opening UDP.The flow is similar for other socket services. Replace the names of the appropriate flags in the flowchart to adapt it to other socket services.



14-5-3 Socket Service Parameters

The Socket Service Parameter Areas in which parameters are set to request socket services are in the CPU Bus Unit Area in the DM Area of the CPU Unit. The Socket Service Parameter Areas are allocated as shown in the following diagrams. The first word of in the DM Area allocated to the Ethernet Unit as a CPU Bus Unit is referred to as “m” and is calculated as follows:

m = D30000 + (100 × unit number)



The configuration of each of the Socket Service Parameter Areas is shown in the following diagram.

Offset	15 14 13 12 11 10 09 08	07 06 05 04 03 02 01 00
+0	Socket option	UDP/TCP socket No.
+1	Local UDP/TCP port No. (0000 to FFFF Hex)	
+2	Remote IP address (00000000 to FFFFFFFF Hex)	
+3		
+4	Remote UDP/TCP port No. (0000 to FFFF Hex)	
+5	Number of bytes to send/receive (0000 to 07C0 Hex)	
+6	Send/Receive data address	
+7		
+8	Time out time (0000 to FFFF Hex)	
+9	Response code	

Parameter Settings

The following table shows the parameters that are required for each service and the use of the parameters by the socket service.

UDP Socket Services

Parameter	No. of words	Range (decimal values in parentheses)	Socket service			
			UDP open	UDP receive	UDP send	UDP close
Socket option	1	Specified bit	---	---	---	---
UDP/TCP socket No.		0001 to 0008 hexadecimal (1 to 8)	W	W	W	W
Local UDP/TCP port No.	1	0000 to FFFF hexadecimal (0 to 65,535)	W	---	---	---
Remote IP address	2	00000000 to FFFFFFFF hexadecimal (0.0.0.0 to 255.255.255.255)	---	R	W	---
Remote UDP/TCP port No.	1	0000 to FFFF hexadecimal (0 to 65,535)	---	R	W	---
Number of bytes to send/receive	1	0000 to 07C0 hexadecimal (0 to 1,984 bytes)	---	RW	RW	---
Send/Receive data address	2	Memory area address	---	W	W	---
Time out time (Unit: 100 ms)	1	0000 to FFFF hexadecimal (0 to 65,535) (0: No limit, 0.1 to 6,553.5 s)	---	W	---	---
Response code	1	---	R	R	R	R

Note
W: Written by user
RW: Written by user at execution and then read for results at completion
R: Read by user for results at completion
---: Not used.

TCP Socket Services

Parameter	No. of words	Range (decimal values in parentheses)	Socket service				
			TCP passive open	TCP active open	TCP receive	TCP send	TCP close
Socket option	1	Specified bit	W	W	---	---	---
UDP/TCP socket No.		0001 to 0008 hexadecimal (1 to 8)	W	W	W	W	W
Local UDP/TCP port No.	1	0000 to FFFF hexadecimal (0 to 65,535)	W	RW	---	---	---
Remote IP address	2	00000000 to FFFFFFFF hexadecimal (0.0.0.0 to 255.255.255.255	RW	W	---	---	---
Remote UDP/TCP port No.	1	0000 to FFFF hexadecimal (0 to 65,535)	RW	W	---	---	---
Number of bytes to send/ receive	1	0000 to 07C0 hexadecimal (0 to 1,984 bytes)	---	---	RW	RW	---
Send/Receive data address	2	Memory area address	---	---	W	W	---
Time out time (Unit: 100 ms)	1	0000 to FFFF hexadecimal (0 to 65,535) (0: No limit, 0.1 to 6,553.5 s)	W	---	W	---	---
Response code	1	---	R	R	R	R	R

Note
W: Written by user
RW: Written by user at execution and then read for results at completion
R: Read by user for results at completion
---: Not used.

14-5-4 Parameters

■ **Socket Option**

For the TCP OPEN REQUEST (ACTIVE or PASSIVE) command, specifies whether or not the keep-alive function is to be used. When the keep-alive function is used, bit 8 is ON (set to 1).

Turn ON bit 9 (set to 1) to use the linger function.

■ **UDP/TCP Socket No.**

Specify the number of the UDP or TCP socket to open.

■ **Local UDP/TCP Port No.**

Specify the number of the UDP or TCP port for the socket to use for communications.

- At the time of UDP OPEN REQUEST, do not specify the ports that are used as FINS UDP port number (default value: 9600) and UDP port number for CIP communications (default value: 2222, 44818).
- At the time of TCP OPEN REQUEST, do not specify FTP server TCP port numbers 20 and 21, and FINS TCP port number (default value: 9600).
- As a rule, use port numbers 1,024 and higher.

If port number 0 is specified when for an active TCP open, the TCP port number will be automatically allocated and the number of the port that was opened will be stored in the local UDP/TCP port number in the Socket Service Parameter Area (i.e., the actual port number will be overwritten on the value of 0 set by the user).

■ **Remote IP Address**

Specify the IP address of the remote device.

- Offset +2 in the Socket Service Parameter Area contains the upper bytes of the Remote IP Address, and offset +3 contains the lower bytes.
  Example: The contents of offsets +2 and +3 would be as shown below when the Remote IP Address is 196.36.32.55 (C4.24.20.37 hexadecimal).
  +2: C424
  +3: 2037
- This parameter is not used when making a receive request for a UDP socket. The remote IP address will be stored with the response data and will be written as the Remote IP Address in the Socket Service Parameter Area.
- When opening a passive TCP socket, the combination of the remote IP address and the remote TCP port number can be used to affect processing as shown in the following table.

Remote IP Address	Remote TCP Port No.	Processing
0	0	All connection requests accepted.
0	Not 0	Connection requests accepted only for the same port number.
Not 0	0	Connection requests accepted only for the same IP address.
Not 0	Not 0	Connection requests accepted only for the same port number and IP address.

If the Remote IP Address is set to 0, a connection can be made to any remote node and the remote IP address of the node that is connected will be stored as the Remote IP Address in the Socket Service Parameter Area. If a specific remote I/O address is set, then a connection can be made only to the node with the specified address.

If the Remote TCP Port No. is set to 0, a connection can be made to any remote node regardless of the TCP port number it is using. If a specific remote TCP port number is set, then a connection can be made only to a node using the specified TCP port number.

■ Remote UDP/TCP Port No.

Specify the UDP or TCP port number used by the remote device.

- This parameter is not used when making a receive request for a UDP socket. The remote UDP/TCP port number will be stored with the response data and will be written as the Remote UDP/TCP Port No. in the Socket Service Parameter Area.
- When opening a passive TCP socket, the combination of the remote IP address and the remote TCP port number can be used to affect processing as shown in the table for the Remote IP Address, above. If the Remote UDP/TCP Port No. is set to 0, the UDP/TCP port number of the remote device will be written as the Remote UDP/TCP Port No. in the Socket Service Parameter Area.

■ Time Out Time

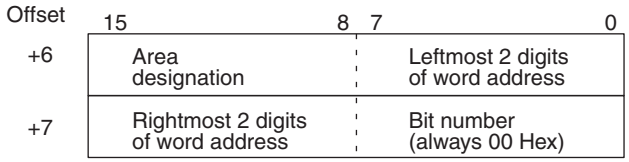
Set the time limit in units of 0.1 s for completion of communications from the time that the Receive Request Switch (TCP or UDP) or the TCP Passive Open Request Switch is turned ON. A response code of 0080 hexadecimal (timeout) will be stored if communications time out. If 0 is set, the requested service will not be timed.

■ Number of Bytes to Send/Receive

Send the number of bytes to be sent or the number of bytes to receive. When the transfer has been completed, the actual number of bytes that have been sent or received will be written here.

■ Send/Receive Data Address

Specify the address of the first word to send or the address of the first word where data is to be received. Always set the bit number to 00 hexadecimal.



The following specifications can be used.

Area		Word address	Area designation (hexadecimal)	Word address (hexadecimal)
CIO, HR, and AR Areas	CIO	0000 to 6143	B0	0000 to 17FF
	HR	H000 to H511	B2	0000 to 01FF
	AR	A448 to A959	B3	01C0 to 03BF
DM Area	DM	D00000 to D32767	82	0000 to 7FFF

EM Area	Bank 0 : Bank 18	E0_00000 to E0_32767 : E18_00000 to E18_32767	A0 : A0~AF or 50~5F	0000 to 7FFF : 0000 to 7FFF

14-5-5 Socket Service Request Switches

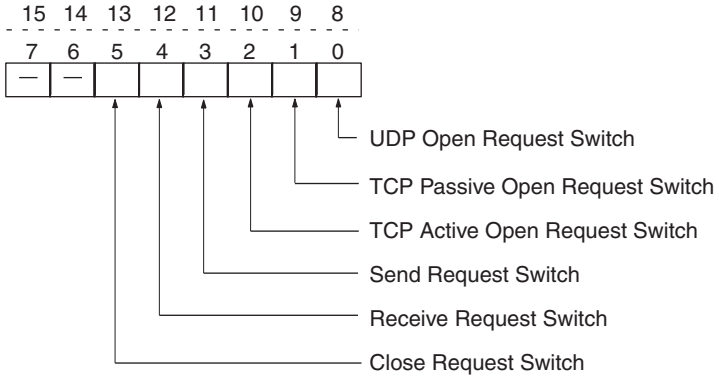
Dedicated control bits can be manipulated to request socket services. These bits are called Socket Service Request Switches, and are turned ON in the CPU Unit to request socket services through the Ethernet Unit.

The Socket Service Request Switches are allocated in the CPU Bus Unit Area in the CIO Area starting at the word n + 19. The value of n can be calculated from the unit number as follows:

n = CIO 1500 + (25 × unit number)

Offset	15 to 08	07 to 00
n+1	Socket Service Request Switch 2	Socket Service Request Switch 1
n+2	Socket Service Request Switch 4	Socket Service Request Switch 3
n+3	Socket Service Request Switch 6	Socket Service Request Switch 5
n+4	Socket Service Request Switch 8	Socket Service Request Switch 7

The configuration of each set of Socket Service Request Switches is shown in the following diagram.



Bit		Switch	Status	Manipulated by	Unit operation
08	00	UDP Open Request Switch	ON	User	UDP socket opened when switch is turned ON.
			OFF	Unit	Unit turns OFF switch when open processing has been completed (i.e., when a connection has been made).
09	01	TCP Passive Open Request Switch	ON	User	Passive TCP socket opened when switch is turned ON.
			OFF	Unit	Unit turns OFF switch when open processing has been completed (i.e., when a connection has been made).
10	02	TCP Active Open Request Switch	ON	User	Active TCP socket opened when switch is turned ON.
			OFF	Unit	Unit turns OFF switch when open processing has been completed (i.e., when a connection has been made).
11	03	Send Request Switch	ON	User	Send processing executed when switch is turned ON. (The protocol (TCP/UDP) is determined when the socket is opened.)
			OFF	Unit	Unit turns OFF switch when send processing has been completed.

Bit		Switch	Status	Manipulated by	Unit operation
12	04	Receive Request Switch	ON	User	Receive processing executed when switch is turned ON. (The protocol (TCP/UDP) is determined when the socket is opened.)
			OFF	Unit	Unit turns OFF switch when receive processing has been completed.
13	05	Close Request Switch	ON	User	Close processing executed when switch is turned ON. (The protocol (TCP/UDP) is determined when the socket is opened.)
			OFF	Unit	Unit turns OFF switch when close processing has been completed.

As shown in the above table, the Request Switches are turned OFF by the EtherNet/IP Unit or built-in EtherNet/IP port when the requested processes has been completed.

Note There is also a Socket Force-close Switch in bit 10 of the first word allocated to the Ethernet Unit in the CPU Bus Unit Area in the CIO Area. When the Socket Force-close Switch is turned ON, all sockets that are open will be force-closed. Refer to *SECTION 4 Memory Allocations* for details.

When using socket services with the Socket Service Request Switches, the ladder diagram should be programmed to check the response codes when Socket Service Request Switches are turned OFF.

14-5-6 Response Codes

When processing of a request has been completed for socket services executed using Socket Service Request Switches, a response code will be stored in the Response Code word in the Socket Service Parameter Area. The following response codes will be stored depending on the service that was requested.

UDP Socket Open Request

Response code	Meaning
0000	Normal end
0105	Local IP address setting error.
0302	CPU Unit error; cannot execute.
1100	UDP socket number is not 1 to 8 or local UDP port number is 0.
110C	Request Switch turned ON during other processing.
220F	Specified socket is already open.
2211	Unit is busy; cannot execute.
2606	Specified socket is already open as TCP socket; cannot open UDP socket.
2607	Specified Socket Service Parameter Area is already being used for another socket.
003E	Internal buffer cannot be obtained due to high reception traffic (ENOBUFS).
0049	The same UDP port number has been specified more than once (EADDRINUSE).
0081	The specified socket was closed during open processing.

UDP Socket Receive Request

Response code	Meaning
0000	Normal end
0302	CPU Unit error; cannot execute.
1100	Number of bytes to receive is not in allowable range.
1101	The area designation of the Send/Receive Data Address is not in allowable range.
1103	The bit number in the Send/Receive Data Address is not 00.
110C	Request Switch turned ON during other processing.
220F	Specified socket is already processing a receive request.
2210	The specified socket is not open.
2211	Unit is busy; cannot execute service.
2607	Specified Socket Service Parameter Area is already being used for another socket.
003E	Internal buffer cannot be obtained due to high reception traffic (ENOBUFS).
0066	Internal memory cannot be obtained; cannot execute service.
0080	Receive request timed out.
0081	The specified socket was closed during reception processing.

UDP Socket Send Request

Response code	Meaning
0000	Normal end
0302	CPU Unit error; cannot execute.
1100	Number of bytes to send is not in allowable range or the remote IP address is 0.
1101	The area designation of the Send/Receive Data Address is not in allowable range.
1103	The bit number in the Send/Receive Data Address is not 00.
110C	Request Switch turned ON during other processing.
220F	Specified socket is already processing a send request.
2210	The specified socket is not open.
2211	Unit is busy; cannot execute.
2607	Specified Socket Service Parameter Area is already being used for another socket.
003E	Internal buffer cannot be obtained due to high reception traffic (ENOBUFS).
0042	The remote IP address is a broadcast address and the number of bytes to send is greater than 1,472 bytes (EMSGSIZE).
004C	The network ID is incorrect or the remote IP address is incorrect (EADDRNOTAVAIL)
004E	The network ID is not in the IP router table, router settings are incorrect, or the remote IP address is incorrect (ENETUNREACH).
0051	The router settings are incorrect or the remote IP address is incorrect (EHOSTUNREACH).
0081	The specified socket was closed during send processing.

UDP Socket Close Request

Response code	Meaning
0000	Normal end
0302	CPU Unit error; cannot execute.

Response code	Meaning
2210	The specified socket is not open.
2211	Unit is busy; cannot execute.
2607	Specified Socket Service Parameter Area is already being used for another socket.

TCP Socket Passive Open Request

Response code	Meaning
0000	Normal end
0105	Local IP address setting error.
0302	CPU Unit error; cannot execute.
1100	TCP socket number is not 1 to 8 or local TCP port number is 0.
110C	Request Switch turned ON during other processing.
220F	Specified socket is already open or already processing an open request.
2211	Unit is busy; cannot execute.
2606	Specified socket is already open as UDP socket; cannot open TCP socket.
2607	Specified Socket Service Parameter Area is already being used for another socket.
003E	Internal buffer cannot be obtained due to high reception traffic (ENOBUFS).
0042 (See note.)	An error occurred. (EMSGSIZE).
0045	Error in communications with remote node (ECONNABORTED).
0049	The same TCP port number has been specified more than once (EADDRINUSE).
004A (See note.)	Error (ECONNREFUSED).
004B (See note.)	Error in communications with remote node (ECONNRESET).
004E (See note.)	Remote IP address parameter error (ENETUNREACH).
0051 (See note.)	Remote IP address parameter error (EHOSTUNREACH).
0053	Error in communications with remote node (ETIMEDOUT) or remote node does not exist.
0066	Internal memory cannot be obtained; cannot execute.
0080	Open request timed out.
0081	The specified socket was closed during open processing.
0082	Connection could not be established with specified remote node.

Note These response codes will be returned only on large, multilevel networks.

TCP Socket Active Open Request

Response code	Meaning
0000	Normal end
0105	Local IP address setting error.
0302	CPU Unit error; cannot execute.
1100	TCP socket number is not 1 to 8 or local TCP port number is 0.
110C	Request Switch turned ON during other processing.

Response code	Meaning
220F	Specified socket is already open or already processing an open request.
2211	Unit is busy; cannot execute.
2606	Specified socket is already open as UDP socket; cannot open TCP socket.
2607	Specified Socket Service Parameter Area is already being used for another socket.
000D	Remote IP address parameter error (EACCES).
003E	Internal buffer cannot be obtained due to high reception traffic (ENOBUFS).
0042 (See note.)	Error (EMSGSIZE).
0044	ICMP data received (ENOPROTOOPT).
0045	Error in communications with remote node (ECONNABORTED).
0049	The same port number has been specified more than once (EADDRINUSE).
004A	Error (ECONNREFUSED) or the remote node has not been opened as passive socket.
004B (See note.)	Error in communications with remote node (ECONNRESET).
004C	Remote IP address parameter error (EADDRNOTAVAIL). Wrong parameter designation. An attempt was made to set the local TCP port of the local node to Active Open.
004E	Remote IP address parameter error (ENETUNREACH). The network ID is not in the IP router table or router settings are incorrect.
0051	Remote IP address parameter error (EHOSTUNREACH). The router settings are incorrect.
0053	Communications error with remote node (ETIMEDOUT). No remote node.
0081	The specified socket was closed during open processing.

Note These response codes will be returned only on large, multilevel networks.

TCP Socket Receive Request

Response code	Meaning
0000	Normal end
0302	CPU Unit error; cannot execute.
1100	Number of receive bytes not in allowable range.
1101	The area designation of the Send/Receive Data Address is not in allowable range.
1103	The bit number in the Send/Receive Data Address is not 00.
110C	Request Switch turned ON during other processing.
220F	Specified socket is already processing a receive request.
2210	Specified socket has not been connected.
2211	Unit is busy; cannot execute.
2607	Specified Socket Service Parameter Area is already being used for another socket.
003E	Internal buffer cannot be obtained due to high reception traffic (ENOBUFS).
0042 (See note.)	ICMP data received (EMSGSIZE).

Response code	Meaning
0044 (See note.)	ICMP data received (ENOPROTOOPT).
0045 (See note.)	Error in communications with remote node (ECONNABORTED).
004B	Error in communications with remote node (ECONNRESET).
004E (See note.)	ICMP data received (ENETUNREACH).
004F (See note.)	ICMP data received (EHOSTDOWN).
0051 (See note.)	ICMP data received (EHOSTUNREACH).
0053	Error in communications with remote host (ETIMEDOUT).
0066	Internal memory cannot be obtained; cannot execute.
0080	Receive request timed out.
0081	The specified socket was closed during receive processing.

Note These response codes will be returned only on large, multilevel networks.

TCP Socket Send Request

Response code	Meaning
0000	Normal end
0302	CPU Unit error; cannot execute.
1100	Number of bytes to send not in allowable range.
1101	The area designation of the Send/Receive Data Address is not in allowable range.
1103	The bit number in the Send/Receive Data Address is not 00.
110C	Request Switch turned ON during other processing.
220F	Specified socket is already processing a send request.
2210	The specified socket is not been connected.
2211	Unit is busy; cannot execute.
2607	Specified Socket Service Parameter Area is already being used for another socket.
0020	Connection with remote socket broken during send (EPIPE).
003E	Internal buffer cannot be obtained due to high reception traffic (ENOBUFS).
0042 (See note.)	The remote IP address is a broadcast address and the number of bytes to send is greater than 1,472 bytes (EMSGSIZE).
0044 (See note.)	ICMP data received (ENOPROTOOPT).
0045 (See note.)	Error in communications with remote node (ECONNABORTED).
004A	Error in communications with remote node (ECONNREFUSED).
004B (See note.)	Error in communications with remote node (ECONNRESET).
004E (See note.)	Remote IP address parameter error (ENETUNREACH).
004F (See note.)	ICMP data received (EHOSTDOWN).
0051 (See note.)	Remote IP address parameter error (EHOSTUNREACH).

Response code	Meaning
0053 (See note.)	Error in communications with remote node (ETIMEDOUT).
0081	The specified socket was closed during send processing.

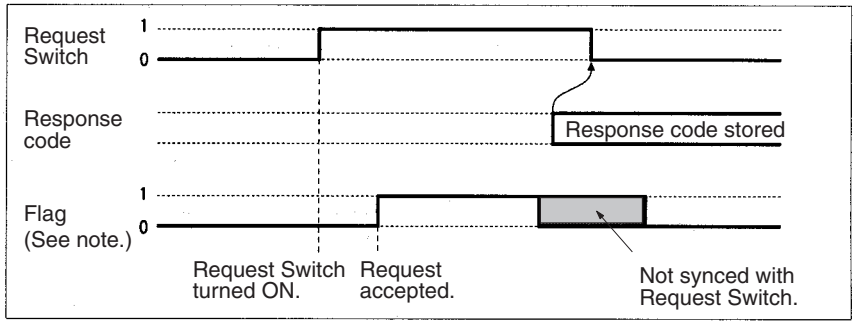
Note These response codes will be returned only on large, multilevel networks.

TCP Socket Close Request

Response code	Meaning
0000	Normal end
0302	CPU Unit error; cannot execute.
2210	The specified socket is not been connected.
2211	Unit is busy; cannot execute.
2607	Specified Socket Service Parameter Area is already being used for another socket.

14-5-7 Timing Charts

The timing of flags for socket services (Opening, Receiving, Sending, or Closing Flag) when the Request Switches are used and the changes in the response code are shown in the following chart.



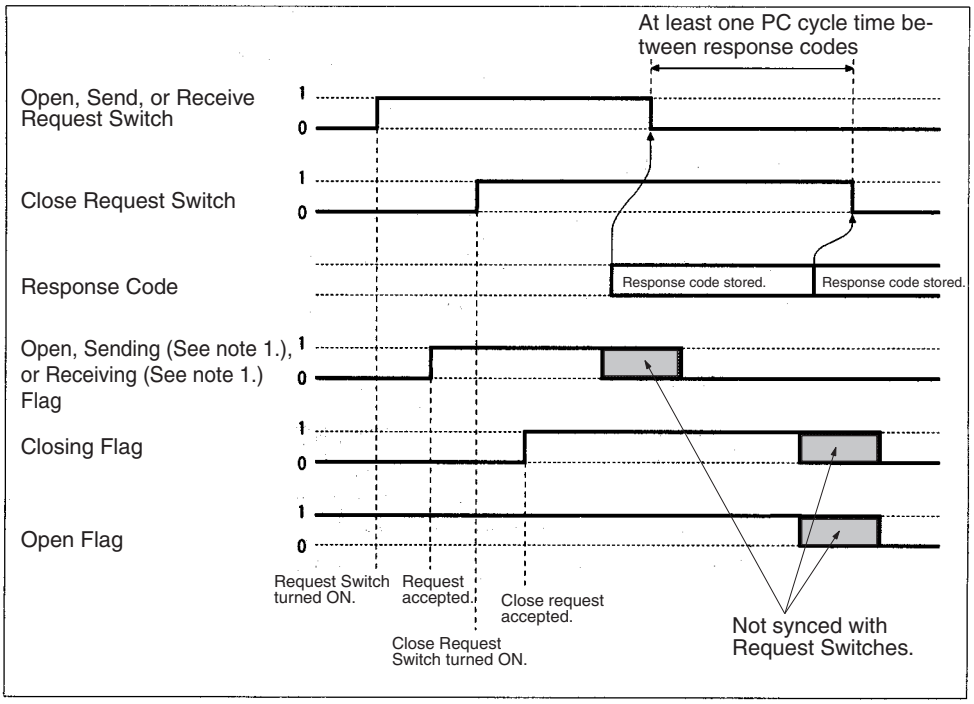
Note The Sending Flag and Receiving Flag will not turn ON if the high-speed socket service option is selected. Therefore, the program can be controlled only by setting the Send Request Switch and Receive Request Switch to OFF.

Closing during Other Processes

The Close Request Switch or Force-close Switch can be used to close a socket even when open, receive, or send processing is being executed. Closing is the only other process that is possible during other processes.

Close Request Switch

The processing results are stored as the response code when the Close Request Switch is used. There will always be one PLC cycle time between turning OFF the Request Switch for the canceled process and turning of the Close Request Switch, allowing time for the response code to be read.

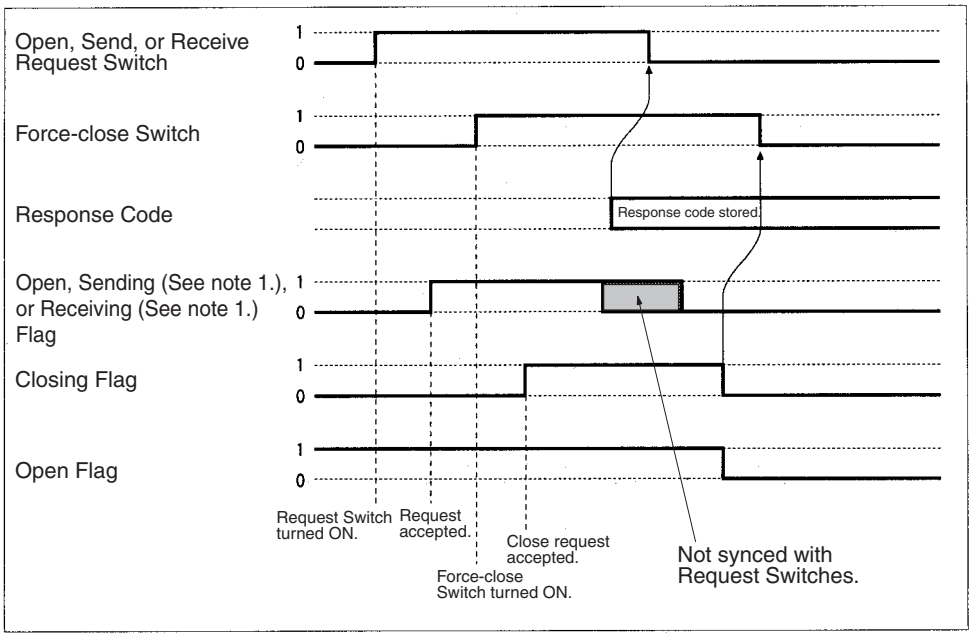


Note

1. The Sending Flag and Receiving Flag will not turn ON if the high-speed socket service option is selected.
2. The Open Flag will not turn ON at all if a close request is made during open processing.

Force-close Switch

The requested processes are canceled and an response code is stored when the Force-close Switch is used.



Note

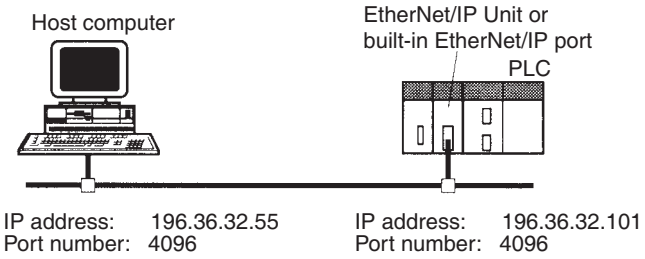
1. The Sending Flag and Receiving Flag will not turn ON if the high-speed socket service option is selected.
2. The Open Flag will not turn ON at all if a force-close request is made during open processing.

14-5-8 TCP/IP Communications Programming Example (Using Socket Services by Manipulating Dedicated Control Bits)

The following programming example illustrates transferring 100 bytes of data between an EtherNet/IP Unit or built-in EtherNet/IP port and a host computer using TCP/IP communications.

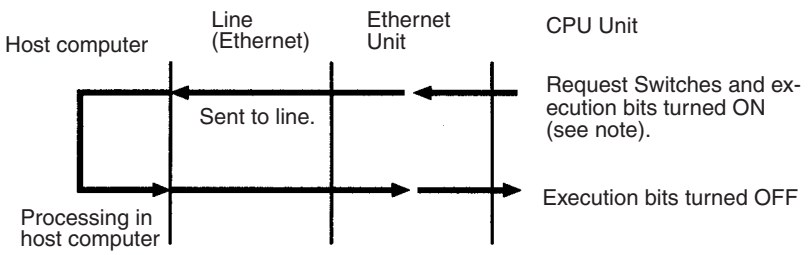
System Configuration

The programming example uses the following system configuration. For the TCP connection, the EtherNet/IP Unit or built-in EtherNet/IP port uses a passive open and the host computer uses an active open.



Data Flow

The data will flow between the CPU Unit, EtherNet/IP Unit or built-in EtherNet/IP port, and host computer as shown in the following diagram.



Note Here, "execution bits" refer to CIO 0000.00 to CIO 0000.03, which are used in the ladder diagram to control execution of communications.

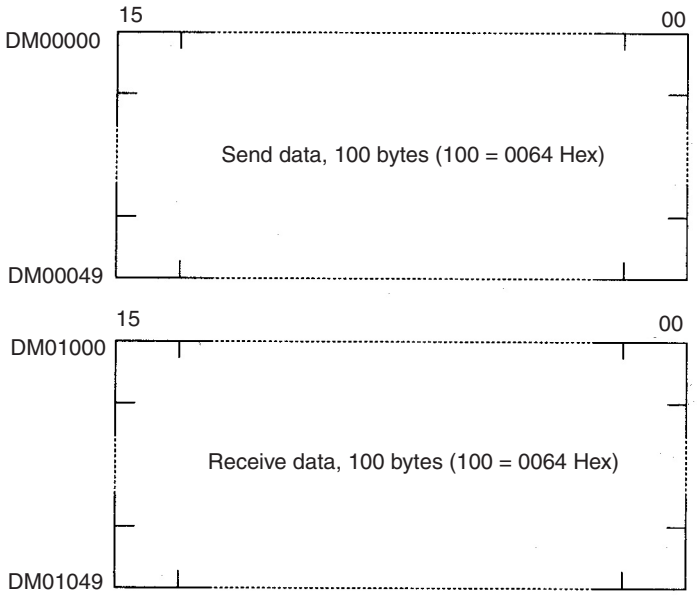
Basic Operations

- CIO 0000.00 is turned ON to request opening a TCP socket from the EtherNet/IP Unit or built-in EtherNet/IP port.
- CIO 0000.01 is turned ON to request closing the TCP socket from the EtherNet/IP Unit or built-in EtherNet/IP port.
- CIO 0000.02 is turned ON to request sending data from the EtherNet/IP Unit or built-in EtherNet/IP port. Data (100 bytes) is sent beginning at D00000.
- CIO 0000.03 is turned ON to request receiving data from the EtherNet/IP Unit or built-in EtherNet/IP port. The data that is received (100 bytes) is stored beginning at D01000.
- One of the bits between CIO 0001.00 and CIO 0001.03 will turn ON if an error occurs. Refer to *14-5-6 Response Codes* for information on errors.

Program Memory Map

The send and receive data and bits (flags) used by the program are shown in the following diagram.

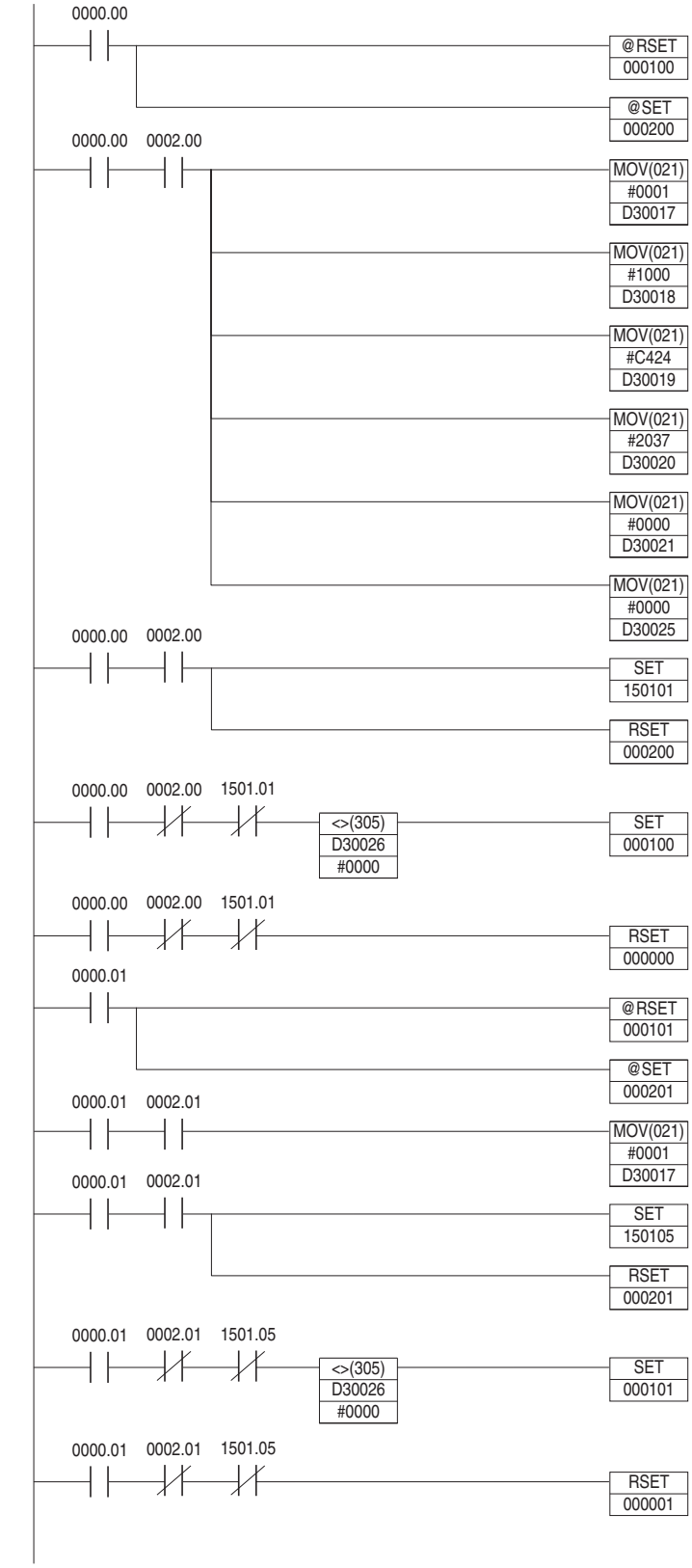
DM Area



CIO Area

	15 …	03	02	01	00
CIO 0000		TCP Receive Bit	TCP Send Bit	TCP Close Bit	TCP Open Bit
CIO 0001		TCP Receive Error Flag	TCP Send Error Flag	TCP Close Error Flag	TCP Open Error Flag
CIO 0002		TCP Receiving Flag	TCP Sending Flag	TCP Closing Flag	TCP Opening Flag

Programming Example



TCP Passive Open

When the TCP Open Bit (CIO 0000.00) turns ON, the TCP Open Error Flag (CIO 0001.00) is turned OFF and the TCP Opening Flag (CIO 0002.00) is turned ON to initialize processing.

When the TCP Opening Flag (CIO 0002.00) turns ON, the following parameters are written to the parameter area for socket number 1.
D30017: 0001 Hex = UDP/TCP socket No. 1
D30018: 1000 Hex = Local UDP/TCP port No. 4096
D30019 and D30020:
C424 2037 Hex =
Remote IP address 196.36.32.55
D30021: 0000 Hex = Any remote UDP/TCP port No.
D30025: 0000 Hex = No timeout time

After the parameters have been set, the TCP Passive Open Request Switch (CIO 1501.01) is turned ON and the TCP Opening Flag (CIO 0002.00) is turned OFF.

If the TCP Passive Open Request Switch (CIO 1501.01) turns OFF while the TCP Opening Flag (CIO 0002.00) is OFF, the contents of the response code (D30026) in the Socket Service Parameter Area is checked, and if it is not 0000 Hex (normal end), the TCP Open Error Flag (CIO 0001.00) is turned ON.

After the execution results have been checked, the TCP Open Bit (CIO 0000.00) is turned OFF.

TCP Close

When the TCP Close Bit (CIO 0000.01) turns ON, the TCP Close Error Flag (CIO 0001.01) is turned OFF and the TCP Closing Flag (CIO 0002.01) is turned ON to initialize processing.

When the TCP Closing Flag (CIO 0002.01) turns ON, the following parameter is written to the parameter area for socket number 1.
D30017: 0001 Hex = UDP/TCP socket No. 1

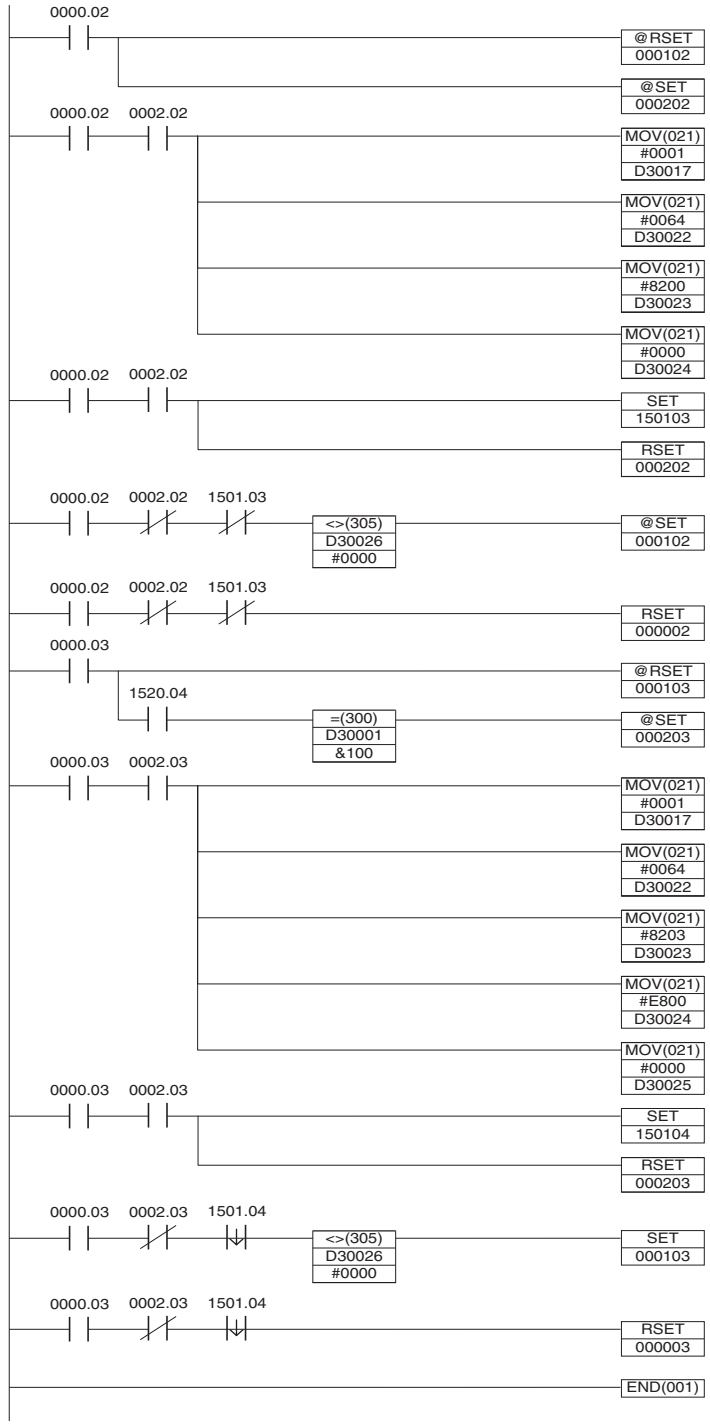
After the parameter has been set, the Close Request Switch (CIO 1501.05) is turned ON and the TCP Closing Flag (CIO 0002.01) is turned OFF.

If the Close Request Switch (CIO 1501.05) turns OFF while the TCP Closing Flag (CIO 0002.01) is OFF, the contents of the response code (D30026) in the Socket Service Parameter Area is checked, and if it is not 0000 Hex (normal end), the TCP Close Error Flag (CIO 0001.01) is turned ON.

After the execution results have been checked, the TCP Close Bit (CIO 0000.01) is turned OFF.

Continued on next page.

Continued from previous page.



TCP Send

When the TCP Send Bit (CIO 0000.02) turns ON, the TCP Send Error Flag (CIO 0001.02) is turned OFF and the TCP Sending Flag (CIO 0002.02) is turned ON to initialize processing.

When the TCP Sending Flag (CIO 0002.02) turns ON, the following parameters are written to the parameter area for socket number 1.
D30017: 0001 Hex = UDP/TCP socket No. 1
D30022: 0064 Hex = No. of send/receive bytes is 100
D30023 and D30024:
8200 0000 Hex =
Send/receive data address D00000

After the parameters have been set, the Send Request Switch (CIO 1501.03) is turned ON and the TCP Sending Flag (CIO 0002.02) is turned OFF.

If the Send Request Switch (CIO 1501.03) turns OFF while the TCP Sending Flag (CIO 0002.02) is OFF, the contents of the response code (D30026) in the Socket Service Parameter Area is checked, and if it is not 0000 Hex (normal end), the TCP Send Error Flag (CIO 0001.02) is turned ON.

After the execution results have been checked, the TCP Send Bit (CIO 0000.02) is turned OFF.

TCP Receive

When the TCP Receive Bit (CIO 0000.03) turns ON, the TCP Receive Error Flag (CIO 0001.03) is turned OFF and the TCP Data Received/Requested Flag (CIO 1520.04), and the Number of Bytes Received at TCP Socket (D30001) are checked. If the data is stored in the buffer, the TCP Receiving Flag (CIO 0002.03) turns ON.
When the TCP Receiving Flag (CIO 0002.03) turns ON, the following parameters are written to the parameter area for socket number 1.
D30017: 0001 Hex = UDP/TCP socket No. 1
D30022: 0064 Hex = No. of send/receive bytes is 100
D30023 and D30024:
8203 E800 Hex =
Send/receive data address D01000
D30025: 0000 Hex = No timeout time.

After the parameter has been set, the Receive Request Switch (CIO 1501.04) is turned ON and the TCP Receiving Flag (CIO 0002.03) is turned OFF.

If the Receive Request Switch (CIO 1501.04) turns OFF while the TCP Receiving Flag (CIO 0002.03) is OFF, the contents of the response code (D30026) in the Socket Service Parameter Area is checked, and if it is not 0000 Hex (normal end), the TCP Receive Error Flag (CIO 0001.03) is turned ON.

After the execution results have been checked, the TCP Receive Bit (CIO 0000.03) is turned OFF.

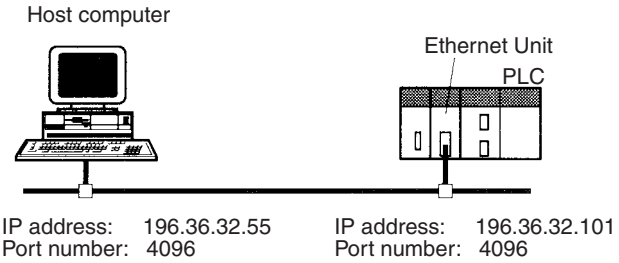
Note When using the above programming example, change the bit and word addresses as necessary to avoid using the same areas used by other parts of the user program or the CPU Bus Unit.

14-5-9 UDP/IP Communications Programming Example (Using Socket Services by Manipulating Dedicated Control Bits)

The following programming example illustrates transferring 100 bytes of data between an Ethernet Unit and a host computer using UDP/IP communications.

System Configuration

The programming example uses the following system configuration.



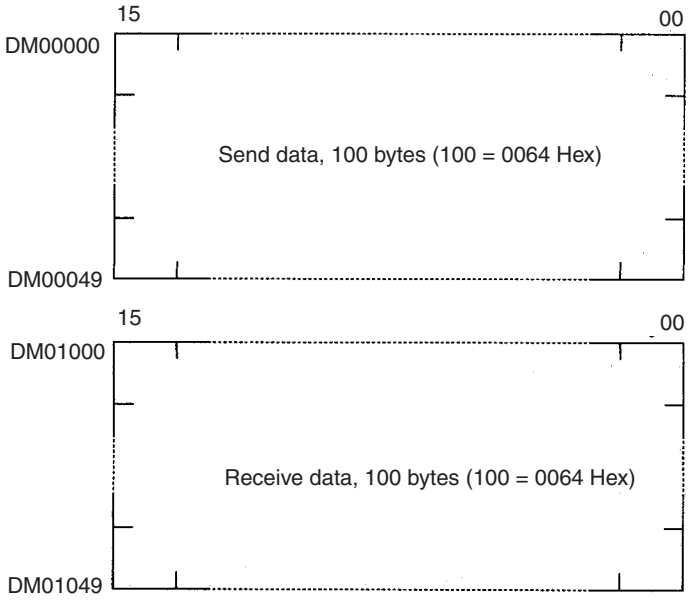
Basic Operations

- CIO 0000.00 is turned ON to request opening a UDP socket from the Ethernet Unit.
- CIO 0000.01 is turned ON to request closing the UDP socket from the Ethernet Unit.
- CIO 0000.02 is turned ON to request sending data from the Ethernet Unit. The data is sent (100 bytes) beginning from word D000.00.
- CIO 0000.03 is turned ON to request receiving data from the Ethernet Unit. The data that is received (100 bytes) is stored beginning at D010.00.
- One of the bits between CIO 0001.00 and CIO 0001.03 will turn ON if an error occurs. Refer to *14-5-6 Response Codes* for information on errors.

Program Memory Map

The send and receive data and bits (flags) used by the program are shown in the following diagram.

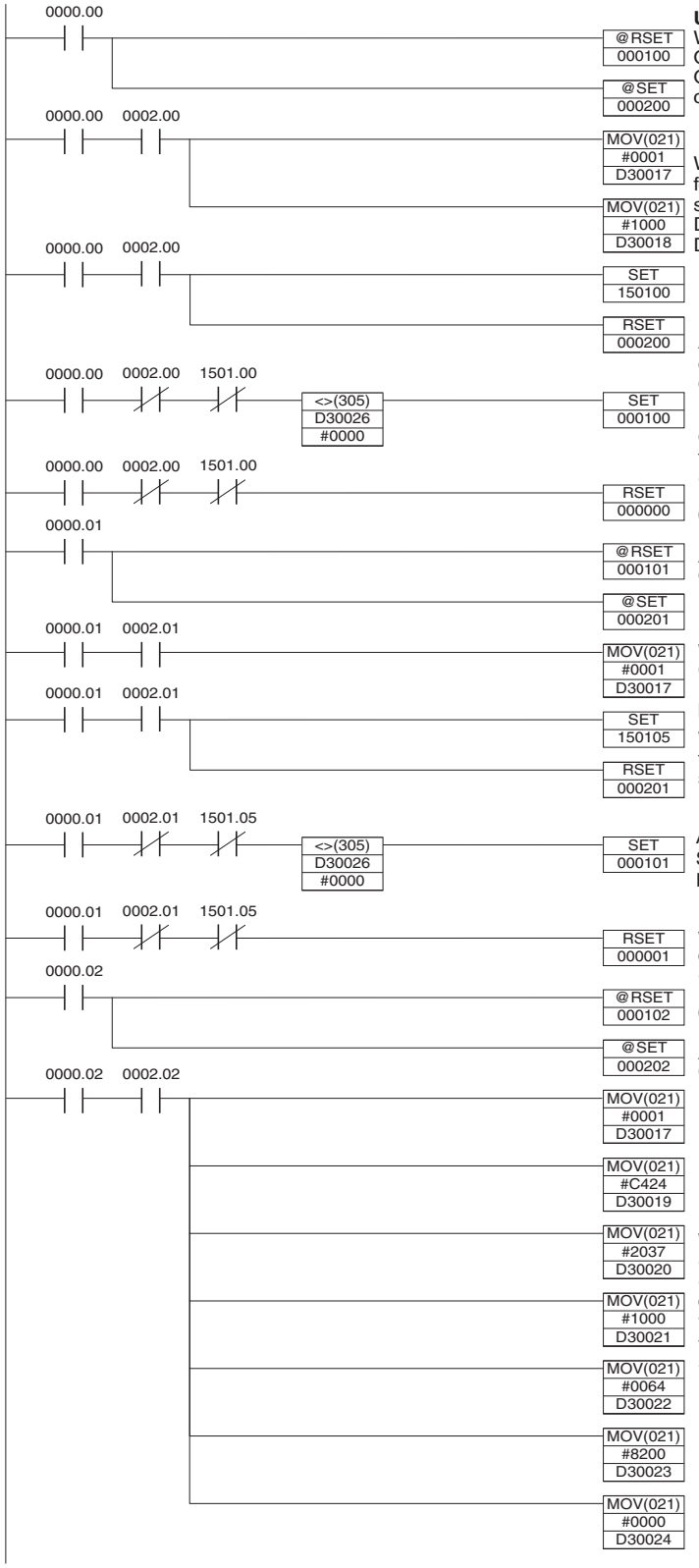
DM Area



CIO Area

	15		03	02	01	00
CIO 0000			UDP Receive Bit	UDP Send Bit	UDP Close Bit	UDP Open Bit
CIO 0001			UDP Receive Error Flag	UDP Send Error Flag	UDP Close Error Flag	UDP Open Error Flag
CIO 0002			UDP Receiving Flag	UDP Sending Flag	UDP Closing Flag	UDP Opening Flag

Programming Example



UDP Open

When the UDP Open Bit (CIO 0000.00) turns ON, the UDP Open Error Flag (CIO 0001.00) is turned OFF and the UDP Opening Flag (CIO 0002.00) is turned ON to initialize processing.

When the UDP Opening Flag (CIO 0002.00) turns ON, the following parameters are written to the parameter area for socket number 1.
D30017: 0001 Hex = UDP/TCP socket No. 1
D30018: 1000 Hex = Local UDP/TCP port No. 4096

After the parameters have been set, the UDP Open Request Switch (CIO 1501.00) is turned ON and the UDP Opening Flag (CIO 0002.00) is turned OFF.

If the UDP Open Request Switch (CIO 1501.00) turns OFF while the UDP Opening Flag (CIO 0002.00) is OFF, the contents of the response code (D30026) in the Socket Service Parameter Area is checked, and if it is not 0000 Hex (normal end), the UDP Open Error Flag (CIO 0001.00) is turned ON.

After the execution results have been checked, the UDP Open Bit (CIO 0000.00) is turned OFF.

UDP Close

When the UDP Close Bit (CIO 0000.01) turns ON, the UDP Close Error Flag (CIO 0001.01) is turned OFF and the UDP Closing Flag (CIO 0002.01) is turned ON to initialize processing.

When the UDP Closing Flag (CIO 0002.01) turns ON, the following parameter is written to the parameter area for socket number 1.
D30017: 0001 Hex = UDP/TCP socket No. 1

After the parameter has been set, the Close Request Switch (CIO 1501.05) is turned ON and the UDP Closing Flag (CIO 0002.01) is turned OFF.

If the Close Request Switch (CIO 1501.05) turns OFF while the UDP Closing Flag (CIO 0002.01) is OFF, the contents of the response code (D30026) in the Socket Service Parameter Area is checked, and if it is not 0000 Hex (normal end), the UDP Close Error Flag (CIO 0001.01) is turned ON.

After the execution results have been checked, the UDP Close Bit (CIO 0000.01) is turned OFF.

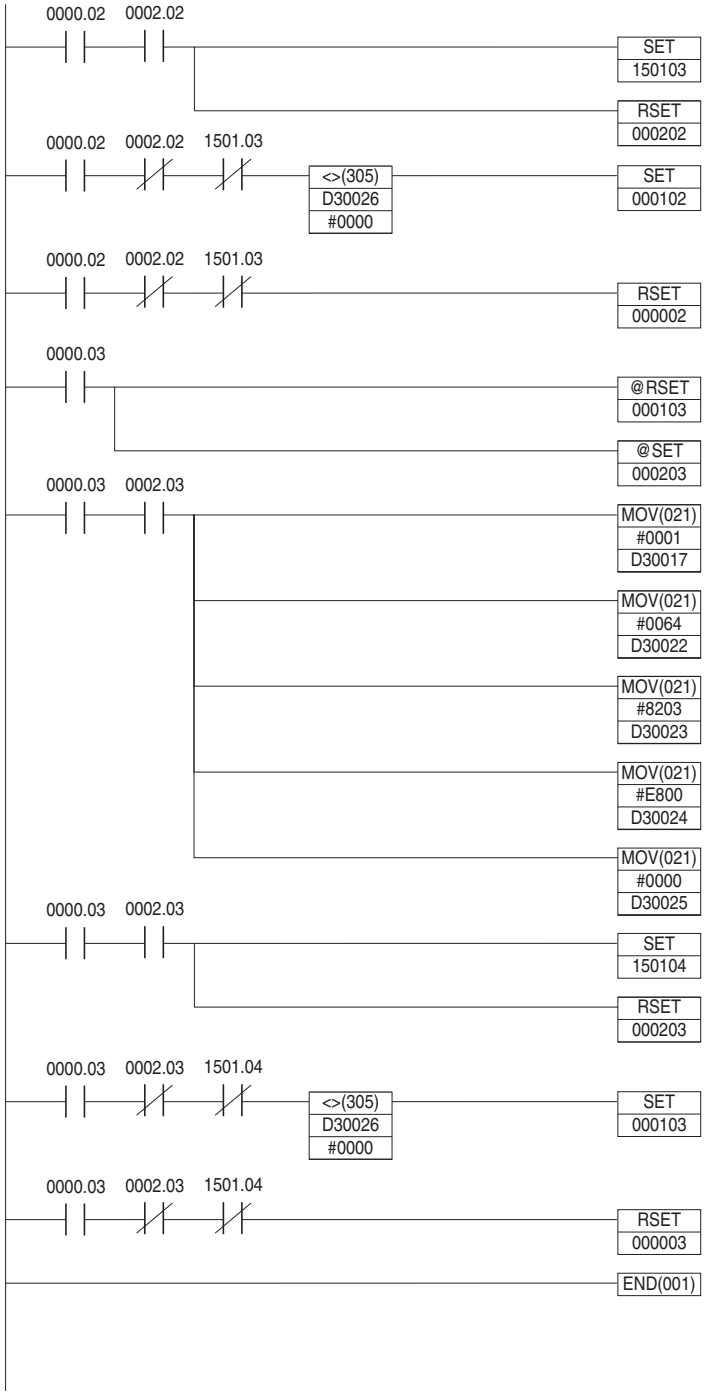
UDP Send

When the UDP Send Bit (CIO 0000.02) turns ON, the UDP Send Error Flag (CIO 0001.02) is turned OFF and the UDP Sending Flag (CIO 0002.02) is turned ON to initialize processing.

When the UDP Sending Flag (CIO 0002.02) turns ON, the following parameters are written to the parameter area for socket number 1.
D30017: 0001 Hex = UDP/TCP socket No. 1
D30019 and D30020:
C424 2037 Hex =
Remote IP address 196.36.32.55
D30021: 1000 Hex = Remote UDP/TCP port No. 4096
D30022: 0064 Hex = No. of send/receive bytes is 100
D30023 and D30024:
8200 0000 Hex =
Send/receive data address D00000

Continued on next page.

Continued from previous page.



After the parameters have been set, the Send Request Switch (CIO 1501.03) is turned ON and the UDP Sending Flag (CIO 0002.02) is turned OFF.

If the Send Request Switch (CIO 1501.03) turns OFF while the UDP Sending Flag (CIO 0002.00) is OFF, the contents of the response code (D30026) in the Socket Service Parameter Area is checked, and if it is not 0000 Hex (normal end), the UDP Send Error Flag (CIO 0001.02) is turned ON.

After the execution results have been checked, the UDP Send Bit (CIO 0000.02) is turned OFF.

UDP Receive

When the UDP Receive Bit (CIO 0000.03) turns ON, the UDP Receive Error Flag (CIO 0001.03) is turned OFF and the UDP Receiving Flag (CIO 0002.03) is turned ON to initialize processing.

When the UDP Receiving Flag (CIO 0002.03) turns ON, the following parameters are written to the parameter area for socket number 1.
D30017: 0001 Hex = UDP/TCP socket No. 1
D30022: 0064 Hex = No. of send/receive bytes is 100
D30023 and D30024:
8203 E800 Hex =
Send/receive data address D01000
D30025: 0000 Hex = No timeout time.

After the parameter has been set, the Receive Request Switch (CIO 1501.04) is turned ON and the UDP Receiving Flag (CIO 0002.03) is turned OFF.

If the Receive Request Switch (CIO 1501.04) turns OFF while the UDP Receiving Flag (CIO 0002.03) is OFF, the contents of the response code (D30026) in the Socket Service Parameter Area is checked, and if it is not 0000 Hex (normal end), the UDP Receive Error Flag (CIO 0001.03) is turned ON.

After the execution results have been checked, the UDP Receive Bit (CIO 0000.03) is turned OFF.

Note When using the above programming example, change the bit and word addresses as necessary to avoid using the same areas used by other parts of the user program or the CPU Bus Unit.

14-6 Using Socket Services with CMND/CMND2

14-6-1 Using Socket Service

Each EtherNet/IP Unit or built-in EtherNet/IP port has eight TCP sockets and eight UDP sockets. Open, close, send, and receive processes are available for communications with sockets.

Open

Enables communications on a specified socket. A socket must be opened before it can be used for socket services. Opening a TCP socket establishes a connection.

Close

Ends use of the socket. Breaks the connection for a TCP socket.

Send

Sends data from a specified open socket.

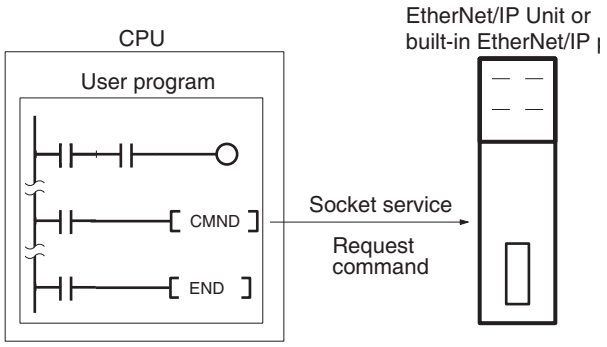
Receive

Specifies an open socket and receives data from that socket.

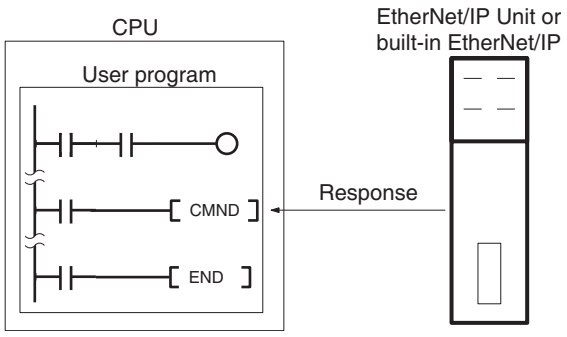
These processes are carried out by sending FINS commands to the Ethernet Unit. The process from sending a request for processing to completion is shown in the following illustrations.

1,2,3... 1. Execute a socket service request command (MRC: 27) for the EtherNet/IP Unit or built-in EtherNet/IP port using CMND.

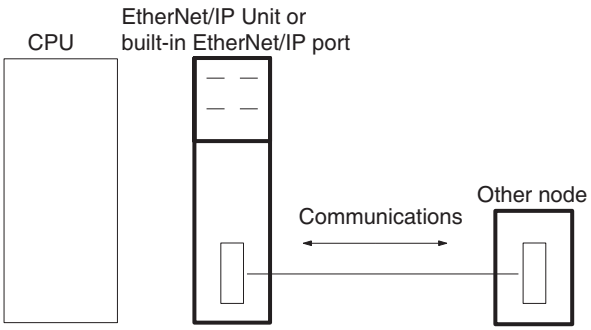
Note The CMND2 instruction is supported by the CJ2 CPU Units. Refer to Network Instructions in the CS/CJ Series Programmable Controllers Instructions Reference Manual (W474) for details on the CMND2 instruction.



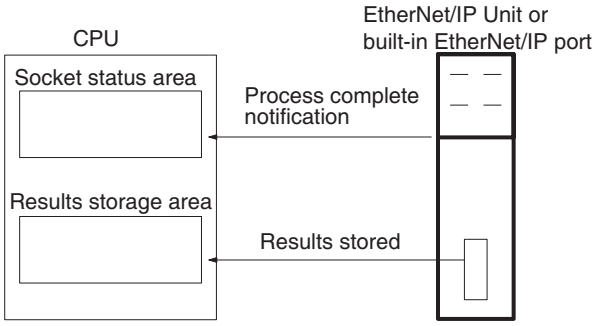
2. CMND ends normally when the socket service request command is received and a response is returned (response code: 0000).



3. The EtherNet/IP Unit or built-in EtherNet/IP port starts the process requested by the parameters in the socket service request command.



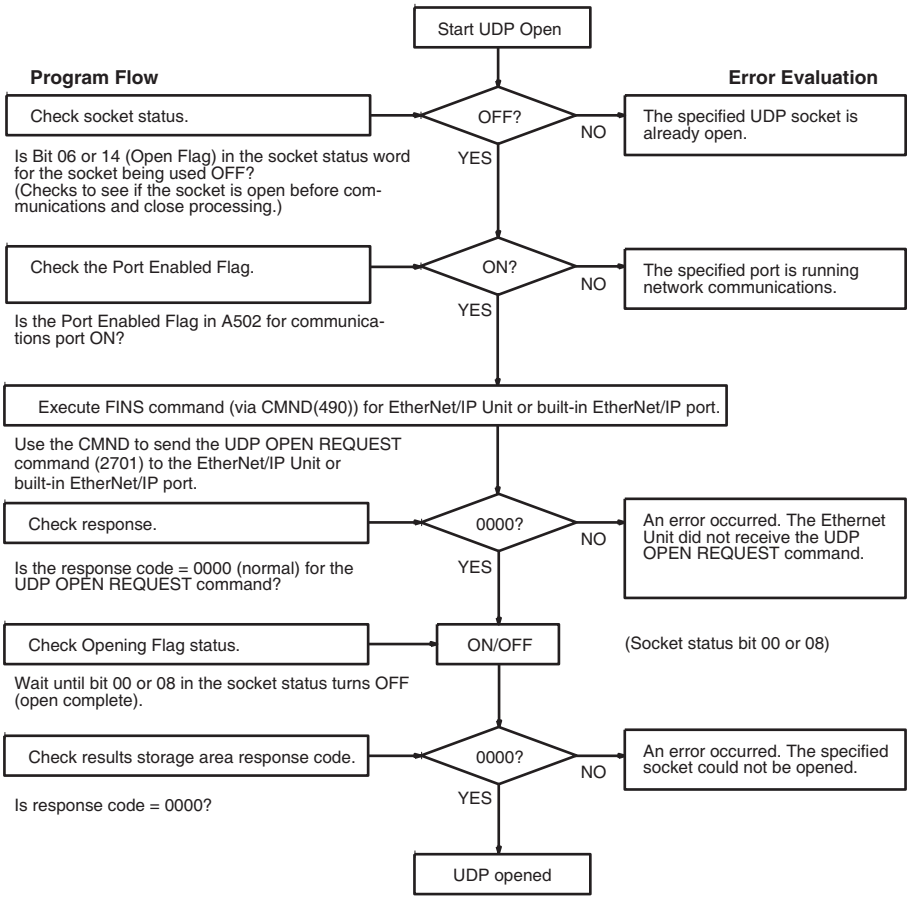
4. When the process has been completed, the result is stored in the results storage area defined in the socket service request command and the socket status will indicate completion of processing.



14-6-2 Socket Services and Socket Status

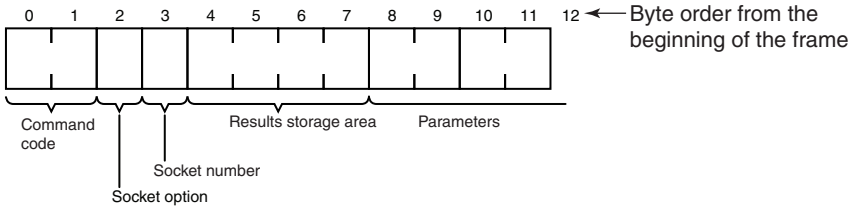
When using socket services, it is important to consider the timing of the status changes in the socket status area. The diagram below shows a program flowchart for opening UDP.

Program flow is similar for other socket services. Replace the names of the appropriate flags in the flowchart to adapt it to other socket services.



14-6-3 Basic FINS Command Format

The basic format for FINS commands used for socket services is shown in the following diagram.



Command Code

Specifies the process code requested from the socket.

Socket Option

For the TCP OPEN REQUEST (ACTIVE or PASSIVE) command, specifies whether or not the keep-alive function is to be used.

Socket Number

Specifies the socket number for the process, between 1 and 8.

Results Storage Area

Specifies the area to store the results of the requested process.

Parameters

Specifies the parameters defined for the command code.

Note If there is more than one Communications Unit mounted to the PLC, the FINS network address must be set as a parameter for CMND and a local network table must be created in the routing tables from the CX-Integrator.

14-6-4 Response Codes in the Command Response

A response code is returned in the command response as a 2-byte code that indicates the results of command execution. The response code is returned just after the command code in the response. The first byte of the response code provides the overall result of command execution and is called the main response code (MRES). The second byte provides details and is called the sub-response code (SRES).

Refer to Appendix E FINS Commands Addressed to EtherNet/IP Units or Built-in EtherNet/IP Ports for details on the response code for FINS commands.

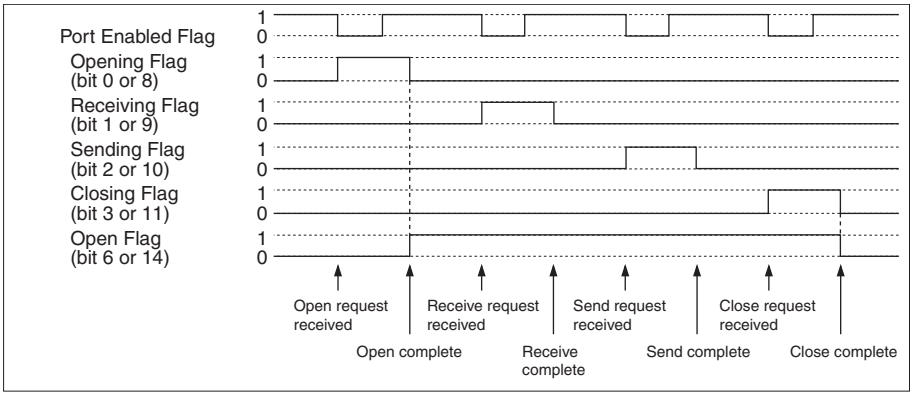
14-6-5 Response Codes in the Results Storage Areas

The response code stored in the Results Storage Area is a 2-byte code that indicates the processing results of the socket service requested by the command. This response code is stored in the Results Storage Area when processing has been completed.

Refer to 14-7-6 Response Codes for the response code.

14-6-6 Communications Timing Chart

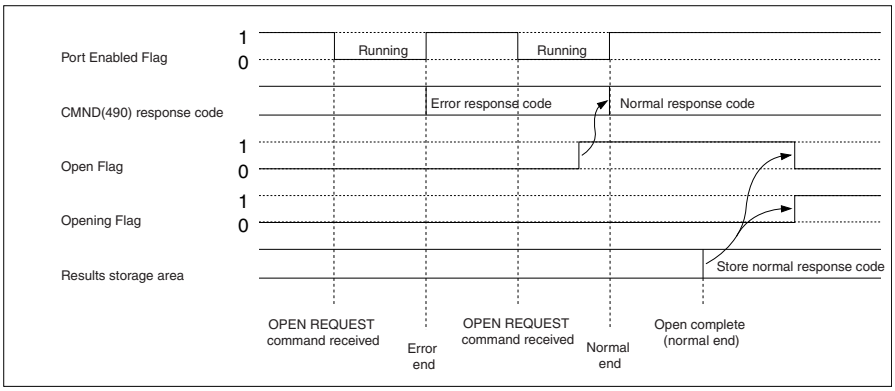
The timing of the status changes of the bits in the socket status area and the Port Enabled Flag is shown in the following diagram.



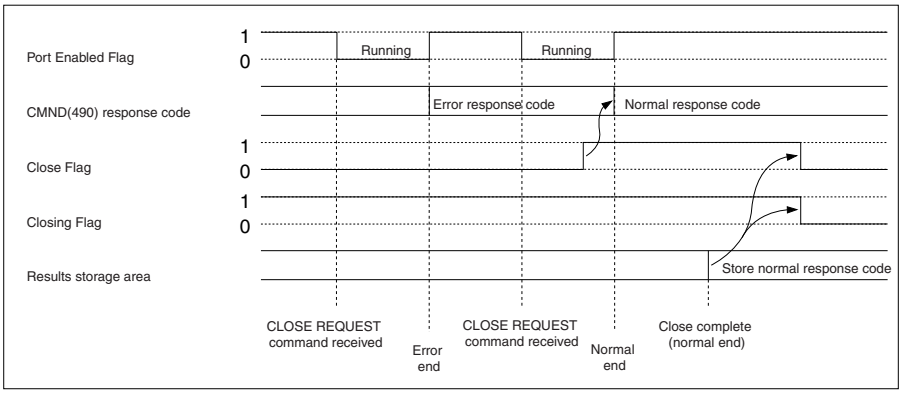
14-6-7 Socket Service Timing Chart

The timing of the socket service open, send, receive, and close request commands are shown in the following diagrams.

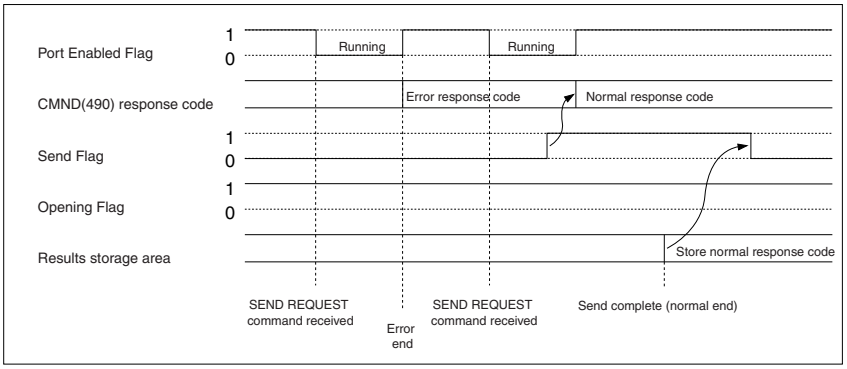
■ OPEN REQUEST



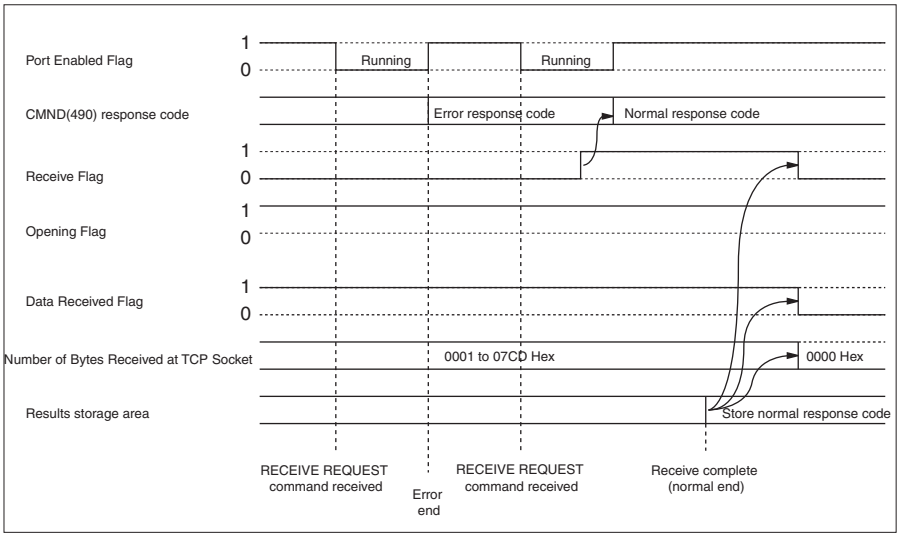
■ CLOSE REQUEST



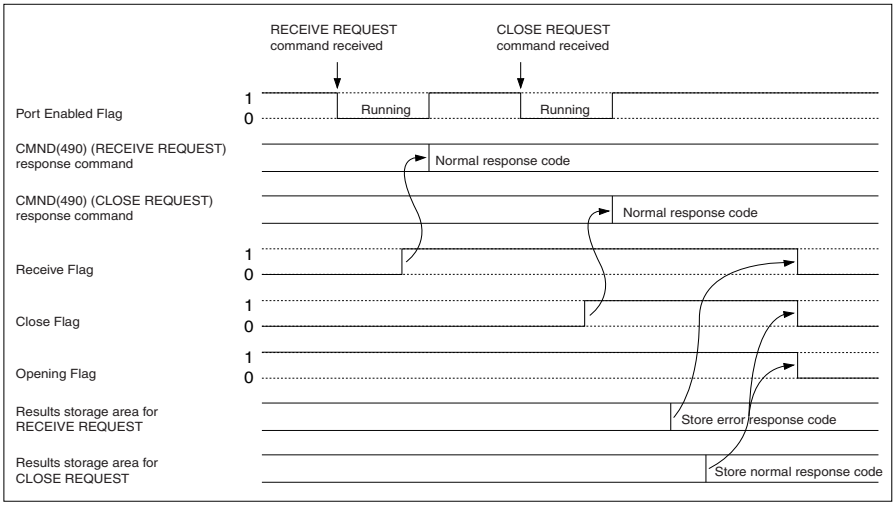
■ SEND REQUEST



■ **RECEIVE REQUEST**



■ **CLOSE REQUEST during RECEIVE REQUEST**



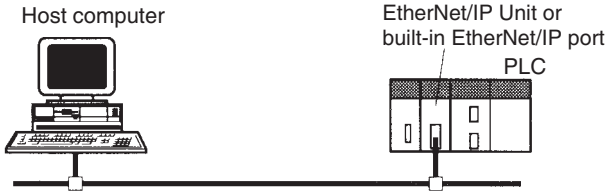
Note The timing shown in the above diagram occurs if a CLOSE REQUEST command is executed during SEND REQUEST command execution. The timing shown in the diagram also applies if a CLOSE REQUEST command is executed during OPEN REQUEST command execution, with the exception of the status of the Opening Flag.

14-6-8 TCP/IP Communications Programming Example (Using Socket Services with CMND)

The following programming example illustrates transferring 100 bytes of data between a EtherNet/IP Unit or built-in EtherNet/IP port and a host computer using TCP/IP communications.

System Configuration

The system configuration for the program example and the Ethernet Unit system setup are shown below. To establish a TCP connection, the EtherNet/IP Unit or built-in EtherNet/IP port is passively opened and the host computer actively opened.

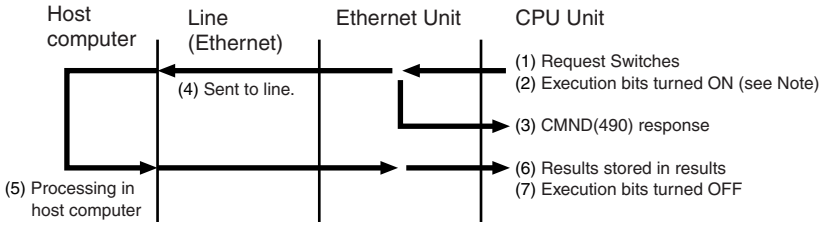


IP address: 196.36.32.55
Port number: 4096

IP address: 196.36.32.101
Port number: 4096
FINS network address: 01 Hex
Node address: 01 Hex
Unit number: 10 Hex

Data Flow

The data will flow between the CPU Unit, EtherNet/IP Unit or built-in EtherNet/IP port, and host computer as shown in the following diagram.



Note Here, “execution bits” refer to CIO 0000.00 to CIO 0000.03, which are used in the ladder diagram to control execution of communications and are not system flags, such as the Port Enabled Flags (A202.00 to A202.07).

Basic Operations

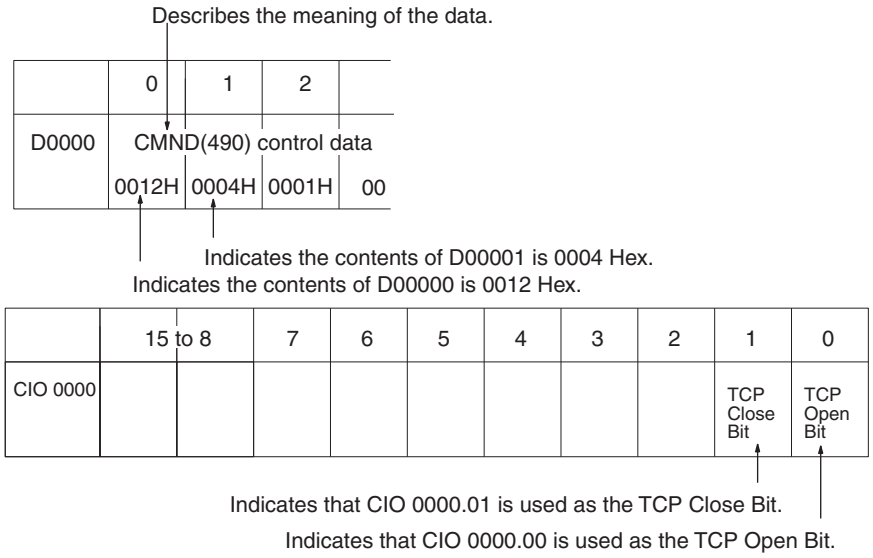
- CIO 0000.00 is turned ON to request opening a passive TCP socket from the EtherNet/IP Unit or built-in EtherNet/IP port.
- CIO 0000.01 is turned ON to request closing the TCP socket from the EtherNet/IP Unit or built-in EtherNet/IP port.
- CIO 0000.02 is turned ON to request sending data from the EtherNet/IP Unit or built-in EtherNet/IP port. Data (100 bytes) is sent beginning at D02005.
- CIO 0000.03 is turned ON to request receiving data from the EtherNet/IP Unit or built-in EtherNet/IP port. The data that is received (100 bytes) is stored beginning at D04022.
- One of the bits between CIO 0001.00 and CIO 0001.03 will turn ON if an error occurs. Refer to *14-5-5 Socket Service Request Switches* for information on errors. The following areas can be used to access details about errors:

  CMND response codes
  Response codes in results storage area
  Network Communications Error Flags (A219.00 to A219.07)
  Completion codes (A203 to A210)

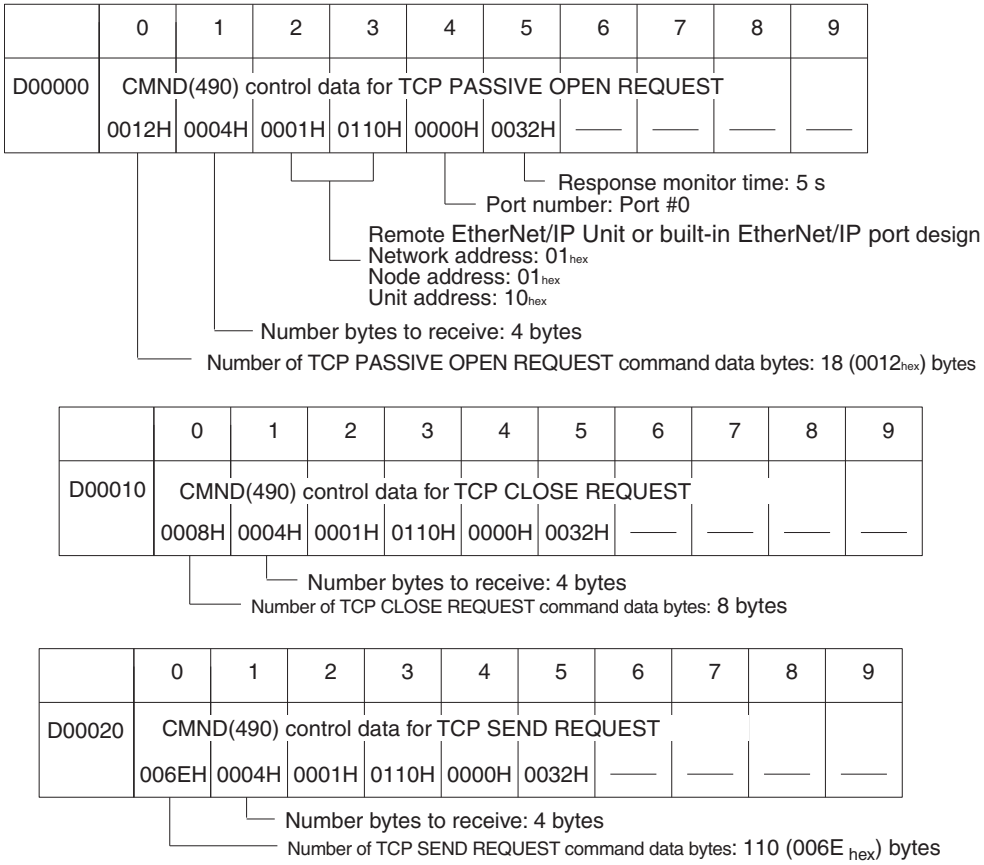
Program Memory Maps

The send and receive data and bits (flags) used by the program are shown in the following diagrams. The following example shows how the memory maps are structured.

Legend



DM Area



Command format = 10 bytes + 100 bytes send data

	0	1	2	3	4	5	6	7	8	9
D00030	CMND(490) control data for TCP RECEIVE REQUEST									
	000CH	0004H	0001H	0110H	0000H	0032H	——	——	——	——

Number bytes to receive: 4 bytes

Number of TCP RECEIVE REQUEST command data bytes: 12 bytes ($000C_{hex}$)

Number of bytes received specified in command data.

	0	1	2	3	4	5	6	7	8	9
D01000	TCP PASSIVE OPEN REQUEST command data									
	2710H	0001H	8203H	FC00H	1000H	0000H	C424H	2037H	0000H	——

Remote node: Not specified

Host computer IP address: 196.36.32.55 ($C4_{hex}.24_{hex}.20_{hex}.37_{hex}$)

Timeout value: Not set

Local port number: set to 4096 (1000_{hex})

Results storage area: set to D01020 ($03FC_{hex}$)
(Refer to *PLC Memory Areas* in *Socket Applications on page 622* for details on the results storage area.)

TCP socket number (EtherNet/IP Unit or built-in EtherNet/IP port socket number): set to 1

Command code

	0	1	2	3	4	5	6	7	8	9
D01010	TCP PASSIVE OPEN REQUEST response									
	2710H	Response code	——	——	——	——	——	——	——	——

Stores the response after command execution.

	0	1	2	3	4	5	6	7	8	9
D01020	TCP PASSIVE OPEN REQUEST results storage area									
	Response code	Remote IP address		Remote TCP port No.	——	——	——	——	——	——

	0	1	2	3	4	5	6	7	8	9
D1030	TCP CLOSE REQUEST command data									
	2714H	0001H	8204H	1A00H	——	——	——	——	——	——

Results storage area: set to D01050 ($041A_{hex}$)

TCP socket number to close: set to 1 (0001_{hex})

Command code

	0	1	2	3	4	5	6	7	8	9
D01040	TCP CLOSE REQUEST response									
	2714H	Response code			____	____	____	____	____	____
D01050	TCP CLOSE REQUEST results storage area									
	Response code	____	____	____	____	____	____	____	____	____

	0	1	2	3	4	5	6	7	8	9
D02000	TCP SEND REQUEST command data									
	2713H	0001H	820BH	C200H	0064H	Send data: 100 bytes (0064_{hex})				

- 0064H: No. of send bytes: 100 bytes (0064_{hex})
- C200H: Results storage area: set to D03010 ($0BC2_{hex}$)
- 0001H: TCP socket number
- 2713H: Command code

	0	1	2	3	4	5	6	7	8	9
D03000	TCP SEND REQUEST response									
	2713H	Response code	____	____	____	____	____	____	____	____
D03010	TCP SEND REQUEST results storage area									
	Response code	No. of bytes sent	____	____	____	____	____	____	____	____

	0	1	2	3	4	5	6	7	8	9
D04000	TCP RECEIVE REQUEST command data									
	2712H	0001H	820FH	B400H	0064H	0000H	____	____	____	____

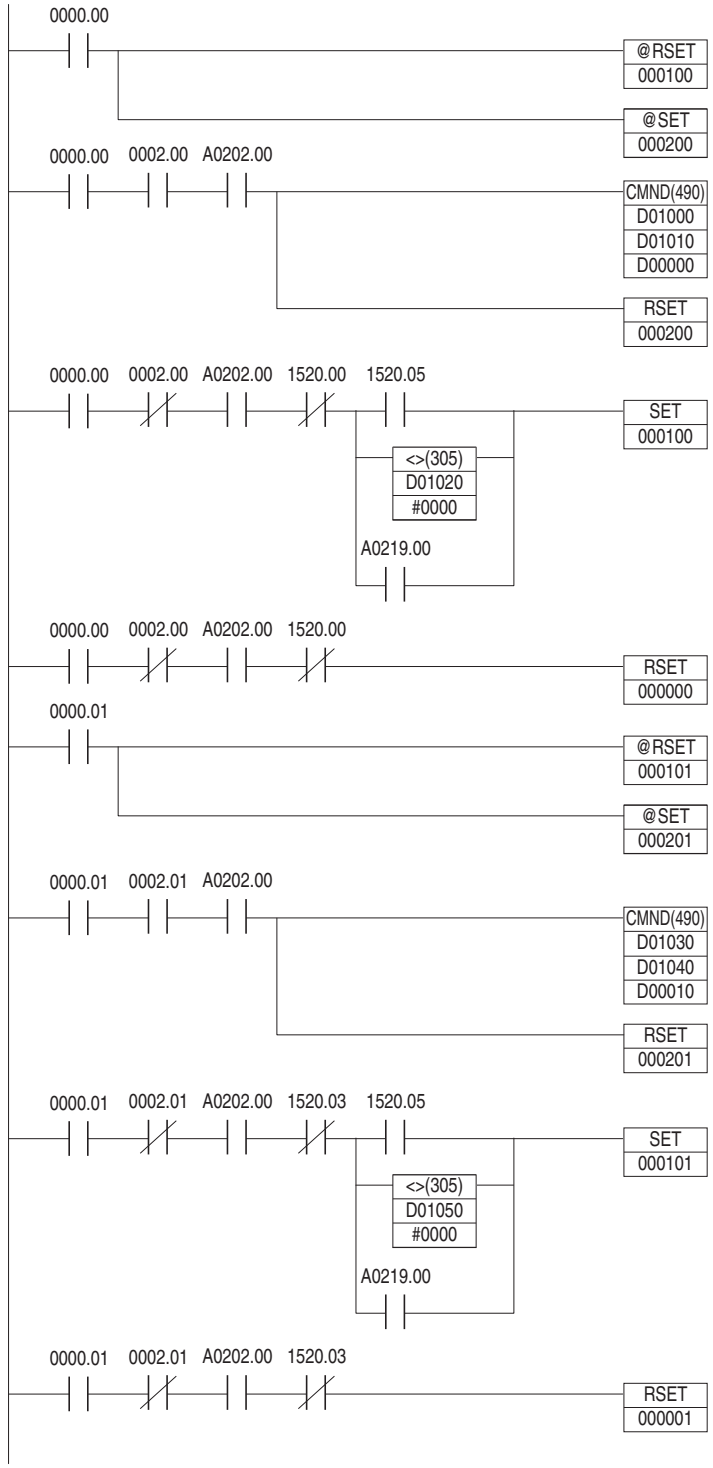
- 0000H: Timeout value: Not set
- 0064H: No. of bytes to receive: 100 bytes (0064_{hex})
- B400H: Results storage area: Set to D04020 ($0FB4_{hex}$)
- 0001H: TCP socket number
- 2712H: Command code

	0	1	2	3	4	5	6	7	8	9
D04010	TCP RECEIVE REQUEST response									
	2712H	Response code	____	____	____	____	____	____	____	____
D04020	TCP RECEIVE REQUEST results storage area									
	Response code	No. of bytes received	Receive data: 100 bytes (0064_{hex})							

CIO Area

	15 to 8	7	6	5	4	3	2	1	0
CIO 0000						TCP Receive Bit	TCP Send Bit	TCP Close Bit	TCP Open Bit
CIO 0001						TCP Receive Error Flag	TCP Send Error Flag	TCP Close Error Flag	TCP Open Error Flag
CIO 0002						TCP Receiving Flag	TCP Sending Flag	TCP Closing Flag	TCP Opening Flag

Programming Example



TCP Passive Open

When the TCP Open Bit (CIO 0000.00) turns ON, the TCP Open Error Flag (CIO 0001.00) is turned OFF and the TCP Opening Flag (CIO 0002.00) is turned ON to initialize processing.

When the TCP Opening Flag (CIO 0002.00) turns ON, the status of the Port Enabled Flag (A202.00) is checked to be sure it is ON and a PASSIVE TCP OPEN REQUEST command is sent using CMND(490).
D01000: First command word
D01010: First response word
D00000: First control data word

The TCP Opening Flag (CIO 0002.00) is also turned OFF.

If the Port Enabled Flag (A202.00) turns ON and the Opening Flag (CIO 1520.00) turns OFF while the TCP Opening Flag (CIO 0002.00) is OFF, checks are made and if any of the following are true, the TCP Open Error Flag (CIO 0001.00) is turned ON.

The Results Storage Error Flag (CIO 1520.05) is ON.

The contents of the Response Storage Area set in the command code (D01020) is not 0000 Hex (normal end).

The Network Communications Error Flag (A219.00) is ON.

After the execution results have been checked, the TCP Open Bit (CIO 0000.00) is turned OFF.

TCP Close

When the TCP Close Bit (CIO 0000.01) turns ON, the TCP Close Error Flag (CIO 0001.01) is turned OFF and the TCP Closing Flag (CIO 0002.01) is turned ON to initialize processing.

When the TCP Closing Flag (CIO 0002.01) turns ON, the status of the Port Enabled Flag (A202.00) is checked to be sure it is ON and a TCP CLOSE REQUEST command is sent using CMND(490).
D01030: First command word
D01040: First response word
D00010: First control data word

The TCP Closing Flag (CIO 0002.01) is also turned OFF.

If the Port Enabled Flag (A202.00) turns ON and the Closing Flag (CIO 1520.03) turns OFF while the TCP Closing Flag (CIO 0002.01) is OFF, checks are made and if any of the following are true, the TCP Close Error Flag (CIO 0001.01) is turned ON.

The Results Storage Error Flag (CIO 1520.05) is ON.

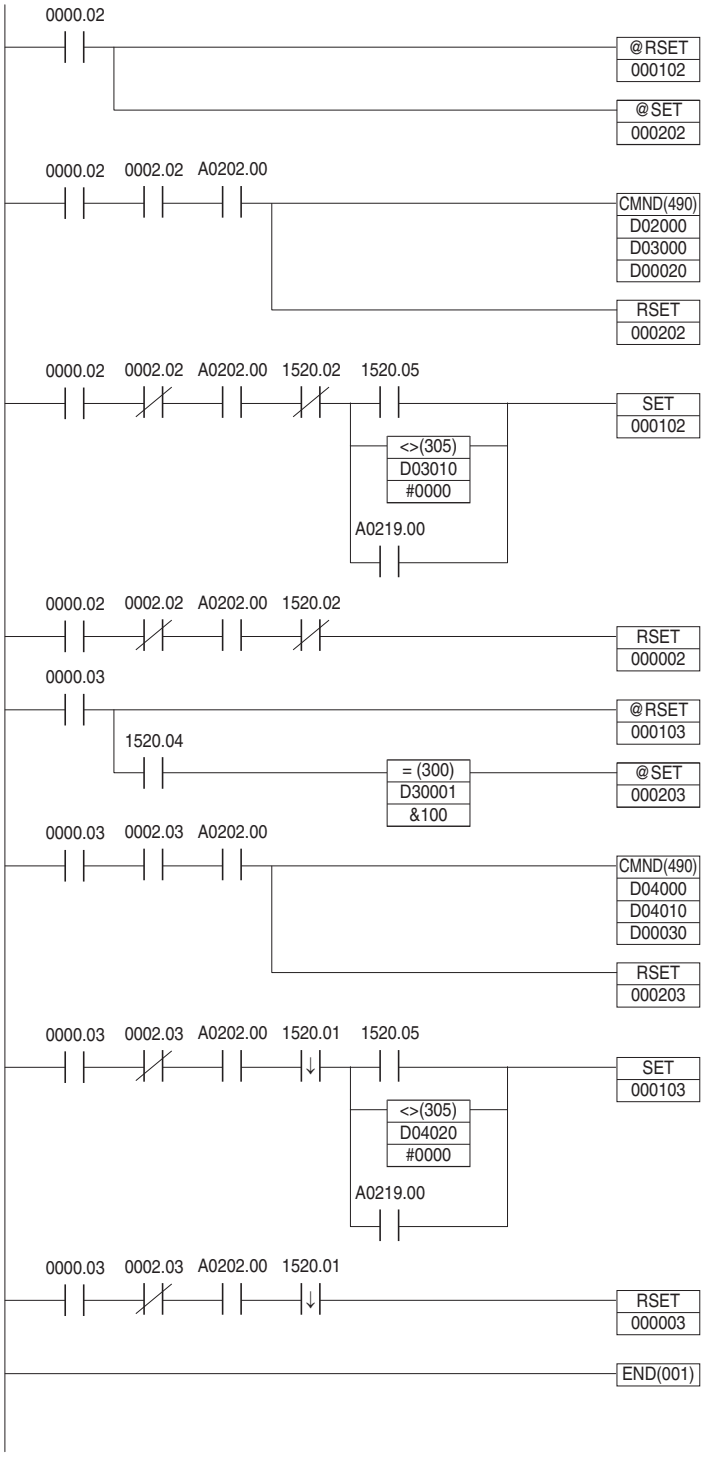
The contents of the Response Storage Area set in the command code (D01050) is not 0000 Hex (normal end).

The Network Communications Error Flag (A219.00) is ON.

After the execution results have been checked, the TCP Close Bit (CIO 0000.01) is turned OFF.

Continued on next page.

Continued from previous page.



TCP Send

When the TCP Send Bit (CIO 0000.02) turns ON, the TCP Send Error Flag (CIO 0001.02) is turned OFF and the TCP Sending Flag (CIO 0002.02) is turned ON to initialize processing.

When the TCP Sending Flag (CIO 0002.02) turns ON, the status of the Port Enabled Flag (A202.00) is checked to be sure it is ON and a TCP SEND REQUEST command is sent using CMND(490).
D02000: First command word
D03000: First response word
D00020: First control data word

The TCP Sending Flag (CIO 0002.02) is also turned OFF.

If the Port Enabled Flag (A202.00) turns ON and the Sending Flag (CIO 1520.02) turns OFF while the TCP Sending Flag (CIO 0002.02) is OFF, checks are made and if any of the following are true, the TCP Send Error Flag (CIO 0001.02) is turned ON.

The Results Storage Error Flag (CIO 1520.05) is ON.

The contents of the Response Storage Area set in the command code (D03010) is not 0000 Hex (normal end).

The Network Communications Error Flag (A219.00) is ON.

After the execution results have been checked, the TCP Send Bit (CIO 0000.02) is turned OFF.

TCP Receive

When the TCP Receive Bit (CIO 0000.03) turns ON, the TCP Receive Error Flag (CIO 0001.03) is turned OFF. The contents of the reception buffer, and the status of the TCP Data Received/Requested Flag (CIO 1520.04), and the Number of Bytes Received at TCP Socket (D30001) are checked. If the data is stored in the buffer, the TCP Receiving Flag (CIO 0002.03) turns ON.

When the TCP Receiving Flag (CIO 0002.03) turns ON, the status of the Port Enabled Flag (A202.00) is checked to be sure it is ON and a TCP RECEIVE REQUEST command is sent using CMND(490).
D04000: First command word
D04010: First response word
D00030: First control data word

The TCP Receiving Flag (CIO 0002.03) is also turned OFF.

If the Port Enabled Flag (A202.00) turns ON and the Receiving Flag (CIO 1520.01) turns OFF while the TCP Receiving Flag (CIO 0002.03) is OFF, checks are made and if any of the following are true, the TCP Receive Error Flag (CIO 0001.03) is turned ON.

The Results Storage Error Flag (CIO 1520.05) is ON.

The contents of the Response Storage Area set in the command code (D04020) is not 0000 Hex (normal end).

The Network Communications Error Flag (A219.00) is ON.

After the execution results have been checked, the TCP Receive Bit (CIO 0000.03) is turned OFF.

Note When using the above programming example, change the bit and word addresses as necessary to avoid using the same areas used by other parts of the user program or the CPU Bus Unit.

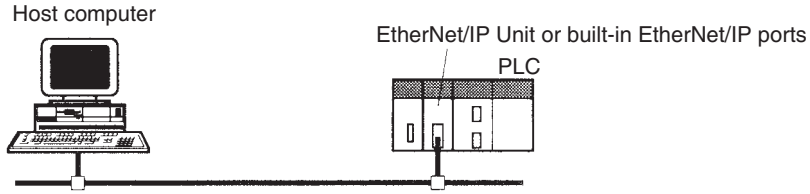
14-6-9 UDP/IP Communications Programming Example (Using Socket Services with CMND)

The following programming example illustrates transferring 100 bytes of data between an EtherNet/IP Unit or built-in EtherNet/IP port and a host computer using UDP/IP communications.

For the UDP connection, the EtherNet/IP Unit or built-in EtherNet/IP port uses a PASSIVE OPEN and the host computer uses an ACTIVE OPEN.

System Configuration

The system configuration for the program example and the Ethernet Unit system setup are shown below.



IP address:	196.36.32.55	IP address:	196.36.32.101
Port number:	4096	Port number:	4096
		FINS network address:	01 Hex
		Node address:	01 Hex
		Unit number:	10 Hex

Basic Operations

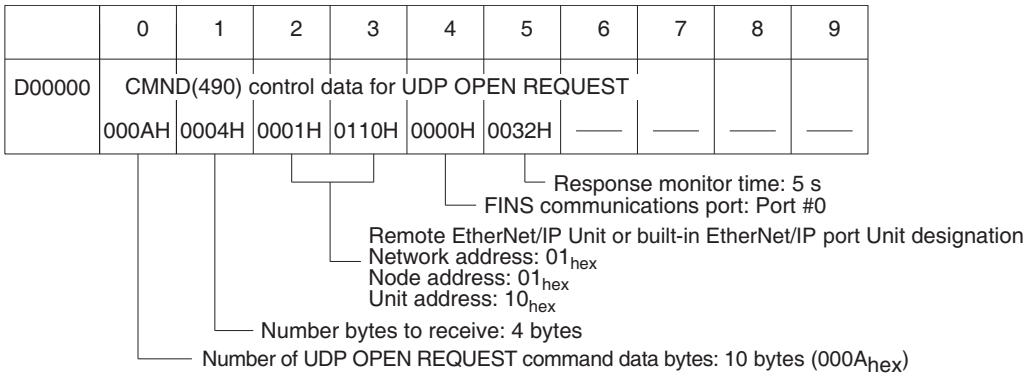
- CIO 0000.00 is turned ON to request opening a UDP socket from the EtherNet/IP Unit or built-in EtherNet/IP port.
- CIO 0000.01 is turned ON to request closing the UDP socket from the EtherNet/IP Unit or built-in EtherNet/IP port.
- CIO 0000.02 is turned ON to request sending data from the EtherNet/IP Unit or built-in EtherNet/IP port. Data (100 bytes) is sent beginning at D02008.
- CIO 0000.03 is turned ON to request receiving data from the EtherNet/IP Unit or built-in EtherNet/IP port. The data that is received (100 bytes) is stored beginning at D04025.
- One of the bits between CIO 0001.00 and CIO 0001.03 will turn ON if an error occurs. Refer to *14-5-5 Socket Service Request Switches* for information on errors. The following areas can be used to access details about errors:

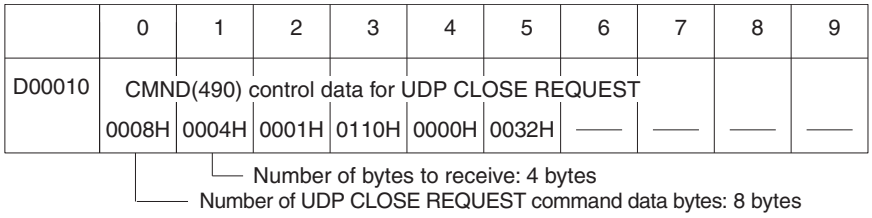
  CMND response codes
  Response codes in results storage area
  Network Communications Error Flags (A219.00 to A219.07)
  Completion codes (A203 to A210)

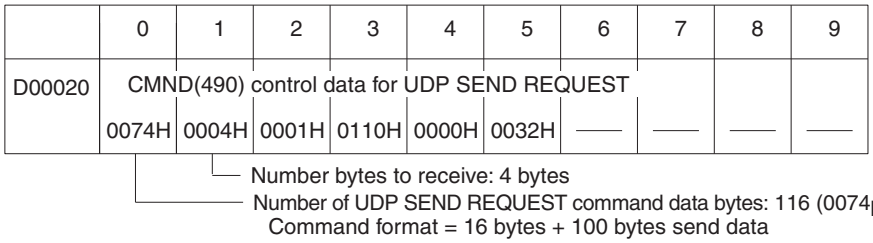
Program Memory Maps

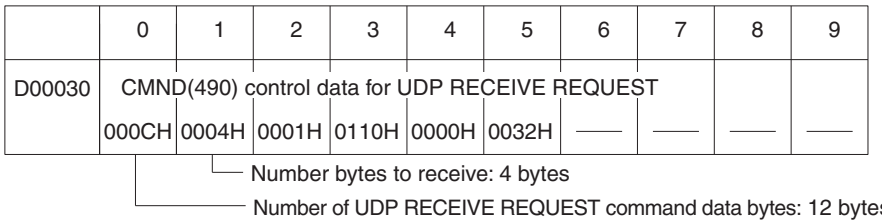
The send and receive data and bits (flags) used by the program are shown in the following diagrams.

DM Area

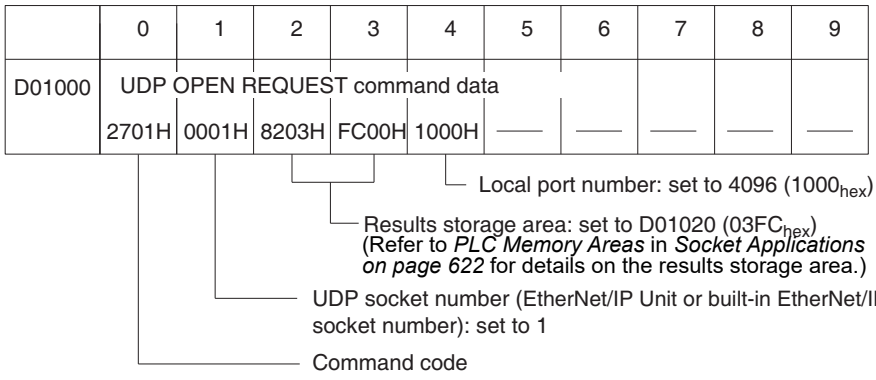








Number of bytes received is specified in command data.



	0	1	2	3	4	5	6	7	8	9
D01010	UDP OPEN response									
	2701H	Response code	____	____	____	____	____	____	____	____

Stores the response after command execution.

	0	1	2	3	4	5	6	7	8	9
D01020	UDP OPEN REQUEST results storage area									
	Response code	____	____	____	____	____	____	____	____	____

	0	1	2	3	4	5	6	7	8	9
D01030	UDP CLOSE REQUEST command data									
	2704H	0001H	8204H	1A00H	____	____	____	____	____	____

Results storage area: set to D01050 ($041A_{hex}$)
UDP socket number closed: set to 1 (0001_{hex})
Command code

	0	1	2	3	4	5	6	7	8	9
D01040	UDP CLOSE REQUEST response									
	2704H	Response code			____	____	____	____	____	____
D01050	UDP CLOSE REQUEST results storage area									
	Response code	____	____	____	____	____	____	____	____	____

	0	1	2	3	4	5	6	7	8	9
D02000	UDP SEND REQUEST command data									
	2703H	0001H	820BH	C200H	C424H	2037H	1000H	0064H	____	____

No. of send bytes: 100 bytes (0064_{hex})
Remote port: Port #4096 (1000_{hex})
Remote address: 196.36.32.55 ($C4_{hex}.24_{hex}.20_{hex}.37_{hex}$)
Results storage area: Set to D03010 ($0BC2_{hex}$)
UDP socket number
Command code

	0	1	2	3	4	5	6	7	8	9
D03000	UDP SEND REQUEST response									
	2703H	Response code	———	———	———	———	———	———	———	———
D03010	UDP SEND REQUEST results storage area									
	Response code	No. of send bytes	———							

	0	1	2	3	4	5	6	7	8	9
D04000	UDP RECEIVE REQUEST command data									
	2702H	0001H	820FH	B400H	0064H	0000H	———	———	———	———

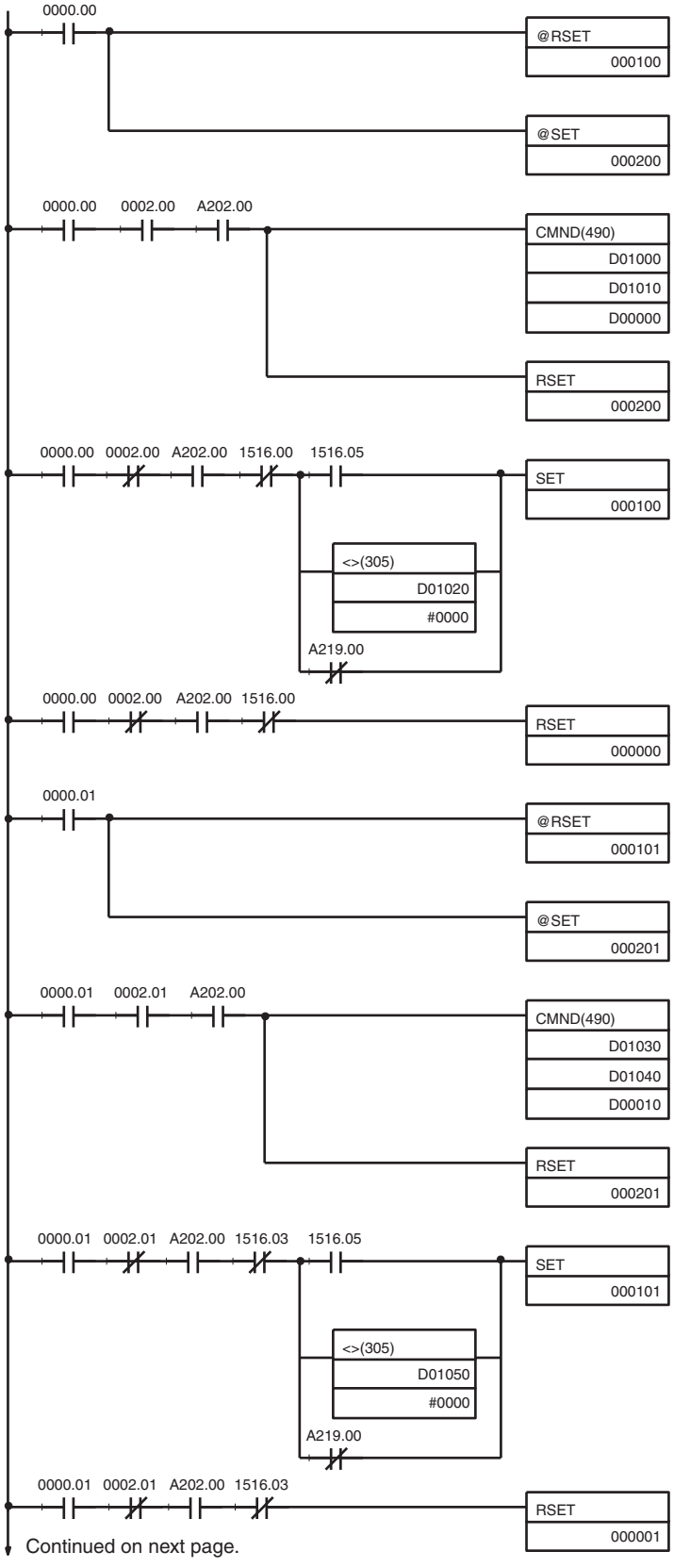
Timeout value: Not set
No. of bytes to receive: 100 bytes (0064_{hex})
Results storage area: set to D04020 ($0FB4_{hex}$)
UDP socket number used
Command code

	0	1	2	3	4	5	6	7	8	9
D04010	UDP RECEIVE REQUEST response									
	2702H	Response code	———	———	———	———	———	———	———	———
D04020	UDP RECEIVE REQUEST results storage area									
	Response code	Source IP address		Source port number	No. of bytes to receive	Receive data: 100 bytes (0064_{hex})				

CIO Area

	15 to 8	7	6	5	4	3	2	1	0
CIO 0000						UDP Receive Bit	UDP Send Bit	UDP Close Bit	UDP Open Bit
CIO 0001						UDP Receive Error Flag	UDP Send Error Flag	UDP Close Error Flag	UDP Open Error Flag
CIO 0002						UDP Receiving Flag	UDP Sending Flag	UDP Closing Flag	UDP Opening Flag

Programming Example



UDP Passive Open
When the UDP Open Bit (CIO 0000.00) turns ON, the UDP Open Error Flag (CIO 0001.00) is turned OFF and the UDP Opening Flag (CIO 0002.00) is turned ON to initialize processing.

When the UDP Opening Flag (CIO 0002.00) turns ON, the status of the Port Enabled Flag (A202.00) is checked to be sure it is ON and a UDP OPEN REQUEST command is sent using CMND(490).
D01000: First command word
D01010: First response word
D00000: First control data word

The UDP Opening Flag (CIO 0002.00) is also turned OFF.

If the Port Enabled Flag (A202.00) turns ON and the Opening Flag (CIO 1516.00) turns OFF while the UDP Opening Flag (CIO 0002.00) is OFF, checks are made and if any of the following are true, the UDP Open Error Flag (CIO 0001.00) is turned ON.

The Results Storage Error Flag (CIO 1516.05) is ON.

The contents of the Response Storage Area set in the command code (D01020) is not 0000 Hex (normal end).

The Network Communications Error Flag (A219.00) is ON.

After the execution results have been checked, the UDP Open Bit (CIO 0000.00) is turned OFF.

UDP Close
When the UDP Close Bit (CIO 0000.01) turns ON, the UDP Close Error Flag (CIO 0001.01) is turned OFF and the UDP Closing Flag (CIO 0002.01) is turned ON to initialize processing.

When the UDP Closing Flag (CIO 0002.01) turns ON, the status of the Port Enabled Flag (A202.00) is checked to be sure it is ON and a UDP CLOSE REQUEST command is sent using CMND(490).
D01030: First command word
D01040: First response word
D00010: First control data word

The UDP Closing Flag (CIO 0002.01) is also turned OFF.

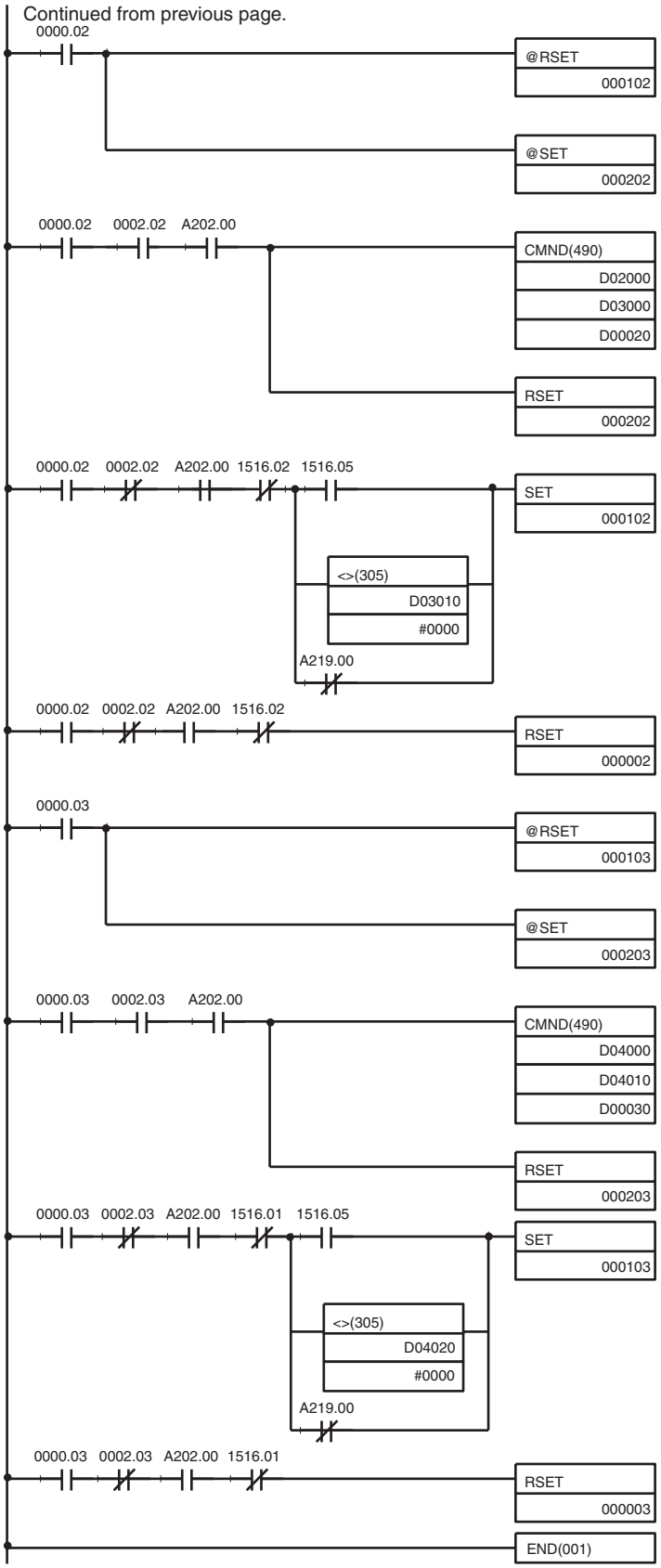
If the Port Enabled Flag (A202.00) turns ON and the Closing Flag (CIO 1516.03) turns OFF while the UDP Closing Flag (CIO 0002.01) is OFF, checks are made and if any of the following are true, the UDP Close Error Flag (CIO 0001.01) is turned ON.

The Results Storage Error Flag (CIO 1516.05) is ON.

The contents of the Response Storage Area set in the command code (D01050) is not 0000 Hex (normal end).

The Network Communications Error Flag (A219.00) is ON.

After the execution results have been checked, the UDP Close Bit (CIO 0000.01) is turned OFF.



UDP Send
When the UDP Send Bit (CIO 0000.02) turns ON, the UDP Send Error Flag (CIO 0001.02) is turned OFF and the UDP Sending Flag (CIO 0002.02) is turned ON to initialize processing.

When the UDP Sending Flag (CIO 0002.02) turns ON, the status of the Port Enabled Flag (A202.00) is checked to be sure it is ON and a UDP SEND REQUEST command is sent using CMND(490).
D02000: First command word
D03000: First response word
D00020: First control data word

The UDP Sending Flag (CIO 0002.02) is also turned OFF.

If the Port Enabled Flag (A202.00) turns ON and the Sending Flag (CIO 1516.02) turns OFF while the UDP Sending Flag (CIO 0002.02) is OFF, checks are made and if any of the following are true, the UDP Send Error Flag (CIO 0001.02) is turned ON.

The Results Storage Error Flag (CIO 1516.05) is ON.

The contents of the Response Storage Area set in the command code (D03010) is not 0000 Hex (normal end).

The Network Communications Error Flag (A219.00) is ON.

After the execution results have been checked, the UDP Send Bit (CIO 0000.02) is turned OFF.

UDP Receive
When the UDP Receive Bit (CIO 0000.03) turns ON, the UDP Receive Error Flag (CIO 0001.03) is turned OFF and the UDP Receiving Flag (CIO 0002.03) is turned ON to initialize processing.

When the UDP Receiving Flag (CIO 0002.03) turns ON, the status of the Port Enabled Flag (A202.00) is checked to be sure it is ON and a UDP RECEIVE REQUEST command is sent using CMND(490).
D04000: First command word
D04010: First response word
D00030: First control data word

The UDP Receiving Flag (CIO 0002.03) is also turned OFF.

If the Port Enabled Flag (A202.00) turns ON and the Receiving Flag (CIO 1516.01) turns OFF while the UDP Receiving Flag (CIO 0002.03) is OFF, checks are made and if any of the following are true, the UDP Receive Error Flag (CIO 0001.03) is turned ON.

The Results Storage Error Flag (CIO 1516.05) is ON.

The contents of the Response Storage Area set in the command code (D04020) is not 0000 Hex (normal end).

The Network Communications Error Flag (A219.00) is ON.

After the execution results have been checked, the UDP Receive Bit (CIO 0000.03) is turned OFF.

Note When using the above programming example, change the bit and word addresses as necessary to avoid using the same areas used by other parts of the user program or the CPU Bus Unit.

14-7 Details on the Socket Service Using with Function Block

14-7-1 Table of Function Block

Function blocks are provided for the EtherNet/IP Unit to enable the socket service functions to be used easily.

Function Block for TCP Socket

Function	Function Block Name
Open TCP Socket Passive	_EIPS001_SOCKET_TcpOpenPassive
Open TCP Socket Active	_EIPS002_SOCKET_TcpOpenActive
Close TCP Socket	_EIPS003_SOCKET_TcpClose
Send via TCP Socket	_EIPS004_SOCKET_TcpSend
Receive via TCP Socket	_EIPS005_SOCKET_TcpRecv

Function Block for UDP Socket

Function	Function Block Name
Open UDP Socket	_EIPS011_SOCKET_UdpOpen
Close UDP Socket	_EIPS013_SOCKET_UdpClose
Receive via UDP Socket	_EIPS014_SOCKET_UdpRecv
Send via UDP Socket	_EIPS015_SOCKET_UdpSend

The CPU Units and EtherNet/IP Units (built-in ports) that support the function blocks for the socket service are as follows.

CPU Units	Built-in EtherNet/IP Unit
CS1□-CPU□□H (Unit version: 3.0 or later) CS1D-CPU□□HA/SA (Unit version: 4.0 or later) CJ2□-CPU□□(-EIP) CJ3□-CPU□□	CS1W/CJ1W-EIP21S CJ3M-CPU3□

For details on the function block, refer to Appendix L Function Block for Socket Service

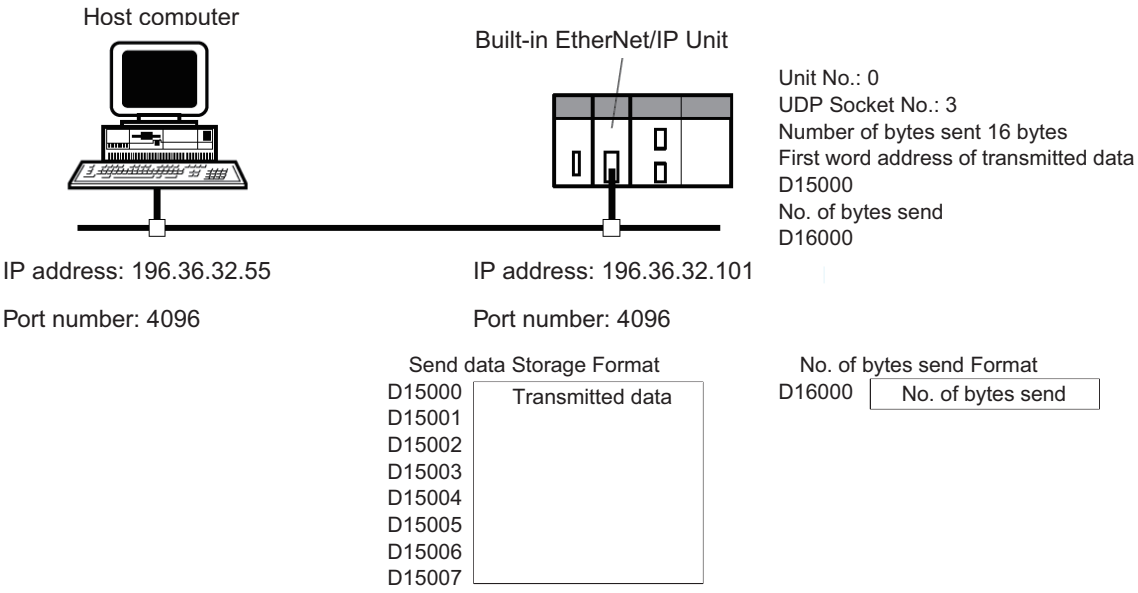
Note The function blocks for the socket service are implemented using the socket service functions by CMND instruction. Therefore, use a maximum of eight sockets or less for each of TCP and UDP.

14-7-2 UDP/IP Communications Programming Example (Using Function Blocks)

The following programming example illustrates transferring 10 bytes of data between an built-in Ethernet/IP Unit and a host computer using UDP/IP communications.

The following programming example illustrates transferring 10 bytes of data between an built-in Ethernet/IP Unit and a host computer using UDP/IP communications.

System Configuration



The programming example uses the following system configuration.

Use a function block for UDP sockets to send D15000 through D15009 to the remote device.

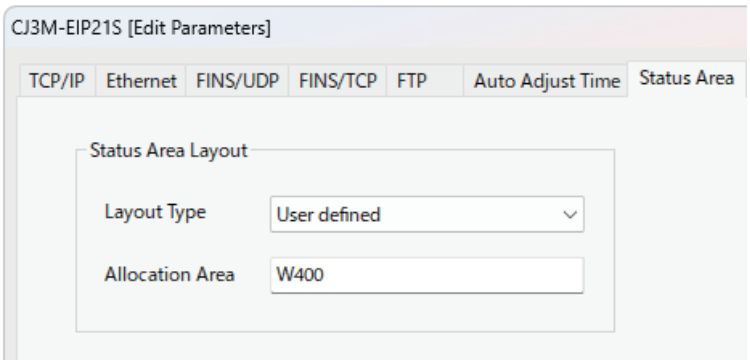
Basic Operations

1. Execute opening of the UDP port upon the rising edge of W0.00. Set the local UDP port number to be allocated automatically.
2. After UDP opening (after W0.02 turns ON), send the data of D15000 through D15007 (16 bytes) to the remote device (IP address: 196.36.32.55, port number: 4096) upon the rising edge of W1.00.
3. Close the UDP port upon the rising edge of W3.00.
4. Set the number of transfer retries to 2, and the response start time to 2 seconds.

Settings

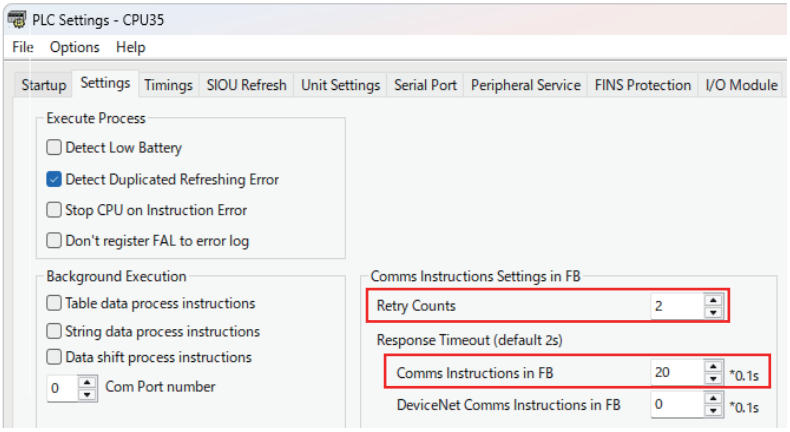
Built-in EtherNet/IP Unit Settings

Select User defined for the Layout Type on the Status Area Tab Page. Allocate any area for the allocated area. The user defined area occupies 64 words.



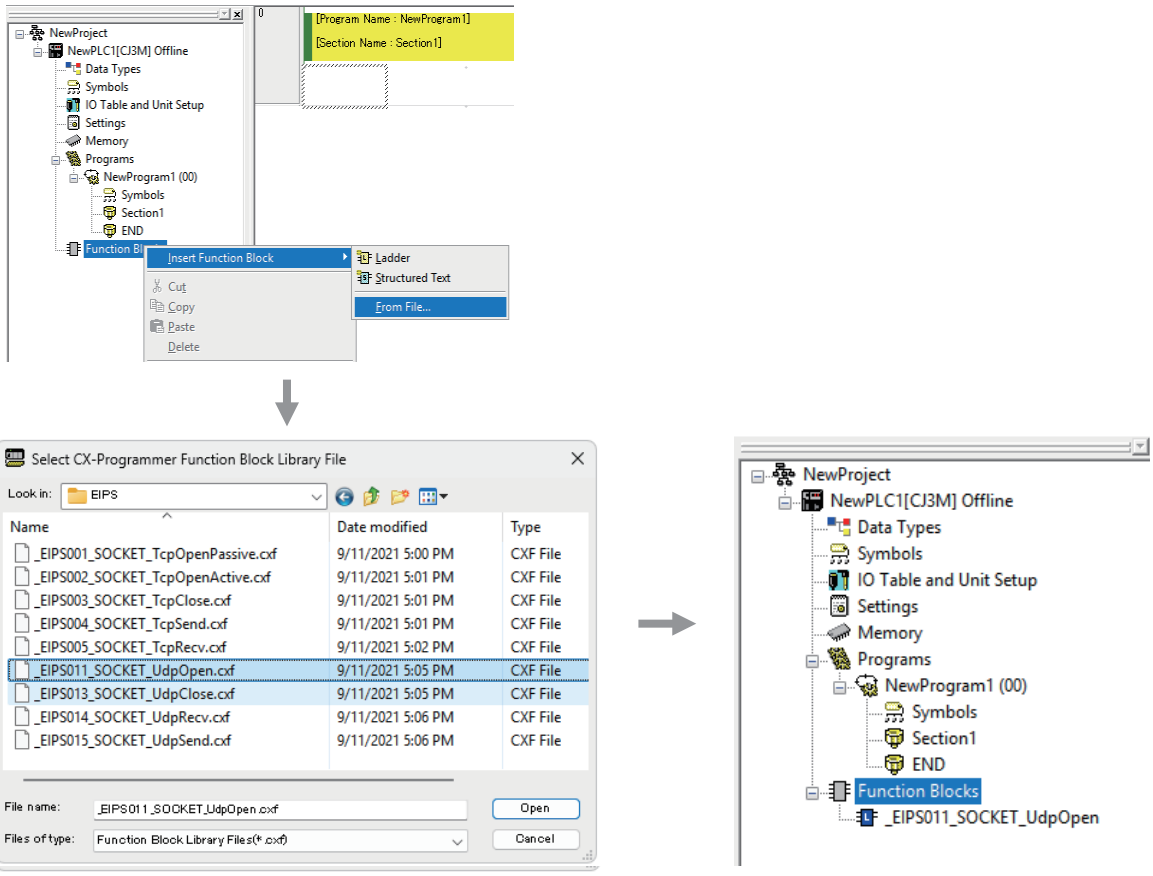
CPU Unit Settings

Set the number of transfer retries and the response monitoring time for the function block internal communication instruction from the function block internal communication instruction settings on the CPU Unit Settings Tab Page of the PLC system settings.



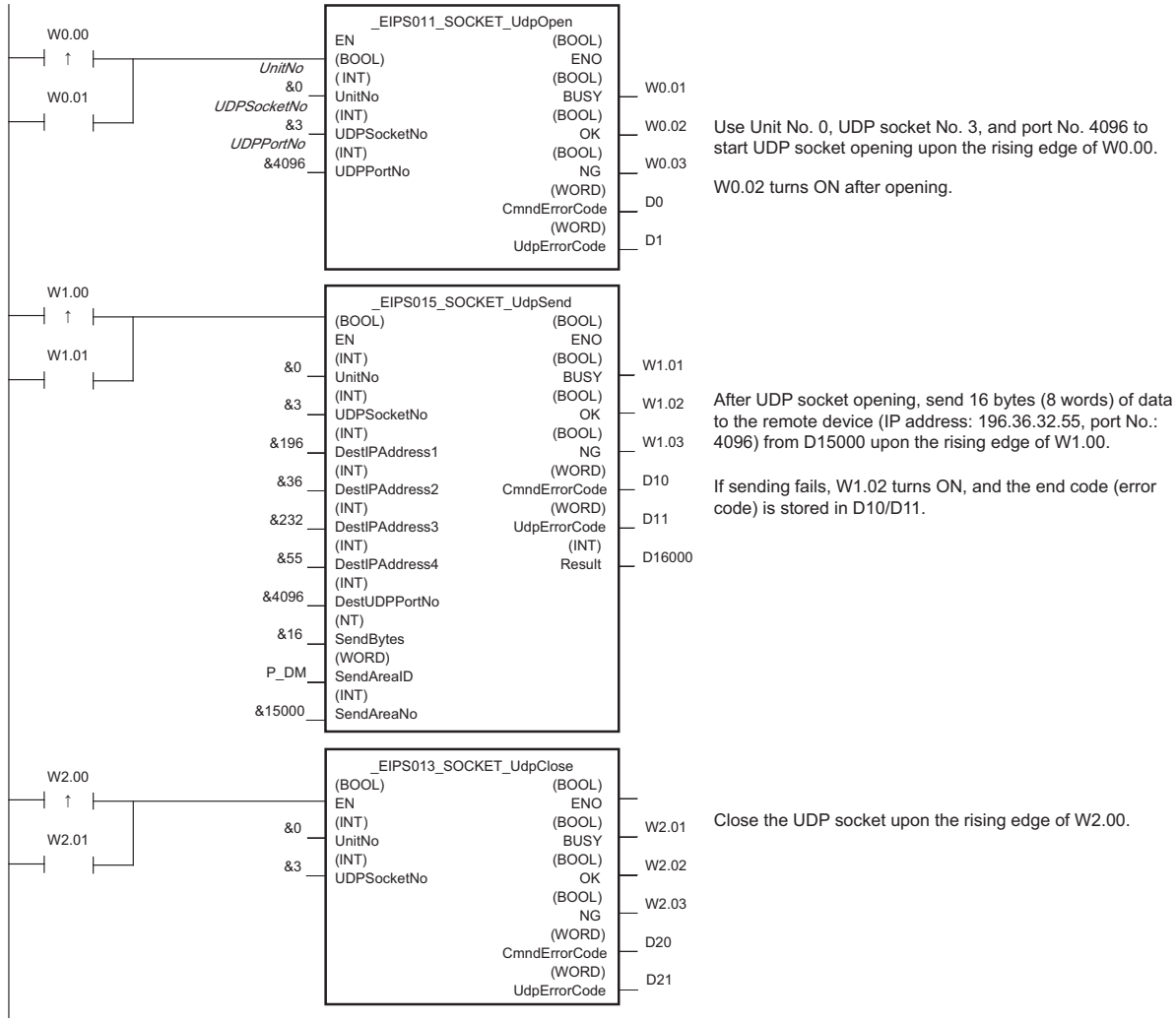
Read Function Blocks

- In the CX-Programmer, right-click the Function Block, and select Insert Function Blocks - Load the Library Files .
- In the selection of the function block library file, select the function block file (.cxf) to insert for the socket service from the following folder.
  C:\Program Files (x86)\OMRON\CX-One\Lib\FBL\omronlib\programmable controller\EIPS



Programming Example

Use function blocks to create a ladder program.



Refer to Appendix E FINS Commands Addressed to EtherNet/IP Units or Built-in EtherNet/IP Ports for the FINS completion code “CmndErrorCode”.

Refer to 14-7-6 Response Codes for the Socket Service completion code “UdpErrorCode”.

Note When using the above programming example, change the bit and word addresses as necessary to avoid using the same areas used by other parts of the user program or the CPU Bus Unit.

14-8 Precautions in Using Socket Services

14-8-1 UDP and TCP Socket Services

- If a short response monitor time is specified in CMND(490) control data and the EtherNet/IP Unit or built-in EtherNet/IP port is operating under a high load, a result may be stored even if the response code indicates a time-out. If this occurs, increase the monitor time specified with CMND(490).
- The socket status area in the CIO Area is zeroed when the PLC's operating mode is changed (e.g., from PROGRAM to RUN). The actual EtherNet/IP Unit or built-in EtherNet/IP port socket status, however, will remain unchanged after the socket status area is zeroed. To avoid this problem, use the IOM Hold setting in the PLC Setup. Refer to the PLC's operation manuals for details on settings.
- The Results Storage Error Flag will turn ON in the socket status to indicate that the specified Results Storage Area does not exist in the PLC. Correct the user program.
- Communications time may increase if multiple EtherNet/IP Unit or built-in EtherNet/IP port functions are used simultaneously or due to the contents of the user program.
- Communications efficiency may decrease due to high communications loads on the network.
- All data is flushed from the socket's communications buffer when a socket is closed with the CLOSE REQUEST command. In some cases, the transmit data for the SEND REQUEST command issued just before the socket was closed may not be sent.
- When sockets are open, the EtherNet/IP Unit or built-in EtherNet/IP port provides a 4,096-byte buffer for each TCP socket and 9,016-byte buffer for each UDP socket to allow data to be received at any time. These buffers are shared by all open sockets. Receive data will be discarded for a socket if the buffer becomes full. The user application must therefore issue RECEIVE REQUEST commands frequently enough to prevent the internal buffers from becoming full.

14-8-2 UDP Socket Service

- The UDP socket sets a broadcast address for the remote node address to broadcast data to all nodes of the network simultaneously. The maximum length of broadcast data is 1,472 bytes. Data in multiple fragments (over 1,473 bytes for a UDP socket) cannot be broadcast.
- The UDP socket does not check the transmitted data to ensure communications reliability. To increase communication reliability, communications checks and retries must be included in the user application program.

14-8-3 TCP Socket Service

- If the TCP socket of the remote node closes (the connection is broken) during communications, the TCP socket at the local node must also be closed. The communications Results Storage Area can be used to check if the connection has been broken. Close the local socket immediately after detecting that the remote TCP socket has closed. The following situations indicate that the remote socket has closed.

TCP Receive Results Storage Area:
Response code = 004B (error at remote node)

TCP Send Results Storage Area:
Response code = 0020 (connection broken with remote socket during transmission)

- Data can remain in a buffer at the local node if the remote TCP socket closes during communications. Any data remaining in the buffer will be discarded when the TCP socket is closed. To avoid problems of this nature, steps will have to be taken in the application program, such as sending data to enable closing, and then only closing once reception of this data has been confirmed.
- When closing a connection for a TCP socket, the first port to be closed cannot be reopened for at least 60 seconds after the other port closes. However, this restriction does not apply for a port opened using the TCP ACTIVE OPEN REQUEST command with a local TCP port number of 0 (port number automatically assigned) which is closed from the side that actively opened the socket.
- A connection is established for a passively opened socket by actively opening it from another socket. A connection will not be established by a different socket attempting to actively open the socket that is already actively opening a socket. Similarly, a connection will not be established if a different socket attempts to passively open a socket that is already being passively opened by another socket. You cannot actively open multiple connections to a socket passively opened at the EtherNet/IP Unit or built-in EtherNet/IP port.
- The EtherNet/IP Unit or built-in EtherNet/IP port TCP sockets have no KEEP ALIVE function to check that the connection is normal if communications do not occur for a set time period through a communications line for which a connection has been established. The EtherNet/IP Unit's or built-in EtherNet/IP port's TCP sockets make no checks to the socket at the other node. Checks made by the remote node, however, are received as responses, so that it is not necessary for the user program to consider the KEEP ALIVE function.

14-8-4 Precautions in Using Socket Service Request Switches

- Send and reception processing can not be performed at the same time when Socket Service Request Switches are used for socket services because there is only one Socket Service Parameter Area for each socket. For example, if the Send Request Switch is turned ON when data is being received, the response code will be 110C hexadecimal, indicating that a Request Switch was turned ON during communications processing. (The response code for the reception will overwrite this code when processing has been completed.)
- If more than one Request Switch is turned ON simultaneously, the response code will be 110C hexadecimal and all requested processing will end in an error.
- Close processing can be performed, however, even during open, send, or receive processing. This enables emergency close processing. Also, the only parameter required for close processing is the socket number, so a socket can be closed even when parameters are set for another process.

14-8-5 Times Required for Sending and Receiving for Socket Services

The transmission delays for socket service is calculated as the sum of the communications processing times for both nodes.

Transmission delay = Remote node send processing time + Local node receive processing time + Local node send processing time + Remote node receive processing time

Calculate the maximum EtherNet/IP Unit or built-in EtherNet/IP port transmission delays for sending and receiving using the following formulas. These times are the same for both UDP and TCP.

The delays found using the following formulas, however, are approximate values when one socket service is used. If multiple socket services are used, the delays will increase depending on the operating conditions. Also, the transmission delay on the network relative to the processing time is so small that it can be ignored, and so it is omitted.

■ **Requesting UDP Socket Services by Manipulating Dedicated Control Bits**

High-speed Socket Services Enabled and CPU Unit Cycle Time of Less Than 1.85 ms

Transmission processing time = reception processing time =
CPU Unit cycle time × 5 + number of send/receive bytes × 0.0002 + 1.45 (ms)

High-speed Socket Services Enabled and CPU Unit Cycle Time of 1.85 ms or Greater

Transmission processing time = reception processing time =
CPU Unit cycle time × 6 (ms)

High-speed Socket Services Disabled

Transmission processing time = reception processing time =
CPU Unit cycle time × 7 (ms)

■ **Requesting TCP Socket Services by Manipulating Dedicated Control Bits**

High-speed Socket Services Enabled and CPU Unit Cycle Time of Less Than 1.85 ms

Transmission processing time = reception processing time =
CPU Unit cycle time × 5 + number of send/receive bytes × 0.0002 + 1.45 (ms)

High-speed Socket Services Enabled and CPU Unit Cycle Time of 1.85 ms or Greater

Transmission processing time = reception processing time =
CPU Unit cycle time × 6 (ms)

High-speed Socket Services Disabled

Transmission processing time = reception processing time =
CPU Unit cycle time × 7 (ms)

■ **Requesting UDP Socket Services by Executing CMND(490)**

CPU Unit Cycle Time Less Than 20 ms

Transmission processing time = reception processing time =
CPU Unit cycle time × 6 + 70.0 (ms)

CPU Unit Cycle Time of 20 ms or Greater

Transmission processing time = reception processing time =
CPU Unit cycle time × 6 (ms)

■ **TCP Socket Services Using CMND(490)**

CPU Unit Cycle Time Less Than 20 ms

Transmission processing time = reception processing time =
CPU Unit cycle time × 6 + 70.0 (ms)

CPU Unit Cycle Time of 20 ms or Greater

Transmission processing time = reception processing time =
CPU Unit cycle time × 6 (ms)

Note

1. The values obtained from the above equations are guidelines for the transmission delay time when one socket in the EtherNet/IP Unit or built-in EtherNet/IP port is used only. The execution time required for the user program is not included.
2. The communications time for the remote nodes depends on the device being used. For remote nodes that are not EtherNet/IP Units or built-in EtherNet/IP ports, calculate the communications time according to the device's operation manual.
3. The actual operating environment can cause transmission delays larger than those calculated with the methods given here. Among the causes of longer delays are the following: traffic on the network, window sizes at network nodes, traffic through the EtherNet/IP Unit or built-in EtherNet/IP port (e.g., simultaneous servicing of multiple sockets and socket service communications, etc.), and the system configuration.
4. The above values are guidelines when 4% for the uniform peripheral servicing time in the PLC Setup is used.
5. By increasing the value of the uniform peripheral servicing time, the maximum transmission delay time for socket services can be shorter.
6. Processing cannot be faster than the send and receive processing performance of the EtherNet/IP Unit or built-in EtherNet/IP port if the send request is processed periodically using a ladder program timer or if receive request processing is performed for continuous data from a remote node. In particular, the data buffer on the receiving side may be exhausted. In such a case, adjust the send timing (i.e., send timing from remote node) or receive frequency so that the actual load is approximately 1.5 times slower than the processing performance.

Example: When using TCP socket services between two PLCs by manipulating specific bits (high-speed socket service enabled) to send/receive 512 bytes in both directions, the guideline for the maximum transmission delay time can be calculated according to the following conditions as shown in the table below.

CPU Unit cycle time (local node) = 1 ms

CPU Unit cycle time (remote node) = 4 ms

Item	Calculation
Reception processing time (local node)	1 × 5 + 512 × 0.0002 + 1.45 = 6.552 ms ≈ 6.6 ms
Transmission processing time (local node)	1 × 5 + 512 × 0.0002 + 1.45 = 6.552 ms ≈ 6.6 ms
Transmission processing time (remote node)	4 × 6 = 24.0 ms
Reception processing time (remote node)	4 × 6 = 24.0 ms
Maximum transmission delay	6.6 + 6.6 + 24.0 + 24.0 = 61.2 ms

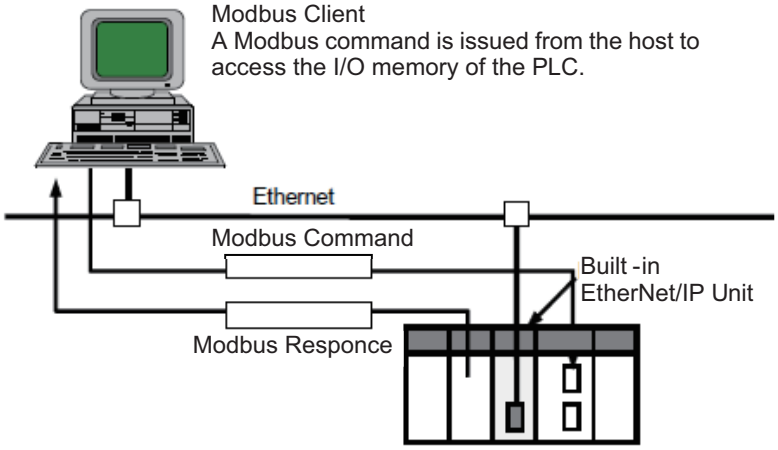
SECTION 15
Modbus Server Function

15-1 Modbus Server Function Overview 494
15-1-1 Overview 494
15-1-2 Specifications 495
15-1-3 Modbus Data Model 495
15-2 Modbus Server Settings 496
15-3 Example of Using the Modbus Server 498
15-4 Modbus Command Response Details 500

15-1 Modbus Server Function Overview

15-1-1 Overview

Allocating Modbus addresses in the I/O memory of the CPU Unit enables reading and writing in the I/O memory of the CPU Unit from a host PC, host PLC, HMI, or other Modbus client device. A Modbus server supports both of TCP and UDP.



The EtherNet/IP Unit (built-in port) that supports the Modbus server function is as follows.

Built-in EtherNet/IP Unit
CJ3M-CPU3□

The supported Modbus commands are as follows.

Function Code	Modbus	Function
0x01	Read Coils	Read multiple bits of I/O memory
0x03	Read Holding Registers	Read multiple words of I/O memory
0x05	Write Single Coil	Write bit of I/O memory
0x06	Write Single Register	Write 1 word of I/O memory
0x0F	Write Multiple Coils	Write multiple bits of I/O memory
0x10	Write Multiple Registers	Write multiple words of I/O memory
0x08	Diagnostic	Echo back test

Note Refer to 15-4 Modbus Command Response Details for details on Modbus commands.

15-1-2 Specifications

Item	Specifications	
	Modbus TCP Server	**Modbus UDP Server**
Protocol used	TCP/IP	UDP/IP
Message length	260 bytes max.	
Number of buffers	8	256
Port number	8 max.	-
Protection	502 (default) Can be changed.	502 (default) Can be changed.
Keep-alive time	Yes IP packet filtering is used (See note 1.)	
0x08	Common items for all connections (See note 2.) The setting range is 0 to 65,535 minutes. (The default is 0, meaning that the checking time is 5 minutes.)	-

Note (1) Refer to *13-5 IP Packet Filtering*.

(2) Set this in TCP/IP keep-alive on the TCP/IP Tab Page.

15-1-3 Modbus Data Model

The following four data models are defined in Modbus.

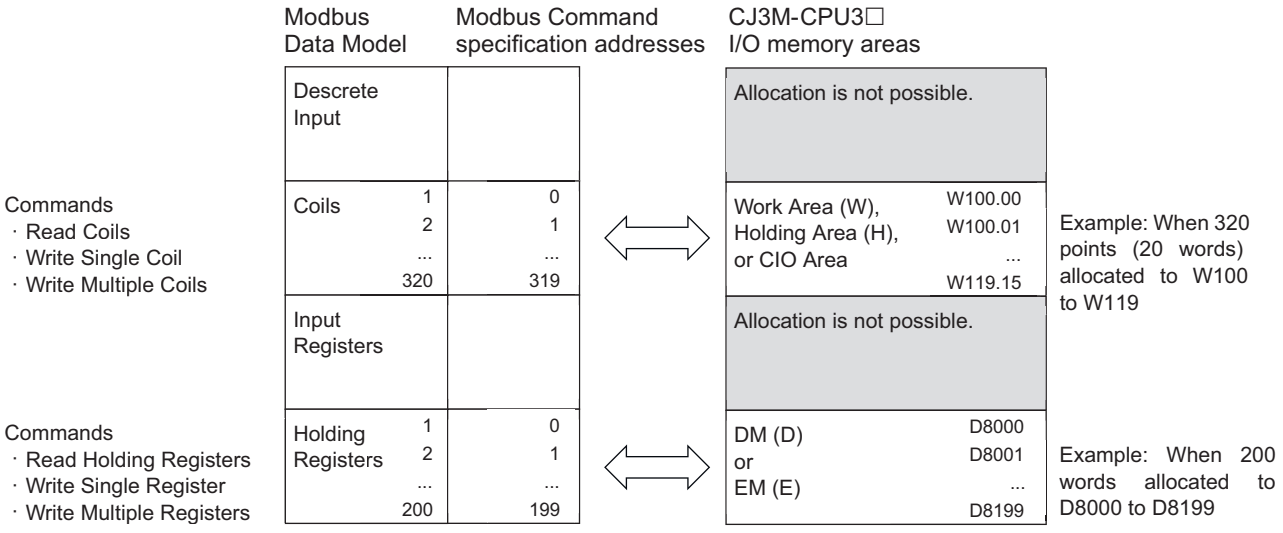
Each area of these data models is allocated to an I/O memory area in a CPU Unit.

■ **Example 1: When allocating 320 points (20 words) to work areas W100.00 to W119.15**

They can be allocated to 1 to 320 of the coils. Specify 0 to 319 in the addresses of the Modbus command.

■ **Example 2: When allocating 200 words to data memory D8000 to D8199**

They can be allocated to 1 to 200 of the holding registers. Specify 0 to 199 in the addresses of the Modbus command.

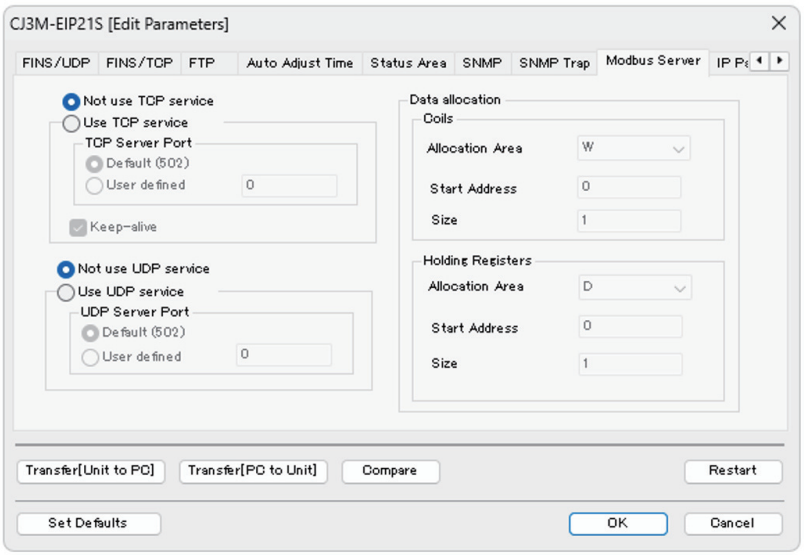


Note The addresses in the Modbus data model start from 1. The addresses to actually specify in the Modbus command start from 0. Consider this when creating an application.

15-2 Modbus Server Settings

Select the built-in ports on the I/O table, and then right-click and select Edit - Unit Setup.

Configure the settings on the Modbus Server Tab Page, and transfer them to the EtherNet/IP Unit (built-in port).



Settings

Item	Description	Default value
Use TCP Service	Select this to use the Modbus TCP server function. **Note** After the use of Modbus TCP server is set, the state becomes the passive open state with the automatically set port number, and the server waits for a connection from the host PLC/PC.	No
TCP Server Port	Sets the port number of the Modbus TCP server. To use a port number other than 502, select User defined and enter any port number. • 502 (default) • User defined: 0 to 65535 (If 0 is set, the default value of 502 will be set.)	502
Keep-alive	Enables or disables keep-alive. To disable it, clear the check box.	ON
Use UDP Service	Select this to use the Modbus UDP server function. **Note** After the use of Modbus UDP server is set, a port with an automatically set port number is opened.	No
UDP Server Port	Sets the port number of the Modbus UDP server. To use a port number other than 502, select User defined and enter any port number. • 502 (default) • User defined: 0 to 65535 (If 0 is set, the default value of 502 will be set.)	502

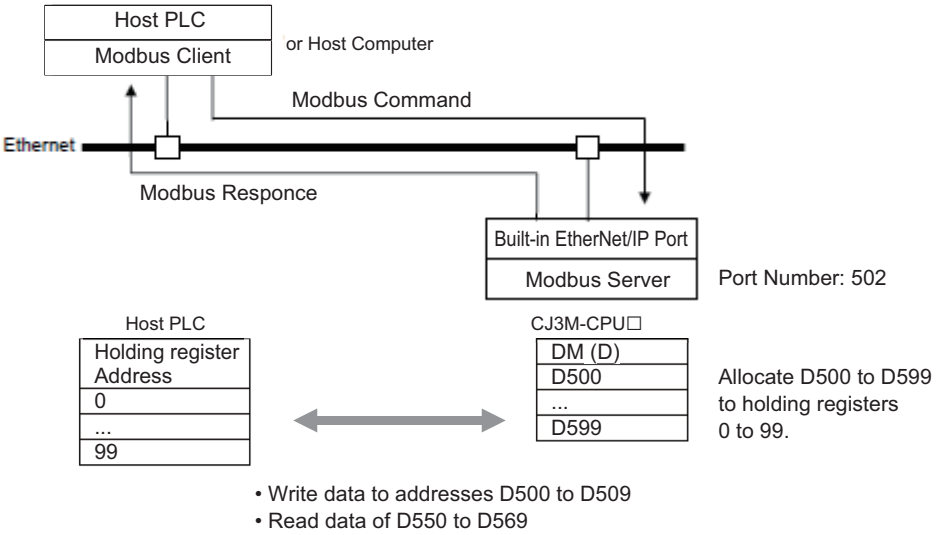
Item			Description	Default value
Data Allocation Settings (See note 2.)				
	Coils	Allocation Area	Sets an area that supports a Modbus data model. (Set Work Area: W, Holding Area: H, or CIO Area: CIO.)	Allocation Area: W
		Start Address	Sets the start address of the allocation area to allocate to the Modbus data model.	Start Address: 0
		Size	Sets the size to allocate to the Modbus data model. **Note** The number of allocation coils for setting word size becomes a multiple of 16. **Note** The allocation size can only be set to a size from the start address to the final address size of each area.	Allocation size: 1
	Holding Registers	Allocation Area	Sets an area that supports a Modbus data model. Set Data Memory: D, Expanded Data Memory: E0 to E9.	Allocation Area: D
		Start Address	Sets the start address of the allocation area to allocate to the Modbus data model.	Start Address: 0
		Size	Sets the size to allocate to the Modbus data model. **Note** The allocation size can only be set to a size from the start address to the final address size of the data memory / expanded data memory.	Allocation size: 1

Note (1) When the Modbus server function is not used, the EtherNet/IP Unit (built-in port) does not send a response to the Modbus command.

(2) Modbus data allocation is common between the Modbus TCP server and Modbus UDP server.

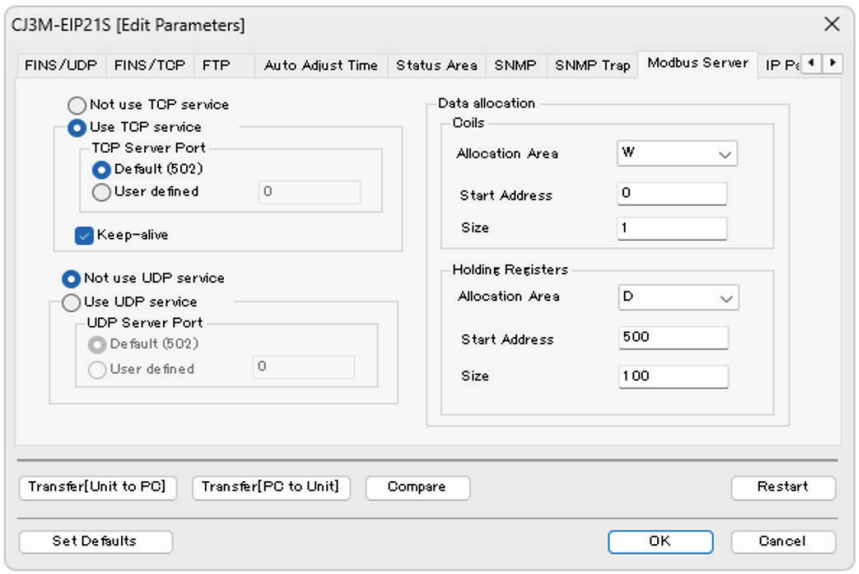
15-3 Example of Using the Modbus Server

A connection is established from the host PLC using Modbus TCP, and reading and writing of the I/O memory of the CPU Unit is performed.



- Write data to addresses D500 to D509
- Read data of D550 to D569

■ **Settings**



- Select Use TCP Service.
- Set area D (data memory), start address 500, and allocation size 100 for the settings of the holding registers.

Note Do not select to use the UDP Service because it will not be used, and also coils will not be used so no particular settings are required.

■ **Connect to the Host PLC**

- TCP opening is requested from the host PLC to the EtherNet/IP Unit (built-in port). (Active open)
- After a TCP connection is established, a Modbus command is sent from the host PLC, and a Modbus response is received from the EtherNet/IP Unit (built-in port).
- When writing data to D500 to D509

Commands

Field name	Data Bits	Data	Remarks
Function Code	1 Byte	0x10	Write Multiple registers
Register Start Address	2 Bytes	0x0000	Holding Register Address: 0
Register Number	2 Bytes	0x000A	10 words
Number of bytes	1 Byte	0x14	20 Bytes (10 words x 2)
Write data	20 Bytes	Write data	Data to write to D500 to D509

Response

Field name	Data Bits	Data	Remarks
Function Code	1 Byte	0x10	Write Multiple registers
Register Start Address	2 Bytes	0x0000	Holding Register Address: 0
Register Number	2 Bytes	0x000A	10 words

- When reading data from D550 to D569

Commands

Field name	Data Bits	Data	Remarks
Function Code	1 Byte	0x03	Read Holding registers
Register Start Address	2 Bytes	0x0032	Holding Register Address: 50
Register Number	2 Bytes	0x0014	20 words

Response

Field name	Data Bits	Data	Remarks
Function Code	1 Byte	0x03	Read Holding registers
Number of bytes	1 Bytes	0x28	40 Bytes (20 words x 2)
Read data	40 Bytes	Read data	Data read from D550 to D569

Note On the Modbus client side (host PLC/PC), incorporate retry processing and other measures to mitigate communication errors.

15-4 Modbus Command Response Details

■ Function 0x01 Read Coils: Read multiple contacts from I/O memory

Commands

Field name	Data Bits	Data
Function Code	1 Byte	01 hex
Coil Start Address	2 Bytes	0 to FFFF hex (0 to 65535)
Coil Size	2 Bytes	1 to 07D0 hex (1 to 2000)

Response

Field name	Data Bits	Data
Function Code	1 Byte	01 hex
Number of bytes data	1 Byte	N
Coil read data	n Bytes	Read data: n = N or N+1

Note N = number of coils / 8, and if the remainder of number of coils / 8 is other than 0, N = N+1

Example: When Modbus coil addresses 0 to 319 are allocated to Work Areas (W) W0 to W20 of the CPU Unit, and the 10 bits of W10.03 to W10.12 are read to Modbus coil addresses 163 to 172

Command: Host PC/PLC

Field name	Data
Function Code	01 hex
Coil Start Address	00A3 hex (163 or more = W10.03 or more) *
Coil Size	000A hex (10 bits)

Note W10.03 is the 163rd from W0.0

Response: Built-in EtherNet/IP Unit

Field name	Data
Function Code	01 hex
Number of bytes data	02 hex
Coil Data (W10.03 to W10.10)	8A hex
Coil Data (W10.11 to W10.12)	02 hex

CPU unit (Modbus server)

Bits	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
W10	(1)	(1)	(1)	(1)	(0)	(1)	(0)	(0)	(0)	(1)	(0)	(1)	(0)	(0)	(0)	(0)

*: The number in ( ) indicates the coil state.

Read

Host PC/PLC (Modbus client)

178	177	176	175	174	173	172	171	170	169	168	167	166	165	164	163
(0)	(0)	(0)	(0)	(0)	(0)	(1)	(0)	(1)	(0)	(0)	(0)	(1)	(0)	(1)	(0)

*: The number is a coil address, and the number in ( ) indicates the coil state.

Since the coil data read from the Modbus server is reflected in the coils of the Modbus client in bytes, coil addresses 173 to 178 are overwritten with 0.

■ Function 0x03 Read Holding Registers: Read multiple words of I/O memory

Commands

Field name	Data Bits	Data
Function Code	1 Byte	03 hex
Register Start Address	2 Bytes	0 to FFFF hex (0 to 65535)
Register Number	2 Bytes	1 to 007D hex (1 to 125)

Response

Field name	Data Bits	Data
Function Code	1 Byte	03 hex
Number of bytes	1 Byte	2 x N
Register read data	N x 2 Bytes	Read data

Note N = Number of read words

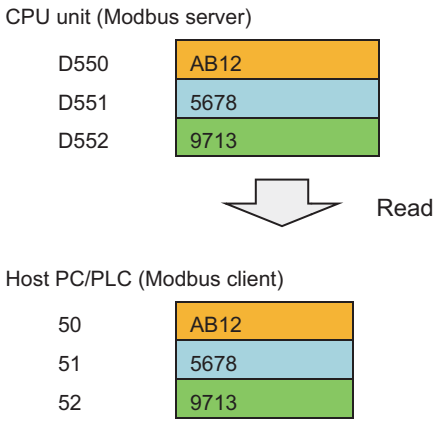
Example: When Modbus holding register addresses 0 to 99 are allocated to Data Registers (D) D500 to D599 of CPU Unit, and the 3 words of D550 to D552 are read to Modbus holding register addresses 50 to 52

Command: Host PC/PLC

Field name	Data
Function Code	03 hex
Register Start Address	0032 hex (50 or more = D550 or more)
Register Number	0003 hex (3 words)

Response: Built-in EtherNet/IP Unit

Field name	Data
Function Code	03 hex
Number of bytes	06 hex
Register Read Data (D550)	AB12 hex
Register Read Data (D551)	5678 hex
Register Read Data (D552)	9713 hex



■ Function 0x05 Write Single Coil: Write contact to I/O memory

Commands

Field name	Data Bits	Data
Function Code	1 Byte	05 hex
Coil Address	2 Bytes	0 to FFFF hex (0 to 65535)
Coil Output	2 Bytes	ON (1): FF00 hex OFF (0): 0000 hex

Response

Field name	Data Bits	Data
Function Code	1 Byte	05 hex
Coil Address	2 Bytes	0 to FFFF hex (0 to 65535)
Coil Output	2 Bytes	ON (1): FF00 hex OFF (0): 0000 hex

Example: When Modbus coil addresses 0 to 319 are allocated to Work Areas (W) W0 to W20 of CPU Unit, and W1.00 (Modbus coil address 16) is turned ON (1).

Command: Host PC/PLC

Field name	Data
Function Code	05 hex
Coil Address	0010 hex (16 = W1.00)
Coil Output	FF00 hex (ON)

Response: Built-in EtherNet/IP Unit

Field name	Data
Function Code	05 hex
Coil Address (W1.00)	0010 hex
Coil Output	FF00 hex (ON)

Note *: W1.00 is the 16th from W0.0

Host PC/PLC (Modbus client)

Coil Address: 16, Write Data: FF00 hex



Write

CPU unit (Modbus server)

Bits	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
W1																(1)

*: The number in ( ) indicates the coil state.

■ Function 0x06 Write Single Register: Write 1 word to I/O memory

Commands

Field name	Data Bits	Data
Function Code	1 Byte	06 hex
Register Address	2 Bytes	0 to 7FFF hex (0 to 32767)
Register write data	2 Bytes	Write data

Response

Field name	Data Bits	Data
Function Code	1 Byte	06 hex
Register Address	2 Bytes	0 to 7FFF hex (0 to 32767)
Register write data	2 Bytes	Write data

Example: When Modbus holding register addresses 00 to 99 are allocated to Data Registers (D) D500 to D599 of CPU Unit, and 3AC5 hex is written to D500 (holding register address 0)

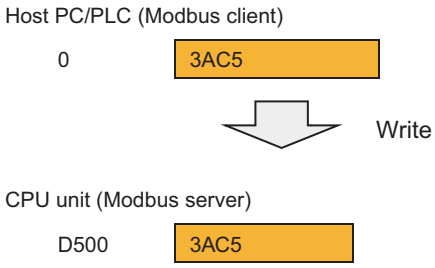
Command: Host PC/PLC

Field name	Data
Function Code	06 hex
Register Address	0000 hex (0 = D500)
Register Write Data	3AC5 hex

Response: Built-in EtherNet/IP Unit

Field name	Data
Function Code	06 hex
Register Address	0000 hex
Register Write Data	3AC5 hex

Note *: W1.00 is the 16th from W0.0



■ Function 0x0F Write Multiple Coils: Write multiple contacts to I/O memory

Commands

Field name	Data Bits	Data
Function Code	1 Byte	0F hex
Coil Start Address	2 Bytes	0 to FFFF hex (0 to 65535)
Coil Size	2 Bytes	1 to 07B0 hex (1 to 1968)
Number of bytes	1 Byte	N
Coil write data	N Bytes	Write data

Note N = number of coils / 8, and if the remainder of number of coils / 8 is other than 0, N = N+1

Response

Field name	Data Bits	Data
Function Code	1 Byte	0F hex
Coil Start Address	2 Bytes	0 to FFFF hex (0 to 65535)
Coil Size	2 Bytes	1 to 07B0 hex (1 to 1968)

Example: When Modbus coil addresses 0 to 319 are allocated to Work Areas (W) W0 to W20 of CPU Unit, and 0571 hex is written to the 11 bits of W5.10 to W6.04 (Modbus coil addresses 90 to 100)

Command: Host PC/PLC

Field name	Data
Function Code	0F hex
Coil Start Address	005A hex (90 or more = W5.10 or more)
Coil Size	000B hex (11 bits)
Coil Data (W5.10 to W6.01)	71 hex
Coil Data (W6.02 to W6.04)	05 hex

Response: Built-in EtherNet/IP Unit

Field name	Data
Function Code	0F hex
Coil Start Address	005A hex
Coil Size	000B hex

Note *: W5.10 is the 90th from W0.0

Host PC/PLC (Modbus client)

(0)	(0)	(0)	(0)	(0)	(1)	(0)	(1)	(0)	(1)	(1)	(1)	(0)	(0)	(0)	(1)

*: The number is a coil address, and the number in ( ) indicates the coil state.

Write

CPU unit (Modbus server)

Bits	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
W5	(1)	(1)	(0)	(0)	(0)	(1)										
W6												(1)	(0)	(1)	(0)	(1)

*: The number is a coil address, and the number in ( ) indicates the coil state.

■ Function 0x10 Write Multiple Registers: Write multiple words to I/O memory

Commands

Field name	Data Bits	Data
Function Code	1 Byte	10 hex
Register Start Address	2 Bytes	0 to 7FFF hex (0 to 32767)
Register Number	2 Bytes	1 to 007B hex (1 to 123)
Number of bytes	1 Byte	2 x N
Coil write data	N Bytes	Write data

Note N = Number of registers to write

Response

Field name	Data Bits	Data
Function Code	1 Byte	0F hex
Coil Start Address	2 Bytes	0 to FFFF hex (0 to 65535)
Coil Size	2 Bytes	1 to 07B0 hex (1 to 1968)

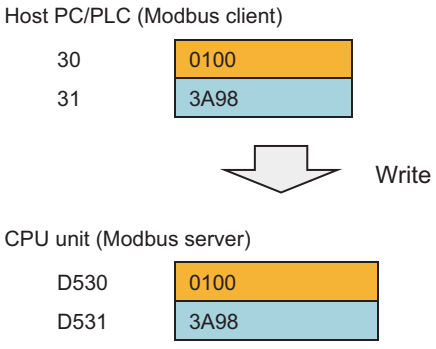
Example: When Modbus holding register addresses 0 to 99 are allocated to Data Registers (D) D500 to D599 of CPU Unit, and data is written to D530 to D531 (holding register addresses 30 to 31)

Command: Host PC/PLC

Field name	Data
Function Code	10 hex
Register Start Address	001E hex (30 or more = D530 or more)
Register Number	02 hex (2 words)
Number of bytes	04 hex
Register Write Data (D500)	0100 hex
Register Write Data (D501)	3A98 hex

Response: Built-in EtherNet/IP Unit

Field name	Data
Function Code	10 hex
Register Start Address	001E hex
Register Number	02 hex (2 words)



■ Function 0x08 Write Multiple Registerss: Write multiple words to I/O memory

Commands

Field name	Data Bits	Data
Function Code	1 Byte	08 hex
Subfunction	2 Bytes	0000 hex Sub-functions other than echoback are not supported.
Data	2 Bytes	0000 to FFFF hex, any data

Note N = Number of registers to write

Response

Field name	Data Bits	Data
Function Code	1 Byte	08 hex
Subfunction	2 Bytes	0000 hex
Data	2 Bytes	Data of received command

Example: Echoback data from host PC/PLC.

Example: Echoback data from host PC/PLC.

Command: Host PC/PLC

Field name	Data
Function Code	08 hex
Subfunction	0000 hex
Data	5555 hex

Response: Built-in EtherNet/IP Unit

Field name	Data
Function Code	08 hex
Subfunction	0000 hex
Data	5555 hex

■ Error response

Response

Field name	Data Bits	Data
Function Code	1 Byte	Function code + 80 hex
Error code	1 Byte	See below.

Error code	Name	Description
01 hex	ILLEGAL FUNCTION	This is a support code that is not supported by the unit.
02 hex	ILLEGAL DATA ADDRESS	There is a mistake with the specified start address. The specified start address and data length exceed the valid range of the allocated I/O memory The specified data length are outside of the valid range The specified data length differs from the actual data length The received data is less than 4 bytes

Error code	Name	Description
03 hex	ILLEGAL DATA VALUE	There is a mistake with the specified data The coil output of Write Single Coil is other than 0000 or FF00 hex
04 hex	SLAVE DEVICE FAILURE	Reading/writing is not possible An area that is not supported by the CPU Unit is set in the Modbus data allocation settings

SECTION 16
Modbus Client Function

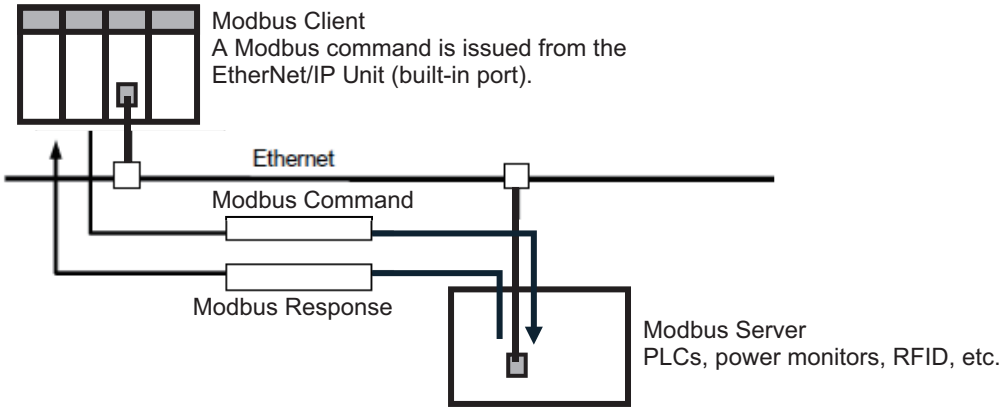
16-1 Modbus Client Function Overview 510
16-1-1 Overview 510
16-1-2 Specifications 511
16-2 Example of Using the Modbus Server 512

16-1 Modbus Client Function Overview

16-1-1 Overview

A device (such as a PLC) with a Modbus server function can be accessed by a Modbus client function.

A Modbus command is issued from the EtherNet/IP Unit (built-in port) to write/read data in the Modbus server device. To issue a Modbus command, a function block using a socket service function is used. The function blocks support Modbus TCP clients and Modbus UDP clients.



The CPU Units and EtherNet/IP Units (built-in ports) that support the function blocks for Modbus clients are as follows.

CPU Units	Built-in EtherNet/IP Unit
CJ2□-CPU□□(-EIP)	CJ1W-EIP21S
CJ3□-CPU□□	CJ3M-CPU3□

Note Use with CS1/CJ1/CP1H CPU Unit is not possible because the CMND2 instruction is used inside the function block.

The function blocks that can be used and supported Modbus commands are as follows.]

- Function Block for Modbus TCP Client

Function	Function Block Name	Function Code	Modbus Function
Read Coils	_EIPS020_ModbusTcp_Fun01	0x01	Read Coils
Read Holding Registers	_EIPS021_ModbusTcp_Fun03	0x03	Read Holding Registers
Write Single Coil	_EIPS022_ModbusTcp_Fun05	0x05	Write Single Coil
Write Single Register	_EIPS023_ModbusTcp_Fun06	0x06	Write Single Register
Write Multiple Coils	_EIPS024_ModbusTcp_Fun0F	0x0F	Write Multiple Coils
Write Multiple Registers	_EIPS025_ModbusTcp_Fun10	0x10	Write Multiple Registers
Open TCP Socket Active	_EIPS002_SOCKET_TcpOpenActive	-	-
Close TCP Socket	_EIPS003_SOCKET_TcpClose	-	-

• Function Block for Modbus UDP Client

Function	Function Block Name	Function Code	Modbus Function
Read Coils	_EIPS030_ModbusUdp_Fun01	0x01	Read Coils
Read Holding Registers	_EIPS031_ModbusUdp_Fun03	0x03	Read Holding Registers
Write Single Coil	_EIPS032_ModbusUdp_Fun05	0x05	Write Single Coil
Write Single Register	_EIPS033_ModbusUdp_Fun06	0x06	Write Single Register
Write Multiple Coils	_EIPS034_ModbusUdp_Fun0F	0x0F	Write Multiple Coils
Write Multiple Registers	_EIPS035_ModbusUdp_Fun10	0x10	Write Multiple Registers
Open UDP Socket	_EIPS011_SOCKET_UdpOpen	-	-
Close UDP Socket	_EIPS013_SOCKET_UdpClose	-	-

For details on function blocks, refer to Appendix M Function Block for Modbus Client.

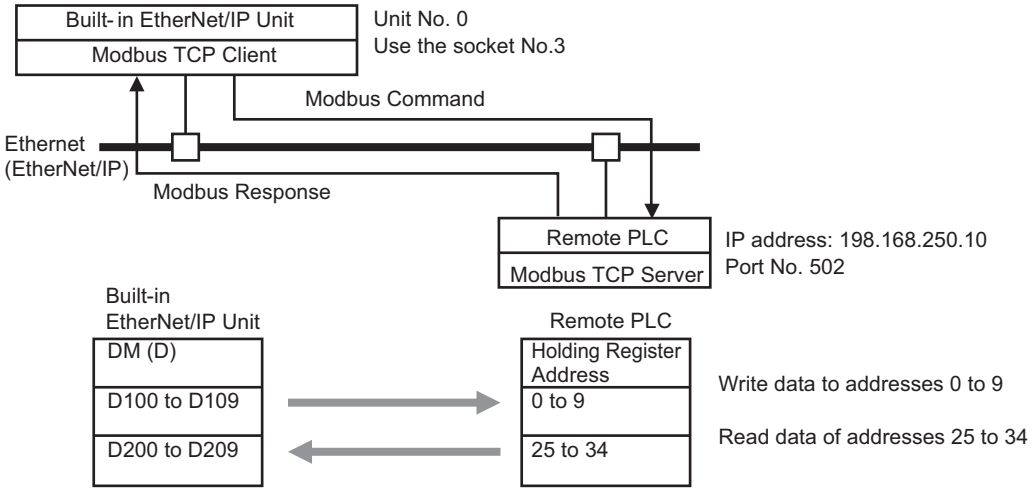
16-1-2 Specifications

Item	Specifications	
	Modbus TCP Server	**Modbus UDP Server**
Protocol used	TCP/IP Use the socket service functions by CMND2 instruction	UDP/IP Use the socket service functions by CMND2 instruction
Socket Number	8 max. Up to 8 in combination with socket service functions	8 max. Up to 8 in combination with socket service functions
Port Number	Specify with input variable of the function block	Specify with input variable of the function block
Keep-alive time (See note 1.)	Common items for all connections The setting range is 0 to 65,535 minutes. (The default is 0, meaning that the checking time is 5 minutes.) Set enable/disable with the TCP socket open (ACTIVE) function block.	-
Response monitor time	Set this in “Response monitoring time / function block internal communication instruction” of “Function block internal communication instruction settings” of the PLC system settings. (Default value: 2 seconds)	
Number of retries	Set this in “Number of retries” of “Function block internal communication instruction settings” of the PLC system settings. (Default value: 0)	

1. Set this in TCP/IP keep-alive on the TCP/IP Tab Page.

16-2 Example of Using the Modbus Server

Use Modbus TCP client function blocks to read/write the memory data allocated in holding registers of the remote PLC.



Use the following four types of function block.

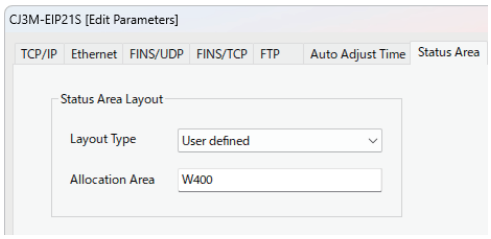
Function	Function Block Name	Function Code	Modbus Function
Read Holding Registers	_EIPS021_ModbusTcp_Fun03	0x03	Read Holding Registers
Write Multiple Registers	_EIPS025_ModbusTcp_Fun10	0x10	Write Multiple Registers
Open TCP Socket Active	_EIPS002_SOCKET_TcpOpenActive	-	-
Close TCP Socket	_EIPS003_SOCKET_TcpClose	-	-

■ Settings

- Built-in EtherNet/IP Unit Settings

Select User defined for the Layout Type on the Status Area Tab Page. Allocate any area for the allocated area. The user defined area occupies 64 words.

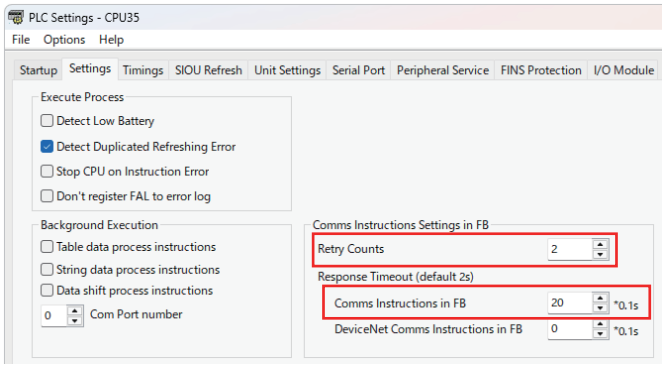
Example: When allocated to W400 to W463



- CPU Unit Settings

Set the number of transfer retries and the response monitoring time / Function block internal communication instruction from the function block internal communication instruction settings on the CPU Unit Settings Tab Page of the PLC system settings.

Example: Set the number of transfer retries to 2 and the response monitoring time to 2 seconds.

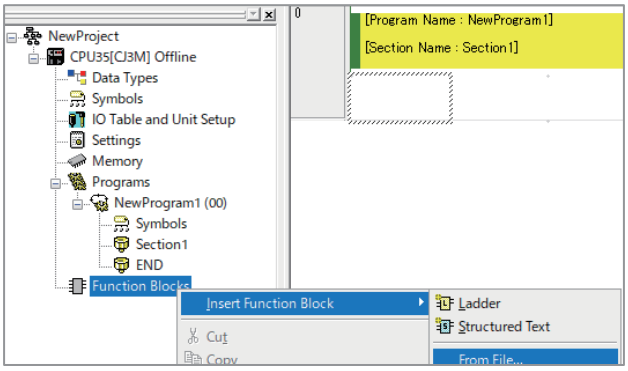


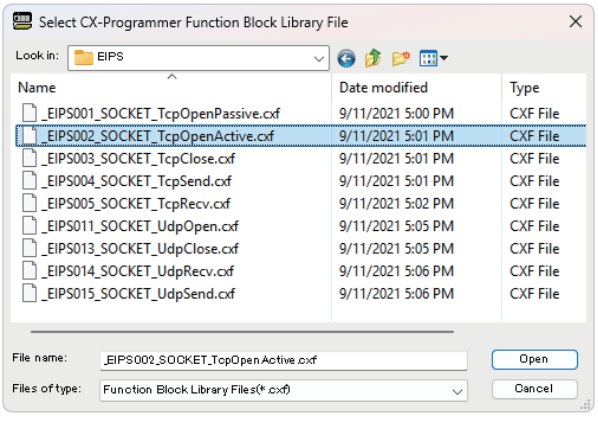
■ Read Function Blocks

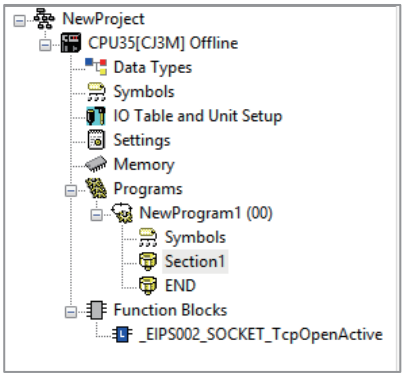
In the CX-Programmer, right-click the Function Block, and select Insert Function Blocks - Load the Library Files.

In the selection of the function block library file, select the function block file (.cxf) to insert for the Modbus client from the following folder.

C:\Program Files (x86)\OMRON\CX-One\Lib\FBL\omronlib\programmable controller\EIPS



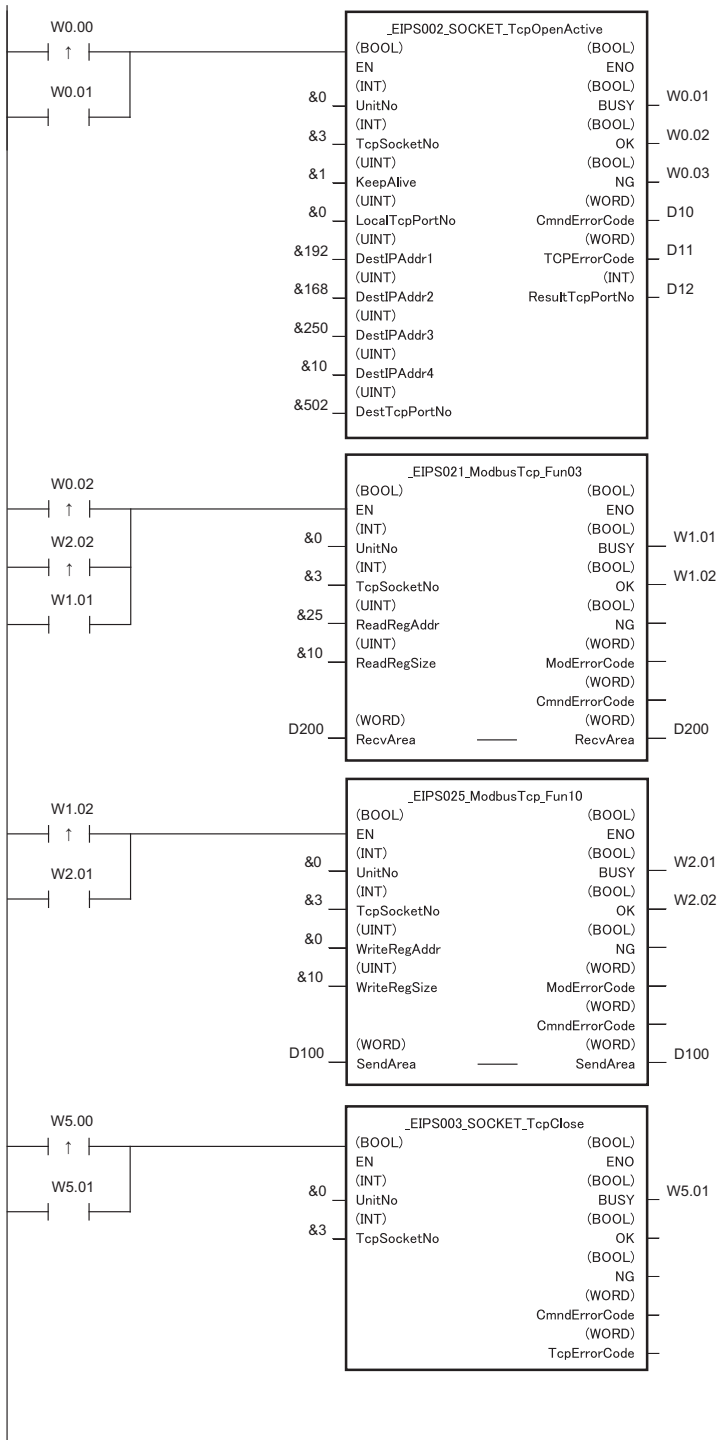




■ Create a ladder program

Insert function blocks to create a ladder program.

- Execute TCP active opening upon the rising edge of W0.00 to establish a connection with the remote PLC (IP address 192.168.250.10, port number 502). Set the local TCP port number to be allocated automatically and enable Keep-alive.
- After a connection is established (after W0.02 turns ON), repeat reading of the data from the remote PLC (reading holding registers 25 to 34 of the remote PLC to D200 to D209) and writing of the data (writing of D100 to D109 to holding registers 0 to 9 of the remote PLC).
- Disconnect the connection with the remote PLC port upon the rising edge of W5.00.



Use Unit No. 0 and TCP socket No. 3 to start TCP active opening upon the rising edge of W0.00. (Destination IP address: 192.168.250.10, port No.: 502)
Enable keep-alive.

After a connection is established, W0.02 turns ON, and the local port number that is connected is stored in D12.

If the connection fails, W0.03 turns ON and the end code (error code) is stored in D10/D11.

Start reading 10 words worth of data from Holding Register address 25 to D200 to D209 upon the rising edge of W0.02 when a _EIPS002_SOCKET_TcpOpenActive connection is established and upon the rising edge of W2.02 when _EIPS025_ModbusTcp_Fun10 writing completes.
W1.02 turns ON after reading completes.

Start writing the data of D100 to D109 from Holding Register addresses 0 to 9 words upon the rising edge of W1.02 when _EIPS025_ModbusTcp_Fun03 reading completes.

W2.02 turns ON after writing completes.

Close the connection upon the rising edge of W5.00.

SECTION 17
Maintenance and Unit Replacement

This section describes cleaning, inspection, and Unit replacement procedures, as well as the Simple Backup Function.

17-1 Maintenance and Replacement 516
17-1-1 Cleaning 516
17-1-2 Inspection 516
17-1-3 Unit Replacement Procedure 516
17-2 Simple Backup Function 517
17-3 Using the Backup Tool 522
17-4 Replacing Target Nodes during Communications 523
17-5 Unit Initialization 526

17-1 Maintenance and Replacement

This section describes the routine cleaning and inspection recommended as regular maintenance, as well as the Unit replacement procedure required if an EtherNet/IP Unit needs to be replaced.

17-1-1 Cleaning

Clean the EtherNet/IP Unit regularly as described below in order to keep the network in its optimal operating condition.

- Wipe the Unit daily with a dry, soft cloth.
- When a spot can't be removed with a dry cloth, dampen the cloth with a neutral cleanser (2% solution), wring out the cloth, and wipe the Unit.
- A smudge may remain on the Unit from gum, vinyl, or tape that was left on for a long time. Remove the smudge when cleaning.

⚠ **Caution** Never use volatile solvents such as paint thinner, benzene, or chemical wipes. These substances could damage the surface of the Unit.

17-1-2 Inspection

Be sure to inspect the system periodically to keep it in its optimal operating condition. In general, inspect the system once every 6 to 12 months, but inspect more frequently if the system is used with high temperature or humidity or under dirty/dusty conditions.

Inspection Equipment

Prepare the following equipment before inspecting the system.

Normally Required Equipment

Have a standard and Phillips-head screwdriver, multimeter, alcohol, and a clean cloth.

Occasionally Required Equipment

Depending on the system conditions, a synchroscope, oscilloscope, thermometer, or hygrometer (to measure humidity) might be needed.

Inspection Procedure

Check the items in the following table and correct any items that are below standard.

Item		Standard	Inspection
Environmental conditions	Ambient and cabinet temperature	0 to 55°C	Thermometer
	Ambient and cabinet humidity	10 to 90% (with no condensation or icing)	Hygrometer
	Dust/dirt accumulation	None	Visual
Installation	Are the Units installed securely?	No looseness	Phillips-head screwdriver
	Are the Ethernet cable connectors fully inserted and locked?	No looseness	Visual

17-1-3 Unit Replacement Procedure

Replace a faulty EtherNet/IP Unit as soon as possible. If the built-in EtherNet/IP port is faulty, replace the CPU Unit as soon as possible. We recommend having spare Units available to restore network operation as quickly as possible.

Precautions

Observe the following precautions when replacing a faulty Unit.

- After replacement, verify that there are no errors with the new Unit.

- When a Unit is being returned for repair, attach a sheet of paper detailing the problem and return the Unit to your OMRON dealer.
- If there is a faulty contact, try wiping the contact with a clean, lint-free cloth dampened with alcohol.

Note To prevent electric shock when replacing a Unit, always stop communications in the network and turn OFF the power supplies to all of the nodes before removing the faulty Unit.

Settings Required after Unit Replacement

After a Unit has been replaced, verify that the following steps have been made correctly.

- Set the node address and unit number.
- Connect the Ethernet cable.
- Set the configuration data (parameter settings) again and download them.

17-2 Simple Backup Function

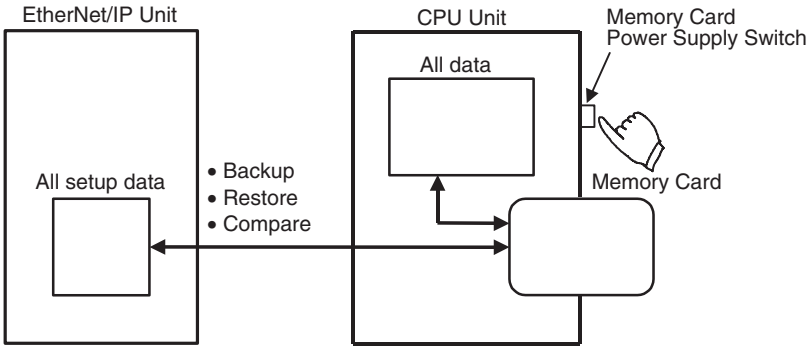
Overview

The simple backup function can be used to back up not only all of the data in the CPU Unit, but also all of the data stored in memory in the EtherNet/IP Unit or data for the built-in EtherNet/IP port. All of this data will automatically be backed up to the Memory Card.

The simple backup function can be used for the following EtherNet/IP Units and built-in EtherNet/IP port.

- CS-series EtherNet/IP Unit (CS1W-EIP21/EIP21S) mounted to a CS1D/CS1-H CPU Unit
- CJ-series EtherNet/IP Unit (CJ1W-EIP21/EIP21S) mounted to a CJ1-H/CJ1M/CJ2H/CJ2M/CJ3M CPU Unit
- A built-in EtherNet/IP port on a CJ2H-CPU□□-EIP/CJ2M-CPU3□/CJ3M-CPU3□ CPU Unit

When the EtherNet/IP Unit's setup data is written to the Memory Card using a simple backup operation, it is stored in the Memory Card as a Unit/Board backup file with the file name BACKUP□□.PRM. (The □□ digits in the backup file name indicate the unit address of the EtherNet/IP Unit or built-in EtherNet/IP port, which is the unit number + 10 hex.)
This backup file is also used when reading data from the Memory Card or comparing data with a file in the Memory Card.



Applications

Use the simple backup function when creating a backup data file for the entire PLC (including the CPU Unit, EtherNet/IP Units, built-in EtherNet/IP port, and Serial Communications Units/Boards), or when replacing all the Units.

Backup Sources and Restore Targets

The data that was backed up with the simple backup function can be restored to Units or built-in ports as shown in the following table. Network Configuration designations are given for the model numbers and versions of the backup sources and restore targets.

The model number must be the same for both the backup source and restore target. The CIP revision must be the same or higher.

CS1W-EIP21, CJ1W-EIP21

Restore target / Backup source	Rev. 1.01	Rev. 2.01	Rev. 3.01
Rev. 1.01	Yes	Yes (See note 1.)	Yes (See note 1.)
Rev. 2.01	No	No	Yes (See note 1.)
Rev. 3.01	No	No	Yes (See note 1.)

CJ2B-EIP21 (CJ2H-CPU6□-EIP), CJ1W-EIP21 (CJ2)

Restore target / Backup source	Rev. 2.01	Rev. 3.01
Rev. 2.01	Yes	Yes (See note 1.)
Rev. 3.01	No	Yes (See note 1.)

CJ2M-EIP21 (CJ2M-CPU3□)

Restore target / Backup source	Rev. 2.01	Rev. 2.02
Rev. 2.01	Yes	Yes
Rev. 2.02	No	Yes

CS1W-EIP21S, CJ1W-EIP21S

Restore target / Backup source	Rev. 4.01
Rev. 4.01	Yes

CJ3M-EIP21S (CJ3M-CPU3□)

Restore target / Backup source	Rev. 4.02
Rev. 4.02	Yes

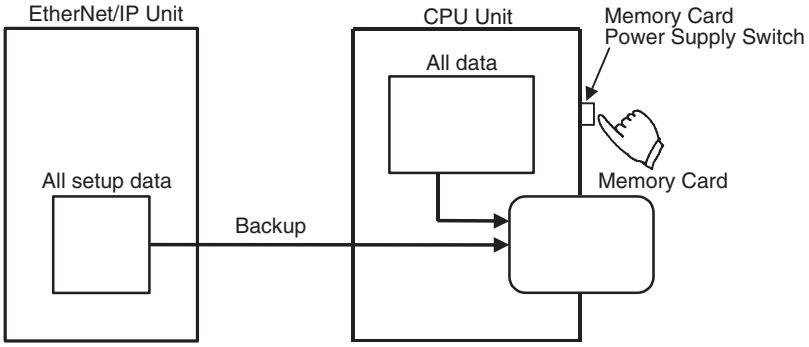
Note Simple backup data that was backed up with a lower version (example: Rev. 2.01) can be restored to a Unit (built-in port) of a higher version (example: Rev. 3.01), but an error will occur in the comparison. In addition, the setting items of the functions added in the higher version will become the defaults. When changing the unit version, refer to *6-2-18 Changing Devices* for information on the Network Configurator device change function.

Operating Methods

Backing Up EtherNet/IP Unit or Built-in EtherNet/IP Port Setup Files to the Memory Card

Set pins 7 and 8 of the DIP switch on the front panel of the CPU Unit as shown in the following table, and press the Memory Card Power Supply Switch for 3 seconds with the Memory Card inserted into the slot. Release the switch when the BUSY indicator lights.

DIP switch settings	
SW7	ON
SW8	OFF



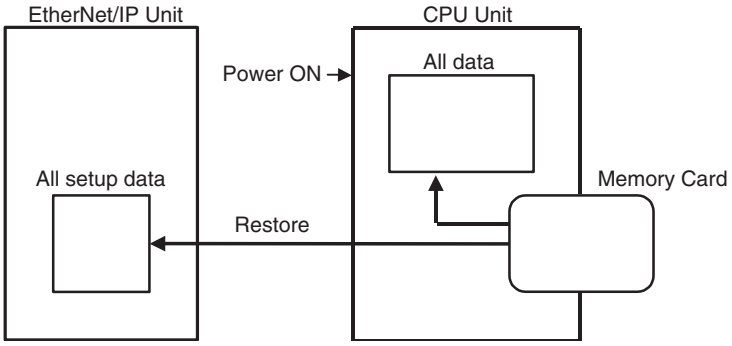
This operation will create an EtherNet/IP Unit or built-in EtherNet/IP port settings file, and write that file to the Memory Card along with the other backup files. When the Memory Card Power Supply Switch is pressed, the MCPWR indicator on the front of the CPU Unit will flash once and then remain lit while data is being written. If the data is written normally, the MCPWR indicator will turn OFF. The BUSY indicator will flash while the data is being written.

Note The backup operation will fail if it is performed after the device parameters were not downloaded successfully from the Network Configurator or CX-Programmer. Perform the backup operation only if the device parameters were downloaded normally.

Restoring the EtherNet/IP Unit or Built-in EtherNet/IP Port Setup File from the Memory Card (Reading and Setting the Data in the Unit)

Set pins 7 and 8 of the DIP switch on the front panel of the CPU Unit, as shown in the following table, and turn the power to the CPU Unit OFF and then ON again with the Memory Card inserted into the slot.

DIP switch settings	
SW7	ON
SW8	OFF



This operation will read the EtherNet/IP Unit or built-in EtherNet/IP port setup data file from the Memory Card and restore the data in the EtherNet/IP Unit or built-in EtherNet/IP port.

When the power supply is ON, the MCPWR indicator on the front of the CPU Unit will turn ON, flash once, and then remain lit while data is being read. The BUSY indicator will flash while data is being read. After the data has been read correctly, the MCPWR and BUSY indicators will turn OFF. If the MCPWR indicator flashes five times or if only the BUSY indicator turns OFF, it means that an error has occurred.

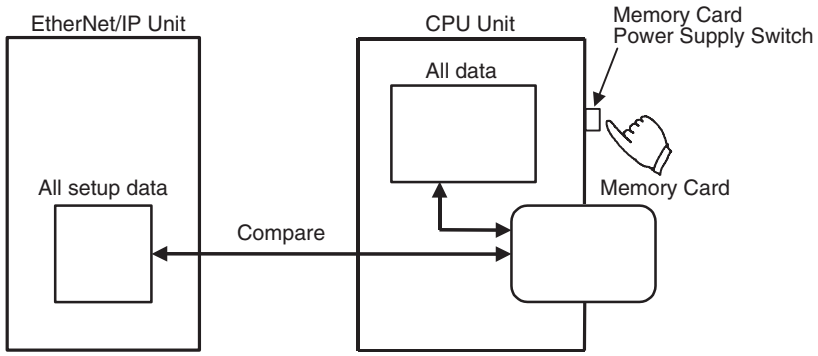
After completion of the restore operation, return the CPU Unit to its original DIP switch settings (change SW7 to OFF), and reset the EtherNet/IP Unit or built-in EtherNet/IP port or turn the power OFF and then ON again to reflect the restored settings.

Note Data backed up for CIP revision 1.01 using a simple backup can be restored to an EtherNet/IP Unit or built-in EtherNet/IP port with revision 2.01, but an error will occur in the comparison. When changing the unit version, refer to *6-2-18 Changing Devices* for information on the Network Configurator device change function.

Comparing EtherNet/IP Unit or Built-in EtherNet/IP Port Data with the Setup File in the Memory Card

Set pins 7 and 8 of the DIP switch on the front panel of the CPU Unit, as shown in the following table, and press down the Memory Card Power Supply Switch for 3 seconds.

DIP switch settings	
SW7	OFF
SW8	OFF



This operation will compare the data in the EtherNet/IP Unit or built-in EtherNet/IP port setup file in the Memory Card with the device parameters in the EtherNet/IP Unit or built-in EtherNet/IP port.

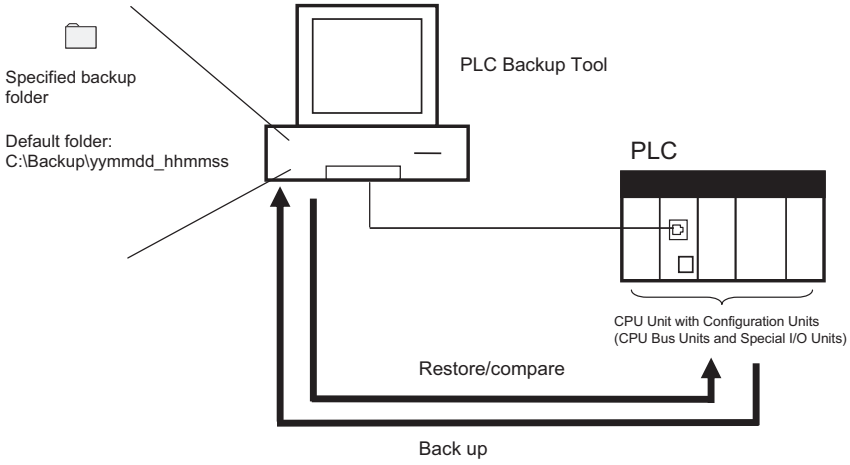
When the Memory Card Power Supply Switch is pressed, the MCPWR indicator on the front of the CPU Unit will flash once, and then remain lit while data is being compared. The BUSY indicator will flash while data is being compared. If the data matches, the MCPWR and BUSY indicators will turn OFF. If the MCPWR and BUSY indicators both flash, it means that the data does not match or that an error has occurred.

Note Data backed up for revision 1.1 using a simple backup can be restored to an EtherNet/IP Unit or built-in EtherNet/IP port with revision 2.1, but an error will occur in the comparison. When changing the unit version, refer to *6-2-18 Changing Devices* for information on the Network Configurator device change function.

17-3 Using the Backup Tool

Overview

The PLC Backup Tool of the CX-Programmer can be used to back up, compare, and restore data for all Units or only specified Units in the PLC that is connected online.



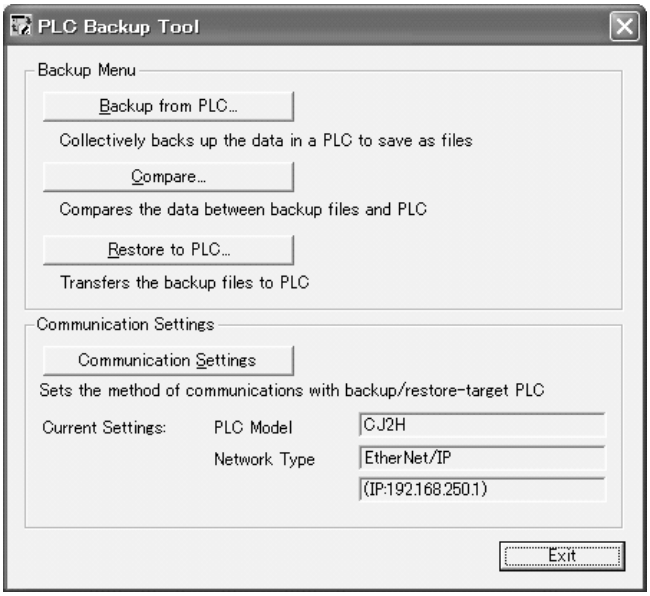
Usage

The PLC Backup Tool can be used for the following:

- Backing up all data in a PLC
- Comparing all of the data in a PLC with data that was previously backed up in the computer
- Using the restore function to transfer all of the PLC data to a system with the same configuration
- Transferring data to a new Unit after replacing a faulty Unit

Procedure

Select ***PLC Backup Tool*** from the CX-Programmer's Tool Menu. You can also select ***OMRON - CX-One - CX-Programmer - PLC Backup Tool*** from the Windows Start Menu.



Backup Menu

Button	Function
Backup from PLC	Click this button to back up data. All of the data in the target PLC will be backed up to the computer.
Compare	Click this button to compare data. The data in the PLC can be compared to the data in a backup file or the data in two backup files can be compared. Any differences will be displayed.
Restore to PLC*1	Click this button to restore data. The data in a backup file will be transferred to the PLC to restore the status that existed when the data was backed up.

*1 After completion of the restore operation, reset the EtherNet/IP Unit or built-in EtherNet/IP port or turn the power OFF and then ON again to reflect the restored settings.

Communications Settings

Button	Function
Communication Settings	Click this button to set communications conditions for the target PLC. The current PLC model and network type will be displayed.

Refer to the *CX-Programmer Operation Manual* for detailed procedures.

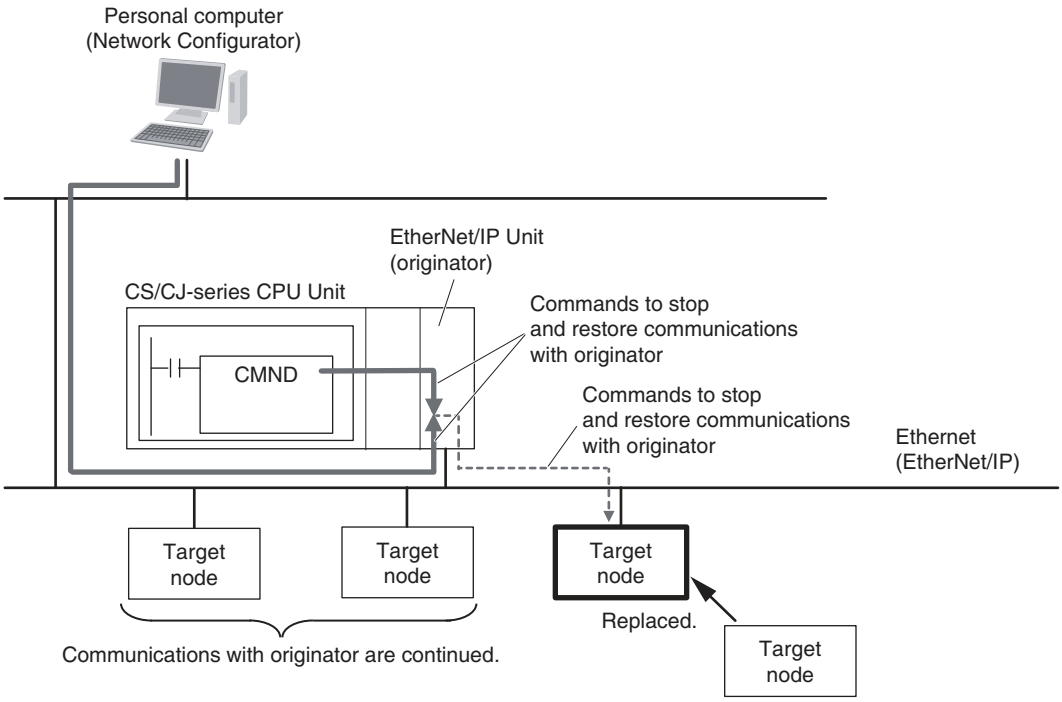
17-4 Replacing Target Nodes during Communications

You can replace a specified target node without stopping the entire communications system to replace a faulty target node or to perform maintenance.

Note This is enabled for CJ3M-CPU3□ or CS1W/CJ1W-EIP21S only.

Overview of Target Node Replacement Work

A command is sent from a computer or CPU Unit to temporarily stop communications for the specified target node. After the node is replaced, another command is sent to restore communications. In the rest of this section, the command used to stop communications with the target node is referred to as the disconnection command and the command to restore communications is referred to as the connection command.



Note (1) Remove the target node to replace only after you send a disconnection command to disconnect the node from the network. A Tag Data Link Error will occur if you remove the target node from the network before you send a disconnection command.

(2) Set the new target node to the same IP address and connection settings as the target node that you are replacing. A Tag Data Link Error or Verification Error will occur if the settings are different.

The procedures to disconnect and connect a target node and the replacement procedure are given below.

Target Node Replacement Procedure

1,2,3...

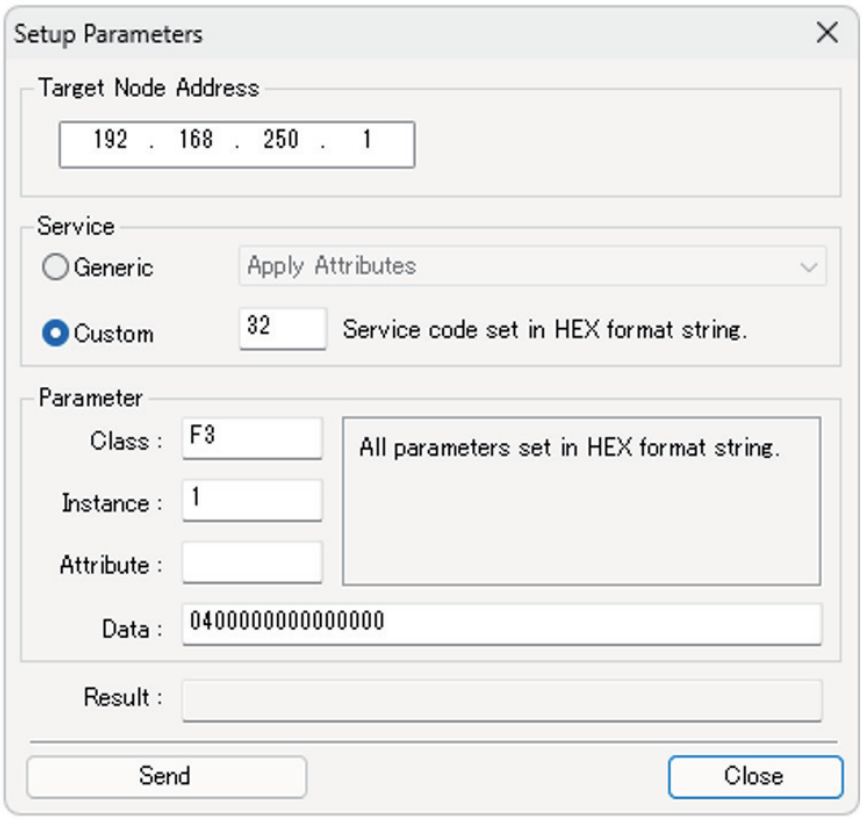
1. Tell the originator to disconnect the target node to replace and confirm that the target node was disconnected.
2. Turn OFF the power supply to the target node to replace and remove the communications cable.
3. Connect the communications cable to the new target node and turn ON the power supply.
4. Tell the originator to connect the new target node and confirm that the target node was connected.

Specific methods for the above steps are provided below.

■ **Sending Disconnection and Connection Commands**

Use one of the following two methods to tell the originator to disconnect and connect the target node.

Method 1: Send a message from the Setup Parameters Dialog Box in the Network Configurator.



Method 2: Send a message by executing the CMND instruction

Send the following messages.

- Disconnection Command
  Execute the Close_Connections_ByNode service of the Connection Configuration object.
- Connection Command
  Execute the Open_Connections_ByNode service of the Connection Configuration object.

For details on the services, refer to *9-2-2 Connection Configuration Object*.

■ **Confirming Disconnection and Connection**

There are the following two methods to confirm if the target node was disconnected or connected.

Method 1: Check the target node status on the Support Software.

For details, refer to *Connection Tab Page* in *18-1-1 The Network Configurator's Device Monitor Function*. Disconnections are displayed in gray and connections are displayed in blue.

Method 2: Check the Normal Target Node Table (EtherNet/IP Unit to CPU Unit) system-defined variable.

Refer to *SECTION 4 Memory Allocations*. The bit for the target node is OFF if the node is disconnected and ON if the node is connected.

17-5 Unit Initialization

This section describes how to initialize an EtherNet/IP Unit (restore it to the factory default state).

Note When the EtherNet/IP Unit is restored to the factory default state, the user authentication account information for CS1W/CJ1W-EIP21S and CJ3M-CPU3☐ is all cleared.

How to Initialize

The following methods are available to initialize your EtherNet/IP Unit to the defaults. Method A is recommended for security reasons.

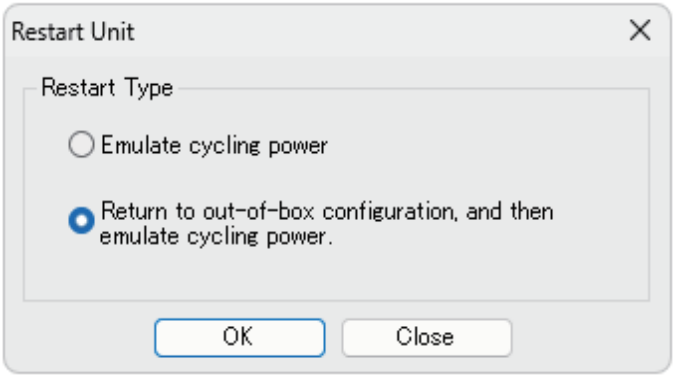
A Initialize the Unit from the Support Software connected to the USB, peripheral, or serial port of the CPU Unit.

B Initialize the Unit from the Support Software connected via Ethernet without using secure communications.

In either case, you must restart the Unit after initializing the Unit to the defaults.

To restart the EtherNet/IP Unit after restoring the factory default settings with the CX-Programmer, follow the steps below.

1. Click [Restart] in the Edit Parameters Dialog Box and, in a confirmation dialog box for restart, click [Yes].
   The Restart Unit Dialog Box is displayed.
2. Select Return to out-of-box configuration, and then emulate cycling power. and click [OK].



Note

- Be aware that the above Method B is for connection via a network that does not use secure communications or user authentication. For this reason, use it only in a network installed with security measures other than the security functions provided by the EtherNet/IP Unit or built-in EtherNet/IP port, such as a firewall.
- Depending on the settings of opening and closing the port or IP packet filtering, your connection attempts may fail. Determine the settings for EtherNet/IP Unit or built-in EtherNet/IP port in consideration of such cases. Refer to *13-4 Opening and Closing the Port* and *13-5 IP Packet Filtering* for details on these functions.

SECTION 18
Troubleshooting and Error Processing

This section describes error processing, periodic maintenance operations, and troubleshooting procedures needed to keep the EtherNet/IP network operating properly. We recommend reading through the error processing procedures before operation so that operating errors can be identified and corrected more quickly.

18-1 Checking Status with the Network Configurator 528
18-1-1 The Network Configurator's Device Monitor Function 528
18-2 Using the LED Indicators and Display for Troubleshooting 535
18-2-1 Errors Occurring at the EtherNet/IP Unit or Built-in EtherNet/IP Port 535
18-3 Connection Status Codes and Error Processing 548
18-4 Error Log Function 554
18-4-1 Error Log Data Specifications 554
18-4-2 Error Log Registration 554
18-4-3 FINS Commands for Error Logs 554
18-4-4 Error Log Error Codes 555
18-5 Troubleshooting 559
18-5-1 CPU Unit's ERR/ALM Indicator Lit or Flashing 559
18-5-2 General Ethernet Problems 559
18-5-3 Tag Data Links Fail to Start 560
18-5-4 Tag Data Link Problems 561
18-5-5 Message Timeout Problems 562
18-5-6 FINS Communications Problems (SEND(090)/RECV(098)/CMND(490)) 563
18-5-7 UDP Socket Problems (CS1W/CJ1W-EIP21S or CJ3M-CPU3□ Only) 564
18-5-8 TCP Socket Problems (CS1W/CJ1W-EIP21S or CJ3M-CPU3□ Only) 567
18-5-9 Troubleshooting with Socket Service Response Codes (CS1W/CJ1W-EIP21S or CJ3M-CPU3□ Only) 570
18-6 Troubleshooting with FINS Response Codes 572
18-7 What to Do If Communications Are Not Possible Due to Security Functions 576
18-7-1 Connection with Support Software 576
18-7-2 Communications with External Devices 592
18-7-3 Communications with HMIs 599

18-1 Checking Status with the Network Configurator

18-1-1 The Network Configurator's Device Monitor Function

Connect the Network Configurator online, select the device to be checked, right-click to display the pop-up menu, and select ***Monitor***.



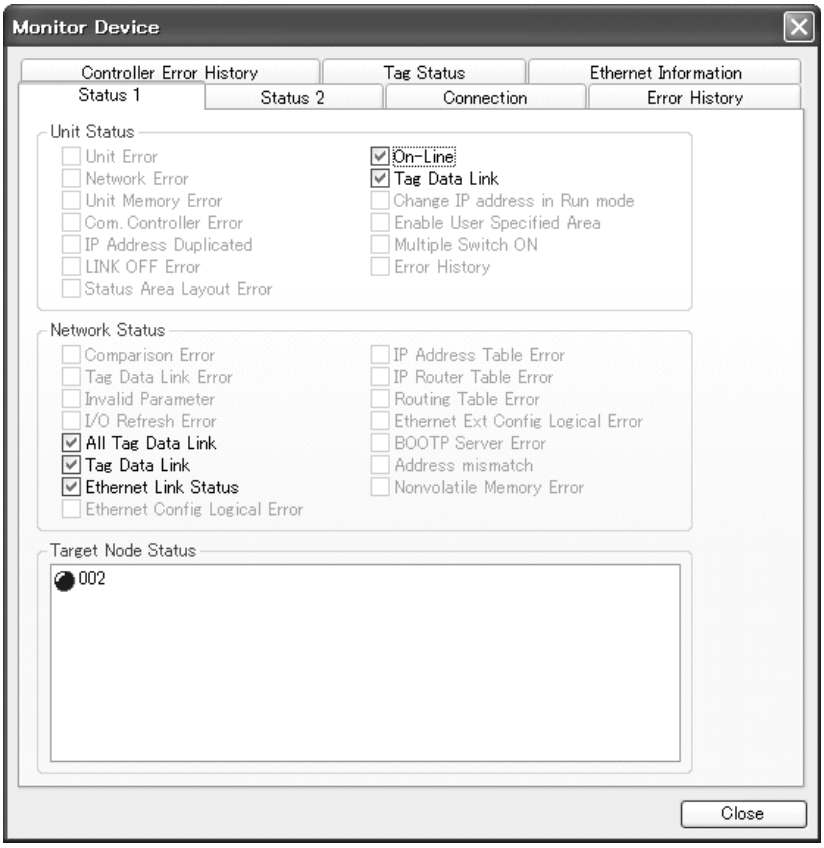
The Monitor Device Dialog Box will be displayed.

Note If a communications error occurs during monitoring, the dialog box will continue to show the last information that was collected. To start monitoring again, close the Monitor Device Dialog Box, and then open the dialog box again.

Status 1 Tab Page

The information displayed on the *Status 1* Tab Page shows the status of the flags in the following allocated CIO Area words: Unit status 1, Unit status 2, Communications status 1, Communications status 2, and Communications status 3. There will be a check mark in the box when the corresponding flag is ON.

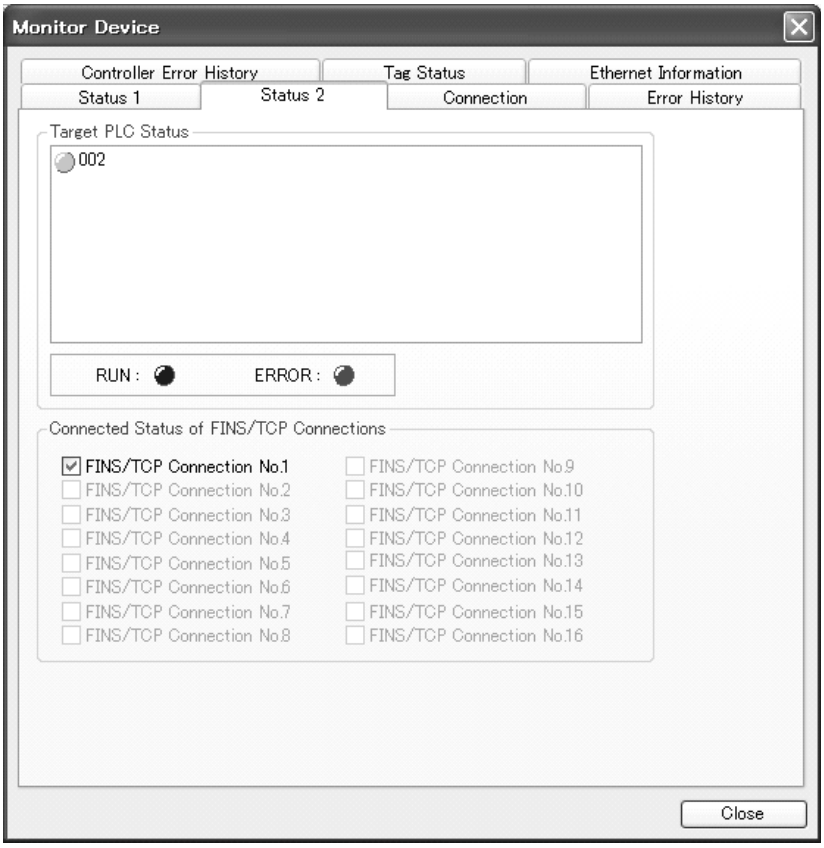
In addition, the *Target Node Status* Field shows the connection status of the target nodes that are connected with the EtherNet/IP Unit as the tag data link originator. The icon will be blue if the connection is normal, or red if an error occurred.



Status 2 Tab Page

The *Status 2* Tab Page's *Target PLC Status* Field shows the status of the target node PLCs that are connected with the EtherNet/IP Unit as the tag data link originator. The icon will be blue if the CPU Unit is in RUN mode or MONITOR mode, gray if it is in PROGRAM mode, or red if an error occurred.

The *Connected Status of FINS/TCP Connections* Field shows the status of FINS/TCP connections. There will be a check mark in the box when the corresponding connection is established (connected).

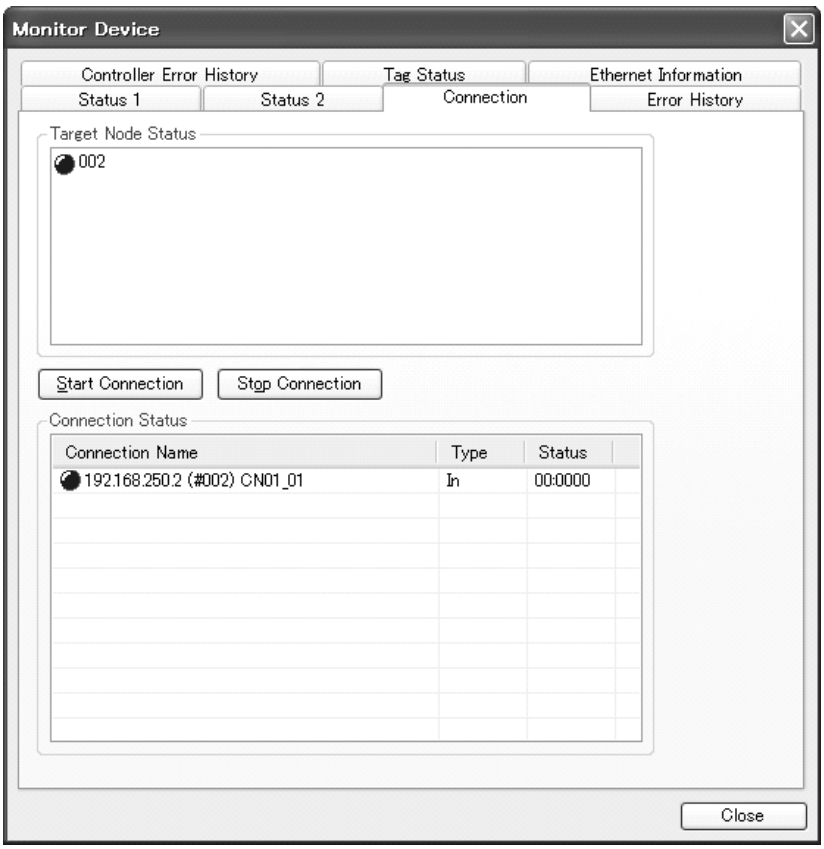


Note The target PLC status can be used when the PLC status is selected for all the target sets for both originator and target connections. For those that are not selected, the status will be grayed-out.

Connection Tab Page

The *Connection* Tab Page's *Target Node Status* Field shows the connection status of the target nodes that are connected with the EtherNet/IP Unit as the tag data link originator. The icon will be blue if the connection is normal, or red if an error occurred.

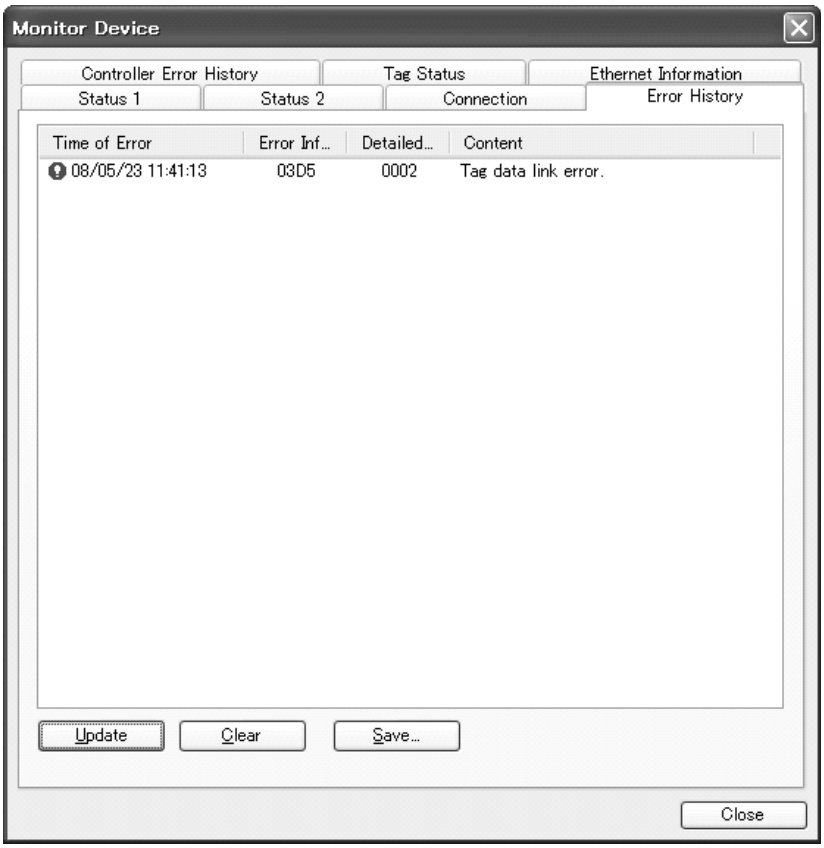
In addition, the *Connection Status* Area shows the current status each connection that is set as the originator. This information can be used to identify the cause of tag data link errors. For details on the connection status, refer to *18-3 Connection Status Codes and Error Processing*.



Error History Tab Page

The *Error History* Tab Page displays the error log stored in the EtherNet/IP Unit or built-in EtherNet/IP port. Errors that occurred in the past are recorded, and can be cleared or saved in a computer file as required.

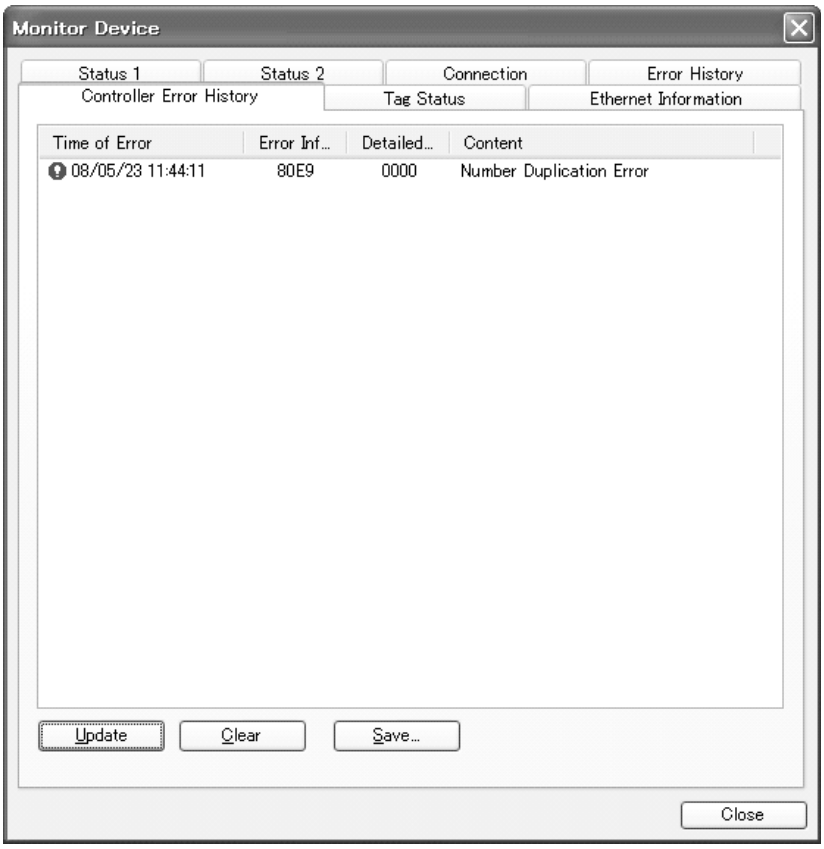
In some cases, error records are cleared when the power is turned OFF, and in other cases the records are retained. For details on the error log, refer to *18-4 Error Log Function*.



Controller Error History Tab Page

The error history of the CPU Unit for the EtherNet/IP Unit or built-in EtherNet/IP port is displayed on this tab page. The error history shows errors that have occurred. It can be cleared or saved in a file in the computer.

Refer to the operation manual of the CPU Unit for details on error information.

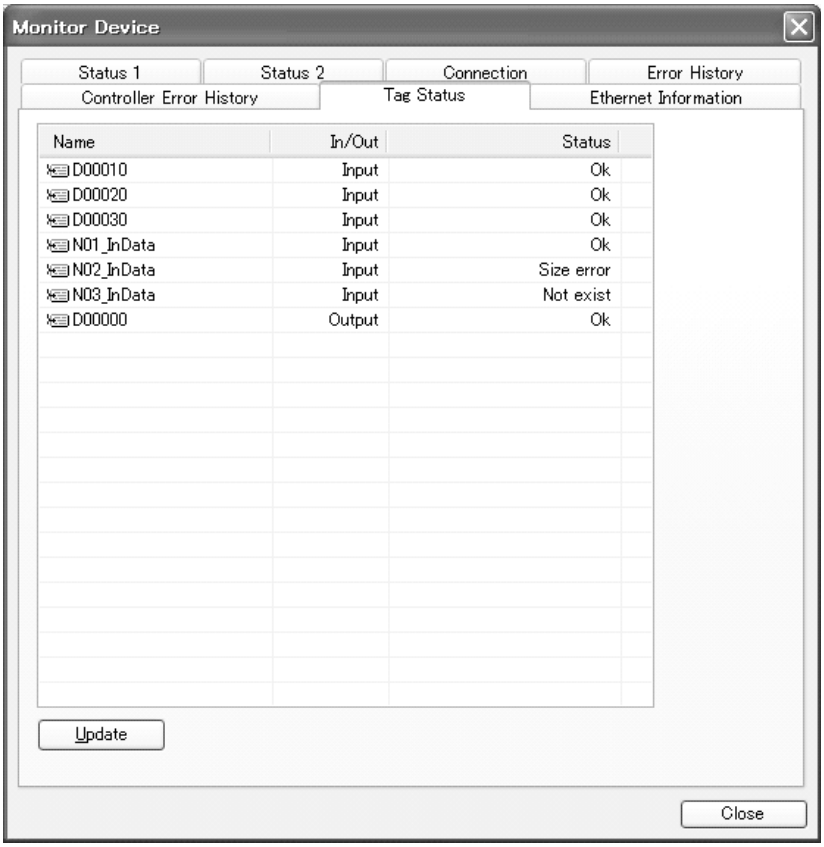


Tag Status Tab Page

This tab page shows if the tag settings for each tag for tag data links is set so that data can be exchanged with the CPU Unit. The following status is displayed.

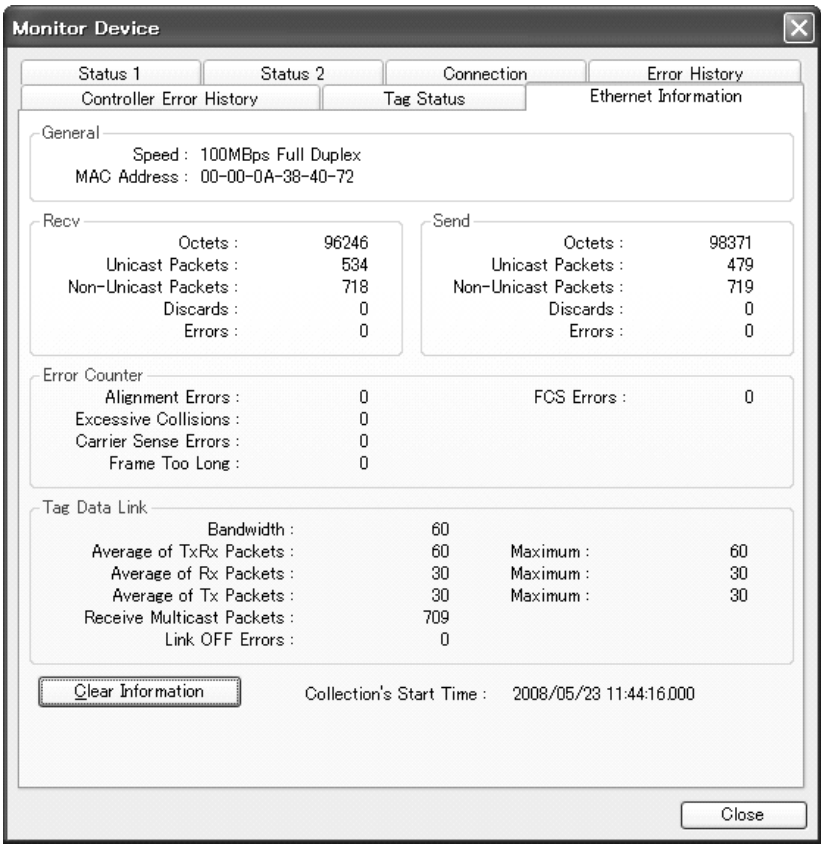
Ok:	Data was exchanged normally.
Processing to solve:	The symbol or I/O memory address for the tag is being resolved. When the resolution is completed normally, a connection will be established and the data exchange will start.
Area type error:	The area (e.g., EM bank) specified by the tag setting does not exist in the CPU Unit. A connection will not be established for a tag for which this error occurs.
Out of address range:	The area specified by the tag setting is outside of the area address range in the CPU Unit. A connection will not be established for a tag for which this error occurs.
Size error:	Different sizes are set for the network symbol and the tag settings. Connections will not be opened for tags with this error.
Not exist:	A network symbol is not set in the symbol table in the CPU Unit for the specified tag setting. A connection will not be established for a tag for which this error occurs.
PLC I/F error:	There is a problem in the bus interface with the CPU Unit. Determine the cause based on the indicators and the error log.

If the status is not “OK,” check the tag data link settings or the network symbol settings in the symbol table in the CJ2/CJ3 CPU Unit.



Ethernet Information Tab Page

The *Ethernet Information* Tab Page shows the communications status at the communications driver level. The error counter information can be used to confirm whether communications problems have occurred. The tag data link information can be used to confirm characteristics such as the bandwidth usage (pps).



18-2 Using the LED Indicators and Display for Troubleshooting

18-2-1 Errors Occurring at the EtherNet/IP Unit or Built-in EtherNet/IP Port

Errors Related to CPU Unit Data Exchange

The 7-segment display alternates between the node address and error code.

Indicator			Error	Cause	Unit operation (Flag status)	Error log (hex)	Countermeasure
MS	NS	7-segment					
Flashing red	Not lit	H1	Duplicate unit number	The same unit number is set on another Unit.	Operation stops.	---	Set the unit numbers correctly and restart the EtherNet/IP Unit or built-in EtherNet/IP port.
Flashing red	Not lit	H2	CPU Unit faulty	---	Operation stops.	---	Replace the CPU Unit if the error recurs when the CPU Unit is restarted.

Indicator			Error	Cause	Unit operation (Flag status)	Error log (hex)	Countermeasure
MS	NS	7-segment					
Lit red	Not lit	H3	EtherNet/IP Unit or built-in EtherNet/IP port faulty	---	Operation stops.	---	Replace the EtherNet/IP Unit or (for a built-in EtherNet/IP port) the CPU Unit if the error recurs when the Unit is restarted.
Flashing red	Not lit	H4	Node address setting error	The node address set on the switches is invalid (00 or FF.)	Operation stops.	---	Set the node address correctly and restart the EtherNet/IP Unit or built-in EtherNet/IP port.
Flashing red	Not lit	H6	CPU Unit faulty	---	Records the error in the error log (time/date all zeroes). Operation stops.	000F	Replace the CPU Unit if the error recurs when the CPU Unit is restarted.
Flashing red	Not lit	H7	I/O table not registered	The CPU Unit's I/O table is not registered.	Operation stops.	0006	Create the I/O table.
Flashing red	---	H8	Simple backup function restore error	The simple backup function's data restoration failed.	The settings of the EtherNet/IP Unit or built-in EtherNet/IP port are all cleared, unless the backup file does not exist, a Memory Card is not mounted, or the PLC model does not match.	---	Perform the simple backup operation again. If the error recurs, replace the Memory Card, or EtherNet/IP Unit, or (for a built-in EtherNet/IP port) the CPU Unit.
Flashing red	---	H9	I/O bus error	An error occurred while exchanging data with the CPU Unit.	• If the Unit is the originator of the tag data link connection, it stops communications. • If the Unit is the target of the tag data link connection and the PLC status is included in the communications data, the corresponding Target Node PLC Error Flag will be turned ON.	000E	Check and correct the CPU Unit's operating environment.

Indicator			Error	Cause	Unit operation (Flag status)	Error log (hex)	Countermeasure
MS	NS	7-segment					
Flashing red	---	HA	CPU Unit memory error	A parity error occurred during an operation such as reading the routing tables.	Records the error in the error log. If the routing tables were being read, the routing tables are treated as missing.	0012	Register the routing tables in the CPU Unit again and restart the CPU Unit. Replace the CPU Unit if the error recurs.
				A memory error has occurred for the tag database in the CPU Unit.	• If a symbol (tag name) is specified in the tag data link or Unit Status Area, refreshing the user-specified status area is stopped and tag data links will operate as follows: • Tag data link communications will be stopped for originator connections. • Communications will continue for target connection. If PLC status is included in the communications data, the target node PLC error flag for the relevant target node will be turned ON. **Note** Recovery is possible from this error. If recovery is achieved, the tag data links will be restarted to return to normal status.	0017	Download the tag data to the CPU Unit again. Replace the CPU Unit if the error recurs.
Flashing red	Not lit	Hb	CPU Unit event servicing timeout	A timeout occurred during an operation such as reading the routing tables to the CPU Unit.	Operation stops.	0011	Replace the EtherNet/IP Unit or (for a built-in EtherNet/IP port) the CPU Unit. if the error recurs when the Unit is restarted.
Flashing red	---	HC	Routing table error	There is a logic error in the routing table settings.	The Unit continues operating without the routing tables.	021A	Create the routing tables again.
Flashing red	---	Hd	I/O refresh error	The EM Area bank in which the device parameters were set was converted to file memory while the tag data link was operating.	Tag data is not refreshed if it is assigned to a non-existent area. Note: Recovery is possible for this error.	0347	Stop using the EM Area bank (in which the device parameters were set) as file memory, or correct the device parameters.

Indicator			Error	Cause	Unit operation (Flag status)	Error log (hex)	Countermeasure
MS	NS	7-segment					
Flashing red	---	HE	CPU Unit service monitoring error	Servicing from the CPU Unit was not completed within the fixed interval. The monitoring time is normally 11 s.	• If the Unit is the originator of the tag data link connection, it stops communications. • If the Unit is the target of the tag data link connection and the PLC status is included in the communications data, the corresponding Target Node PLC Error Flag will be turned ON. Note: Recovery is possible for this error. When operation is restored, tag data link startup processing will be performed and operations will return to normal.	0002	Check and correct the CPU Unit's operating environment.
Flashing red	---	HF	CPU Unit watchdog timer error	An error occurred in the CPU Unit.	• If the Unit is the originator of the tag data link connection, it stops communications. • If the Unit is the target of the tag data link connection and the PLC status is included in the communications data, the corresponding Target Node PLC Error Flag will be turned ON.	0001	Replace the CPU Unit.

Errors Related to the CPU Unit

The 7-segment display alternates between the node address and error code.

Indicator			Error	Cause	Unit operation (Flag status)	Error log (hex)	Countermeasure
MS	NS	7-segment					
Flashing red	---	HH	CPU Unit Fatal Error	A fatal error occurred in the CPU Unit.	• If the Unit is the originator of the tag data link connection, it stops communications. • If the Unit is the target of the tag data link connection and the PLC status is included in the communications data, the corresponding Target Node PLC Error Flag will be turned ON.	0015	Eliminate the cause of the error in the CPU Unit. The tag data link will restart automatically when the cause of the error is eliminated.
---	---	---	Output OFF Error	An Output OFF (output inhibit) condition occurred in the CPU Unit.	The tag data link's send data will be cleared to 0 in accordance with the Output OFF settings, and data transfer will continue with that data.	---	Turn OFF the CPU Unit's Output OFF Bit (A50015). The tag data link's send data will be restored automatically when this bit is turned OFF.

Errors Related to the Control Bits

The 7-segment display alternates between the node address and error code.

Indicator			Error	Cause	Unit operation (Flag status)	Error log (hex)	Countermeasure
MS	NS	7-segment					
---	---	C6	Multiple Switches ON	Two or more software switches were ON simultaneously, or a second software switch was turned ON before a prior operation was completed.	The error code will be displayed on the 7-segment display for 30 seconds, and the Multiple Switches ON Error Flag (n+11, bit 14) will go ON. The error display will be cleared the next time that a settings operation is completed normally.	---	Execute control bit operations one at a time.

Errors Related to the Tag Data Links

The 7-segment display alternates between the node address and error code.

Indicator			Error	Cause	Unit operation (Flag status)	Error log (hex)	Countermeasure
MS	NS	7-segment					
---	---	d5	Verification Error (target non-existent) **Note** This error will not occur if the d5 error (verification error, target nonexistent) mask is enabled.	The target registered in the device parameters does not exist.	The Unit will periodically attempt to reconnect to the target. The Verification Error Flag (n+12, bit 00), Unit Error Occurred Flag (n+10, bit 00), and Network Error Occurred Flag (n+10, bit 01) will go ON.	--- (See note 1.)	Check the following items: • Is the registered node's power supply ON? • Is the cable connected? • Is the cable damaged or loose? • Are CIP message communications stopped at the target node or originator? • Are CIP message communications permitted for packet filtering for the target node and devices in the communications path? • Is there excessive noise?

Indicator			Error	Cause	Unit operation (Flag status)	Error log (hex)	Countermeasure
MS	NS	7-segment					
---	---	d6	Connection Failed	The connection could not be established because device parameters (such as the variable name and size) did not match in the originator and target, or connection resources are insufficient.	The Unit will periodically attempt to reconnect to the target. The Verification Error Flag (n+12, bit 00) and Unit Error Occurred Flag (n+10, bit 00) will go ON.	03D4	Correct the device parameter settings, and download the device parameters again from the Network Configurator.
---	---	d9	Tag Data Link Error	A timeout occurred in the tag data link. (Tag data was not received from the target within the specified timeout time.)	The Unit will periodically attempt to reconnect to the target where the error occurred. The Tag Data Link Error Flag (n+12, bit 02), Unit Error Occurred Flag (n+10, bit 00), and Network Error Occurred Flag (n+10, bit 01) will go ON.	03D5	Check the following items: • Is the registered node's power supply ON? • Is the cable connected? • Is the cable damaged or loose? • Are CIP message communications stopped at the target node? • Are CIP message communications permitted for packet filtering for the originator and devices in the communications path? • Is there excessive noise?

Note (1) For CS1W/CJ1W-EIP21S and EtherNet/IP Units or built-in EtherNet/IP ports with unit version 2.0 or later excluding the CS1W/CJ1W-EIP21S, the error log will not be recorded.

Errors Related to Memory Access

The 7-segment display alternates between the node address and error code.

Indicator			Error	Cause	Unit operation (Flag status)	Error log (hex)	Countermeasure
MS	NS	7-segment					
Flashing red	---	E9	Memory Access Error	An error occurred in the Unit's non-volatile memory itself. This error will occur in the following cases. 1. An error occurred while writing the error log. 2. An error occurred while writing the device parameters. Note: This error does not indicate checksum errors detected when reading data.	Case 1: The error record remains in RAM only. Subsequent writes to non-volatile memory are all ignored. Other than that, normal operation continues. (Error records continue to be written to RAM.) Case 2: Tag data links and message communications will continue operating. The Unit Error Occurred Flag (n+10, bit 00), Unit Memory Error Flag (n+10, bit 04), and Non-volatile Memory Error Flag (n+14, bit 15) will turn ON.	0602	Download the Unit Setup from the tab pages of the Edit Parameters Dialog Box of the CX-Programmer and download the device parameters from the Network Configurator. If the error recurs, replace the EtherNet/IP Unit or (for a built-in EtherNet/IP port) the CPU Unit.

Indicator			Error	Cause	Unit operation (Flag status)	Error log (hex)	Countermeasure
MS	**NS**	**7-segment**					
Flashing red	---	E8	Device Parameters Error	The I/O Area set in the device parameters does not exist in the CPU Unit, or the EM Area was converted to file memory. A checksum error or logic error was detected in the parameters. The Unit was mounted to a different PLC (e.g., from CJ1 to CJ2/CJ3) after the Unit settings were made.	There is an error in the parameter settings stored in the Unit's non-volatile memory. (An error can occur when power is interrupted while data is being written to non-volatile memory.) The Unit Error Occurred Flag (n+10, bit 00) and Invalid Communications Parameter Flag (n+12, bit 04) will go ON.	021A	Download the Unit Setup from the tab pages of the Edit Parameters Dialog Box of the CX-Programmer and download the device parameters from the Network Configurator. If the error recurs, replace the EtherNet/IP Unit or (for a built-in EtherNet/IP port) the CPU Unit. If the ladder program uses the OUT instruction to turn ON the CPU Bus Unit Restart Bit, change the OUT instruction to the SET instruction and download the parameters again.
Flashing red	---	EA	IP Advanced Settings Error			03D1	Identify the error log data, correct the settings, and then download the Unit Setup from the tab pages of the Edit Parameters Dialog Box of the CX-Programmer
Flashing red	---	F2	Basic Ethernet Setting Error			03D0	Download the settings from the TCP/IP or Ethernet Tab Pages of the Edit Parameters Dialog Box of the CX-Programmer or download the TCP/IP settings from the Network Configurator.

Errors Related to the Network

The 7-segment display alternates between the node address and error code.

Indicator			Error	Cause	Unit operation (Flag status)	Error log (hex)	Countermeasure
MS	NS	7-segment					
---	---	E1	Ethernet Link Not Detected	The link with the switching hub could not be detected.*1	• The Unit will be offline and unable to communicate. Errors will be returned to all communications requests. • Data exchanges (refreshing) will continue with the CPU Unit. The Unit Error Occurred Flag (n+10, bit 00), Network Error Occurred Flag (n+10, bit 01), and Link OFF Error Flag (n+10, bit 09) will go ON. The Link Status Flag (n+13, bit 14) will go OFF.	03D3	Check the following items: • Is the cable connected? • Is the cable damaged or loose? • Is there excessive noise?

Indicator			Error	Cause	Unit operation (Flag status)	Error log (hex)	Countermeasure
MS	NS	7-segment					
--- *1	---	E3	Server Connection Error	An error occurred in communications with the DNS server.	The DNS Server Error Flag (n+14, bit 05) will turn ON.	03C4 Details: 00xx	Perform one of the following: • Correct the DNS server settings. • Check the communications path (EtherNet/IP Unit or built-in EtherNet/IP port, cable connections, hubs, routers, and servers) and correct any problems.
				An error occurred with the BOOTP server. 1. There was no response from the BOOTP server. 2. The BOOTP server attempted to set an invalid IP address in the EtherNet/IP Unit or built-in EtherNet/IP port.	Case 1: The Unit will continue sending requests to the BOOTP server until there is a response. In the meantime, the Unit will be offline and unable to communicate. Errors will be returned to all communications requests. Data exchanges (refreshing) will continue with the CPU Unit. Case 2: The Unit will operate with the default IP address (192.168.250.node_address). The Unit Error Occurred Flag (n+10, bit 00), Network Error Occurred Flag (n+10, bit 01), and BOOTP Server Error Flag (n+14, bit 10) will go ON.	03C4 Details: 06xx	Perform one of the following: • Correct the BOOTP server settings. • Check the communications path (EtherNet/IP Unit or built-in EtherNet/IP port, cable connections, hubs, routers, and servers) and correct any problems.
				An error occurred in communications with the STNP server.	The SNTP Server Error Flag (n+14, bit 11) will turn ON.	03C4 Details: 03xx	Perform one of the following: • Correct the SNTP server settings. • Check the communications path (EtherNet/IP Unit or built-in EtherNet/IP port, cable connections, hubs, routers, and servers) and correct any problems.

Indicator			Error	Cause	Unit operation (Flag status)	Error log (hex)	Countermeasure
MS	NS	7-segment					
---	---	E3	Server Connection Error	An error occurred in transmission to the SNMP trap.	---	03C4 Details: 07xx	Perform one of the following: • Correct the SNMP trap settings. • Check the communications path (EtherNet/IP Unit or built-in EtherNet/IP port, cable connections, hubs, routers, and servers) and correct any problems.
---	Lit red	F0	IP Address Duplication	The IP address of the EtherNet/IP Unit or built-in EtherNet/IP port is the same as the IP address set for another node.	• The Unit will be offline and unable to communicate. Errors will be returned to all communications requests. • Data exchanges (refreshing) will continue with the CPU Unit. The Unit Error Occurred Flag (n+10, bit 00), Network Error Occurred Flag (n+10, bit 01), and IP Address Duplication Error Flag (n+10, bit 06) will go ON.	0211	Check the IP addresses set on other nodes. Restart the EtherNet/IP Unit or built-in EtherNet/IP port after correcting the IP address settings to eliminate duplications.
Flashing red	---	F3	Address mismatch	The address conversion method was set for automatic generation, but the host ID of the local IP address does not match the FINS node address. *3	• Operation will continue with the set IP address as the local IP address. The Address Mismatch Flag (n+14, bit 14) will turn ON.	---	Check the IP address and the Node Address Setting Switch setting.

Indicator			Error	Cause	Unit operation (Flag status)	Error log (hex)	Countermeasure
MS	NS	7-segment					
Flashing red	Not lit	F4	Communications Controller Error	An error occurred in the Communications Controller in the EtherNet/IP Unit or built-in EtherNet/IP port.	• The Unit will be offline and unable to communicate. Errors will be returned to all communications requests. • Data exchanges (refreshing) will continue with the CPU Unit. The Unit Error Occurred Flag (n+10, bit 00), Network Error Occurred Flag (n+10, bit 01), and Communications Controller Error Flag (n+10, bit 05) will go ON.	020F	Replace the EtherNet/IP Unit or (for the built-in EtherNet/IP port) the CPU Unit if the error recurs when the Unit is restarted.
Flashing red	---	C8	Node Address Setting Changed During Operation	The Node Address Setting Switch was changed during operation.	Operation will continue. The IP Address Changed During Operation Flag (n+11, bit 02) will turn ON.	---	Restart the EtherNet/IP Unit or built-in EtherNet/IP port after setting the correct node address.
Flashing red	---	EC	User Authentication Setting Error	The user authentication setting could not be saved to the Unit's non-volatile memory.	The Unit will operate with the default user authentication setting. However, the error status will not be cleared.	03D6	Use the EIP21S User Management Tool to reset the user authentication setting, transfer the setting, and then restart the Unit.

*1 This error does not occur when tag data links are not set for EtherNet/IP Unit (built-in port) version 2.0 and later excluding CS1W/CJ1W-EIP21S, CJ3M-CPU3□ and CS1W/CJ1W-EIP21S or CJ3M-CPU3□.

*2 With CS1W/CJ1W-EIP21S, this flashes in green.

*3 When the CS1W/CJ1W-EIP21S or CJ3M-CPU3□ is used, this error does not occur when the FINS/UDP service is set not to be used.

Errors Related to the Unit The 7-segment display alternates between the node address and error code.

Indicator			Error	Cause	Unit operation (Flag status)	Error log (hex)	Countermeasure
MS	NS	7-segment					
Lit red	Not lit	---	Special Unit Error	An error occurred in a Special I/O Unit or CPU Bus Unit.	Records the error in the error log. Operation stops.	0601	Restart the CPU Unit. Replace the EtherNet/IP Unit or (for the built-in EtherNet/IP port) the CPU Unit if the error recurs.

18-3 Connection Status Codes and Error Processing

This section explains how to identify and correct errors based on the tag data link's connection status. The connection status can be read using the *Connection* Tab Page of the Network Configurator's Monitor Device Window. For details, refer to *18-1-1 The Network Configurator's Device Monitor Function*.

Note

1. The connection status has the same meaning as the Connection Manager's General and Additional error response codes, as defined in the CIP specifications.
2. The Open DeviceNet Vendor Association, Inc. (ODVA) can be contacted at the following address to obtain a copy of the CIP specifications.

   ODVA, Inc.
   4220 Varsity Drive, Suite A
   Ann Arbor, Michigan 48108-5006
   USA

   TEL: 1 734-975-8840

   Email odva@odva.org

   WEB www.odva.org

The following table shows the possible originator/target configurations.

Configuration	Originator	Target
Configuration 1	CS1W-EIP21/EIP21S, CJ1W-EIP21/EIP21S, CJ2H-CPU□□-EIP, CJ2M-CPU3□, CJ3M-CPU3□	CS1W-EIP21/EIP21S, CJ1W-EIP21/EIP21S, CJ2H-CPU□□-EIP, CJ2M-CPU3□, CJ3M-CPU3□
Configuration 2	CS1W-EIP21/EIP21S, CJ1W-EIP21/EIP21S, CJ2H-CPU□□-EIP, CJ2M-CPU3□, CJ3M-CPU3□	Other company's device
Configuration 3	Other company's device	CS1W-EIP21/EIP21S, CJ1W-EIP21/EIP21S, CJ2H-CPU□□-EIP, CJ2M-CPU3□, CJ3M-CPU3□

The following table shows the likely causes of the errors causes for each configuration and connection status (code).

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
00	0000	Normal status code: The connection has been opened and the tag data link is communicating normally.	---	---	---
01	0100	Error code returned from target: Attempted to open multiple connections at the same connection.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer for details on preventing the error from occurring in the future.)	Depends on the originator's specifications. (Contact the originator device's manufacturer for details on preventing the error from occurring in the future.)
01	0103	Error code returned from target: Attempted to open a connection with an unsupported transport class.	This error does not occur.	Confirm that the target supports Class 1.	Confirm that the originator supports Class 1.

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
01	0106	Duplicate consumers: Attempted to open multiple connections for single-consumer data.	If the tag data link is stopped or started, this error may occur according to the timing, but the system will recover automatically.	Depends on the target's specifications. (Contact the target device's manufacturer.)	If the tag data link is stopped or started, this error may occur according to the timing, but the system will recover automatically.
01	0107	Error code returned from target: Attempted to close a connection, but that connection was already closed.	This error does not occur.	This error does not occur.	This is not an error because the connection is already closed.
01	0108	Error code returned from target: Attempted to open a connection with an unsupported connection type.	This error does not occur.	Check which connection types can be used by the target. (Contact the manufacturer.) Only multicast and point-to-point can be set.	Check which connection types can be used by the originator. (An error will occur if a connection other than multicast or point-to-point is set.)
01	0109	Error code returned from target: The connection size settings are different in the originator and target.	Check the connection sizes set in the originator and target.		
01	0110	Error code returned from target: The target was unable to open the connection, because of its operating status, such as downloading settings.	Check whether the tag data link is stopped at the target. (Restart the tag data link communications with the control bit.)	Depends on the target's specifications. (Contact the target device's manufacturer.)	Check whether the tag data link is stopped at the originator. (Restart the tag data link communications with the control bit.)
01	0111	Error code returned from target: The RPI was set to a value that exceeds the specifications.	This error does not occur.	Check the target's RPI setting specifications.	Set the originator's RPI setting to 10 seconds or less.
01	0112	Error code generated by originator or returned from target: A packet interval (RPI) that cannot be set has been requested.	Check the connection settings (RPI) at the originator and target.	Check the connection settings (RPI) at the originator and target. Check the connection specifications for another company's devices.	Check the connection settings (RPI) at the originator and target. Check the connection specifications for another company's devices.
01	0113	Error code generated by originator or returned from target: Attempted to open more connections than allowed by the specifications (CJ2M-EIP21: 32, other CPU Units: 256).	Check the connection settings (number of connections) at the originator and target.	Check the connection settings (number of connections) at the originator and target. Check the connection specifications for another company's devices.	Check the connection settings (number of connections) at the originator and target. Check the connection specifications for another company's devices.

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
01	0114	Error code returned from target: The Vendor ID and Product Code did not match when opening connection.	If the target device has been changed, download the connection settings of the new target device to the originator.	Depends on the target's specifications. (Contact the target device's manufacturer.) Confirm that the target device's EDS file is correct.	Check the originator's connection settings.
01	0115	Error code returned from target: The Product Type did not match when opening connection.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.) Confirm that the target device's EDS file is correct.	Check the originator's connection settings.
01	0116	Error code returned from target: The Major/Minor Revisions did not match when opening connection.	Check the major and minor revisions set for the target device and connection. If necessary, obtain the EDS file and set it again.	Depends on the target's specifications. (Contact the target device's manufacturer.) Confirm that the target device's EDS file is correct.	Check the originator's connection settings.
01	0117	Error code returned from target: The tag set specified in the connection's target variables does not exist.	Check whether the originator and target tag sets and tags are set correctly. CJ2/CJ3 CPU Units Only: Check symbol settings in the CPU Unit.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Check the originator's connection settings. Check whether the target's tag sets and tags are set correctly. CJ2/CJ3 CPU Units Only: Check symbol settings in the CPU Unit.
01	011A	Error code returned from originator: Connection could not be established because the buffer was full due to high traffic.	An unexpected network load may have been received. Use the Network Configurator Device Monitor or the Ethernet Tab Page to check the bandwidth usage, and correct the load. If there are places where broadcast storms occur, such as loop connections in the network connection format, then correct them.	An unexpected network load may have been received. Use the Network Configurator Device Monitor or the Ethernet Tab Page to check the bandwidth usage, and correct the load. If there are places where broadcast storms occur, such as loop connections in the network connection format, then correct them.	Follow the operating specifications for the originator. (Consult the originator manufacturer.)
01	011B	Error code returned from target: The RPI was set to a value that is below the specifications.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Set the originator's RPI setting to 0.5 ms or greater.

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
01	0127	Error code returned from target: The connection data size differs between the settings of the originator and target. (Data in direction of originator → target)	This error does not occur.	Check the connection settings (size) of the originator and target. (Data in direction of originator → target) If the issue is not resolved, contact the manufacturer of the target because this is dependent on the operation specifications of the target.	This error does not occur.
01	0128	Error code returned from target: The connection data size differs between the settings of the originator and target. (Data in direction of target → originator)	Check the connection settings (size) of the originator and target. (Data in direction of target → originator)		
01	0136	Error code returned from target: Opening a connection with a priority setting that differs from opened multicast connection was requested. (Data in direction of target → originator)	This error does not occur.	To match the multicast communication from another company's originator, check the priority specified by that originator.	This error does not occur.
01	0203	Error code returned from target: The connection timed out.	Tag data link communications from the target timed out. Check the power supply and cable wiring of the devices in the communications path, including the target and switches. If performance has dropped due to heavy load, change the performance settings. For example, increase the timeout time or RPI setting.		
01	0204	Error code returned from target: The connection-opening process timed out.	There was no response from the target. • Check the power supply and cable wiring of the devices in the communications path, including the target and switches. • Check that the CIP message server function is permitted for the registered node. • Check that CIP communications are permitted by packet filtering for the originator and devices in the communications path.		
01	0205	Error code returned from target: There was a parameter error in the frame used to open the connection.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Depends on the originator's specifications. (Contact the originator device's manufacturer.)
01	0302	Error occurred at originator or error code returned from target: The tag data link's allowable bandwidth (pps) was exceeded.	Check the originator and target connection settings (number of connections and RPI).	Check the target's connection settings (number of connections and RPI).	Check the originator and target connection settings (number of connections and RPI).
01	0311	Error code returned from target: There was a parameter error in the frame used to open the connection.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Depends on the originator's specifications. (Contact the originator device's manufacturer.)
01	0312	Error code returned from target: There was a parameter error in the frame used to open the connection.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Depends on the originator's specifications. (Contact the originator device's manufacturer.)

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
01	0315	Error code returned from target: There was a parameter error in the frame used to open the connection.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Depends on the originator's specifications. (Contact the originator device's manufacturer.)
01	0316	Error code returned from target: There was a parameter error in the frame used to close the connection.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Depends on the originator's specifications. (Contact the originator device's manufacturer.)
01	031C	Error code generated in originator: Some other error occurred.	This error does not occur.	The originator generates this code when an unsupported response code is returned from the target in reply to a connection-opening request.	Depends on the originator's specifications. (Contact the originator device's manufacturer.)
08	---	Error code returned from target: There is no Forward Open or Large Forward Open service in the target device.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Depends on the originator's specifications. (Contact the originator device's manufacturer.)
D0	0001	Error code generated in originator: The connection operation is stopped.	The connection was stopped because the Tag Data Link Stop Bit was turned ON, or the settings data is being downloaded. Either turn ON the Tag Data Link Start Bit, or wait until the settings data has been downloaded. Includes Controller stop errors, Unit failure, and EM bank files at the refresh destination. To handle these errors, refer to *18-2-1 Errors Occurring at the EtherNet/IP Unit or Built-in EtherNet/IP Port*.	The meaning of this error code is defined by each vendor, so it depends on the target's specifications. (Contact the target device's manufacturer.)	Depends on the originator's specifications. (Contact the originator device's manufacturer.)
D0	0002	Error code generated in originator: The connection is being opened (opening processing in progress).	Wait until the opening processing is completed.	The meaning of this error code is defined by each vendor, so it depends on the target's specifications. (Contact the target device's manufacturer.)	Depends on the originator's specifications. (Contact the originator device's manufacturer.)

Connection status		Source of error	Handling		
General Status (hex)	**Additional Status (hex)**		**Configuration 1**	**Configuration 2**	**Configuration 3**
Unique OMRON Error Codes					
01	0810	Error code returned from target: New data could not be obtained from the CPU Unit when opening connection. (The Unit will automatically retry, and attempt to open the connection again.)	This error may occur if the CPU Unit's cycle time was long when opening the connection, the specified EM bank was converted to file memory, or some problem in the PLC caused the PLC to stop. If the cycle time was too long, the problem will be resolved automatically. If the EM bank is set as file memory, change the storage location for the tag data. If the PLC has stopped, identify and correct the error. If the PLC system is stopped, identify the cause of the error from the CPU Unit error data.	The meaning of this error code is defined by each vendor, so it depends on the target's specifications. (Contact the target device's manufacturer.)	The meaning of this error code is defined by each vendor, so it depends on the originator's specifications. (Contact the originator device's manufacturer.)
01	0811	Error code generated in originator: New data could not be obtained from the CPU Unit when opening connection. (The Unit will automatically retry, and attempt to open the connection again.)	This error may occur if the CPU Unit's cycle time was long when opening the connection, or the specified EM bank was converted to file memory. If the cycle time was too long, the problem will be resolved automatically. If the EM bank is set as file memory, change the storage location for the tag data.	The meaning of this error code is defined by each vendor, so it depends on the target's specifications. (Contact the target device's manufacturer.)	The meaning of this error code is defined by each vendor, so it depends on the originator's specifications. (Contact the originator device's manufacturer.)

18-4 Error Log Function

Errors detected by the EtherNet/IP Unit or built-in EtherNet/IP port are stored in the error log along with the date and time of their occurrence. The error log can be read and cleared from the Network Configurator.

Some error log records are cleared when the CPU Unit's power goes OFF, and other records are not cleared.

18-4-1 Error Log Data Specifications

Each error is recorded as one record in the error log.

Item	Specifications
Record length	10 bytes/record
Number of records	64 records max.
Data type	Binary (time information: BCD)

Structure of Each Record

Bit 15	Bit 00
Error code	
Detail code	
Minutes	Seconds
Day of month	Hour
Year	Month

18-4-2 Error Log Registration

Error Log Storage Area

When an error occurs, information on the error and the time stamp are stored in the Unit's internal RAM as an error log record. Serious errors are recorded in non-volatile memory as well as RAM. The time read from the CPU Unit during cyclic servicing is used for the time stamp.

The error log records stored in non-volatile memory are copied to RAM when the Unit starts operating, so these records are retained even when the Unit's power is turned OFF or the Unit is restarted.

When the error log is read, the error log records in RAM are read. When the error log is cleared, the error log records in both RAM and non-volatile memory are erased.

Error Log Overflows

The error log can record up to 64 records. If another error occurs when the log is full, the oldest record will be erased to make room for the new error record.

Power Interruptions when Saving to Non-volatile Memory

If the power supply is interrupted or the Unit is restarted while the error log is being written to non-volatile memory, the error log may be corrupted. When the Unit starts, it performs a checksum test on the error log data read from non-volatile memory to detect corrupted data.

18-4-3 FINS Commands for Error Logs

The following FINS commands can be sent to the EtherNet/IP Unit or built-in EtherNet/IP port to read or clear the error log.

Command code		Function name
MRC	SRC	
21	02	ERROR LOG READ
	03	ERROR LOG CLEAR

For details, refer to *Appendix E FINS Commands Addressed to EtherNet/IP Units or Built-in EtherNet/IP Ports*.

18-4-4 Error Log Error Codes

Error code (hex)	Error	Detail code		Saved in EEPROM
		First byte	Second byte	
0001	CPU Unit watchdog timer error	00 hex	00 hex	Yes
0002	CPU Unit service monitoring error	Monitoring time (ms)		Yes
0006	Other CPU error	Bit D11: Unit not in Registered I/O Tables (Other bits are reserved for system use.)		Yes
000E	I/O bus error	00 hex	00 hex	Yes
000F	CPU Unit initialization error	00 hex	00 hex	Yes
0011	Event timed out	MRC (main command)	SRC (subcommand)	Yes
0012	CPU Unit memory error	01 hex: Read error 02 hex: Write error	03 hex: Routing tables 50 hex: CPU Bus Unit Area (CIO or DM)	Yes
0015	CPU Unit fatal error	00 hex	00 hex	Yes
0017	Tag database error	00 hex	00 hex	Yes
0103	Resend count exceeded (send failed)	FINS Command: Bit 15: OFF Bits 08 to 14: Source network address Bits 00 to 07: Source node address FINS Response: Bit 15: ON Bits 08 to 14: Destination network address Bits 00 to 07: Destination node address CIP Frame: FFFF		No
0105	Node address setting error (send failed)			No
0107	Remote node not in network (send failed)			No
0108	No Unit with specified unit address (send failed)			No
010B	CPU Unit error (send failed)			No
010D	Destination address not in routing tables (send failed)			No
010E	Not registered in routing tables (send failed)			No
010F	Routing table error (send failed)			No
0110	Too many relay points (send failed)			No
0111	Command too long (send failed)			No
0112	Header error (send failed)			No
0117	Internal buffers full; packet discarded			No
0118	Illegal packet discarded			No
0119	Local node busy (send failed)			No
0120	Unexpected routing error			No
0122	Service not supported in current mode; packet discarded			No
0123	Internal send buffer full; packet discarded			No
0124	Maximum frame size exceeded; routing failed			No
0125	Response timeout; packet discarded			No
020F	Communications controller error	00 hex	01 hex	Yes
0211	IP address duplication	Port number (always 02)	Lower byte of IP address	Yes
021A	Logic error in setting table	00 hex	02 hex: Network parameters 03 hex: Routing tables 04 hex: Unit Setup 0E hex: Unit name 12 hex: Status area layout setting error 13 hex: Status area layout setting verification error 15 hex: Installation in a PLC of another series (e.g., from CJ1 to CJ2/CJ3) after setting the Unit.	Yes

Error code (hex)	Error	Detail code		Saved in EEPROM
		First byte	Second byte	
0300	Parameter error; packet discarded	FINS Command: Bit 15: OFF Bits 08 to 14: Source network address Bits 00 to 07: Source node address FINS Response: Bit 15: ON Bits 08 to 14: Destination network address Bits 00 to 07: Destination node address CIP Frame: FFFF		No
0347	I/O refreshing error	00 hex	00 hex	Yes
03C0	FINS/TCP setting error	01 to 10 hex: Connection number	01: Automatically allocated FINS node address duplication 02: Destination IP address error 03: Destination port number error	No
03C1	Server settings error	00 hex: DNS 03 hex: SNTP 04 hex: FTP 06 hex: BOOTP 07 hex: SNMP 08 hex: SNMP Trap 09 hex: FINS/UDP 0A hex: FINS/TCP	01: IP address 02: Host name 03: Port number 04: Other parameter	No
03C2	FINS/TCP packet discarded	01 to 10 hex: Connection number	02 hex: Reopening because remote node closed 03 hex: Reopening because of reception error 04 hex: Reopening because of transmission error 05 hex: Reopening because RST received from remote node 06 hex: Reopening because of no keep-alive response 07 hex: Illegal FINS/TCP procedure 08 hex: Insufficient memory during server processing 09 hex: Insufficient memory during client processing 0A hex: Insufficient memory during node switching	No
03C3	FINS/UDP packet discarded	00 hex	01 to FE hex: Source node address	No

Error code (hex)	Error	Detail code		Saved in EEPROM
		First byte	Second byte	
03C4	Server connection error	00 hex: DNS 03 hex: SNTP 04 hex: FTP 06 hex: BOOTP 07 hex: SNMP 08 hex: SNMP Trap	01 hex: Specified host does not exist 02 hex: No such service at specified host 03 hex: Timeout 06 hex: Host name resolution error 07 hex: Transmission error 08 hex: Reception error 09 hex: Other error 0A hex: Obtaining IP address error	No
03C6	Clock write error	0001: The clock time could not be updated because a error occurred in the CPU Unit.	Clear the error from the CPU Unit.	No
		0002: The clock time could not be updated because the CPU Unit or operating mode does not support this function.	Refer to *SECTION 12 Automatic Clock Adjustment Function* and check the application conditions.	
03D0	Basic Ethernet setting error	01 hex: Ethernet setting error	01 hex: Checksum error 11 hex: Inconsistent settings 12 hex: Specified baud rate is not supported.	Yes
		02 hex: TCP/IP basic setting error	01 hex: Checksum error 11 hex: Invalid IP address 12 hex: Invalid subnet mask 13 hex: Invalid default gateway address 14 hex: Invalid primary name server 15 hex: Invalid secondary name server 16 hex: Invalid domain name 17 hex: Invalid host name	

Error code (hex)	Error	Detail code		Saved in EEPROM
		First byte	Second byte	
03D1	Ethernet advanced setting error	02 hex: FINS setting error	01 hex: Checksum error 10 hex: Invalid IP router table 11 hex: Invalid FINS/UDP setting 12 hex: Invalid FINS/TCP setting 13 hex: Invalid FTP setting 14 hex: Invalid SNTP setting 15 hex: Invalid SNMP setting 16 hex: Invalid SNMP trap setting 17 hex: Invalid packet filter setting	Yes
03D2	Packet discarded.	01 hex	00 hex	No
03D3	Link OFF error	00 hex	00 hex	No
03D4	Verification error (Tag data link only) **Note** For details on identifying the cause of the verification error, refer to *18-3 Connection Status Codes and Error Processing*. This error log is recorded for CS1W/CJ1W-EIP21 and CJ2H-CPU6□-EIP version 1.0 only.	00 hex	Lower byte of IP address	No
03D5	Tag data link error	00 hex	Lower byte of IP address	No
03D6	User authentication setting error	00 hex	00 hex	Yes
0601	CPU Bus Unit error	Variable		Yes
0602	CPU Bus Unit memory error	01: Read error 02: Write error	02 hex: Network parameter 06 hex: Error log 09 hex: Identity data 0E hex: Unit name 0F hex: Ethernet basic setting 10 hex: Ethernet advanced setting 11 hex: MAC address 12 hex: Status area layout setting 14 hex: Term Tag address resolution memory write error	Yes (See note.)

Note If a memory error occurs in the error log area of EEPROM, the record will not be stored in EEPROM.

18-5 Troubleshooting

18-5-1 CPU Unit's ERR/ALM Indicator Lit or Flashing

Use the following table to troubleshoot the system when the CPU Unit's ERR/ALM indicator is lit or flashing when the EtherNet/IP Unit or built-in EtherNet/IP port is mounted.

An I/O verification error occurred.	• Confirm that the Unit is connected properly. • Check the I/O table with the I/O Table Verification operation and correct it if necessary. After correcting it, perform the I/O Table Create operation.
A CPU Bus Unit setting error occurred.	• The CPU Bus Unit model registered in the I/O tables does not match the model of CPU Bus Unit actually mounted. Check the I/O tables with the I/O Table Verification operation and correct it if necessary. After correcting the I/O tables, perform the I/O Table Create operation.
A CPU Bus Unit error occurred.	• Confirm that the Unit is connected properly. • Restart the Unit. Replace the Unit if it doesn't restart.
An I/O Bus error occurred.	• Confirm that the Unit is connected properly. • Restart the Unit. Replace the Unit if it doesn't restart.

For details, refer to the CPU Unit's Operation Manual.

18-5-2 General Ethernet Problems

The 100M and 10M Indicators on the EtherNet/IP Unit or CPU Unit are both OFF.	• Confirm that the cable being used has the correct ratings. • Confirm that the cable is properly connected to the switching hub, and the hub's power supply is ON. (The 7-segment display will indicate error E1.) • If the switching hub's settings can be changed, confirm that the Ethernet link settings are the same as the settings for the EtherNet/IP Unit or built-in EtherNet/IP port. (For details, refer to *3-4 Network Installation*.)
The NS Indicator on the EtherNet/IP Unit or CPU Unit is lit red.	• Check whether the same IP address is set on another node. (The 7-segment display will indicate error F0.)

18-5-3 Tag Data Links Fail to Start

Use the following table to troubleshoot tag data links when the Tag Data Links Operating Flag (bit 15 in Communications Status 1) does not go ON.

The indicators on the EtherNet/IP Unit or CPU Unit are all OFF.	• Check whether power is being supplied to the PLC. • Check whether the EtherNet/IP Unit or built-in EtherNet/IP port is mounted in the Backplane correctly. • If a watchdog timer (WDT) error has occurred in the PLC, follow the procedures described in the PLC's Operation Manual to correct the problem. • All of the indicators for the EtherNet/IP Unit or built-in EtherNet/IP port will be OFF if a CPU Bus Unit error has occurred. Check for a CPU Bus Unit error. • Restart the Unit. Replace the Unit if it doesn't restart.
The MS indicator on the EtherNet/IP Unit or CPU Unit is lit green, but the NS indicator remains OFF.	• If the EtherNet/IP Unit's 7-segment display is displaying an error code, refer to the tables in *18-2 Using the LED Indicators and Display for Troubleshooting*. • Confirm that the cables are properly connected to the switching hub and the power supply to the switching hub is ON. • If data is being restored by the simple backup function, wait until the restore operation is completed.
The MS indicator on the EtherNet/IP Unit or CPU Unit is lit green, but the NS indicator continues to flash green.	• If the EtherNet/IP Unit's 7-segment display is displaying an error code, refer to the tables in *18-2 Using the LED Indicators and Display for Troubleshooting*. • The NS indicator will continue to flash green if the tag data link settings have not been set in the Unit. Use the Network Configurator to set the tag data link settings in the Unit, and then restart the Unit.
The MS indicators is lit green on the EtherNet/IP Unit or CPU Unit, but the NS indicator continues to flash red.	• Identify the error code shown on the 7-segment display based on the tables in *18-2 Using the LED Indicators and Display for Troubleshooting*, and eliminate the cause of the error.

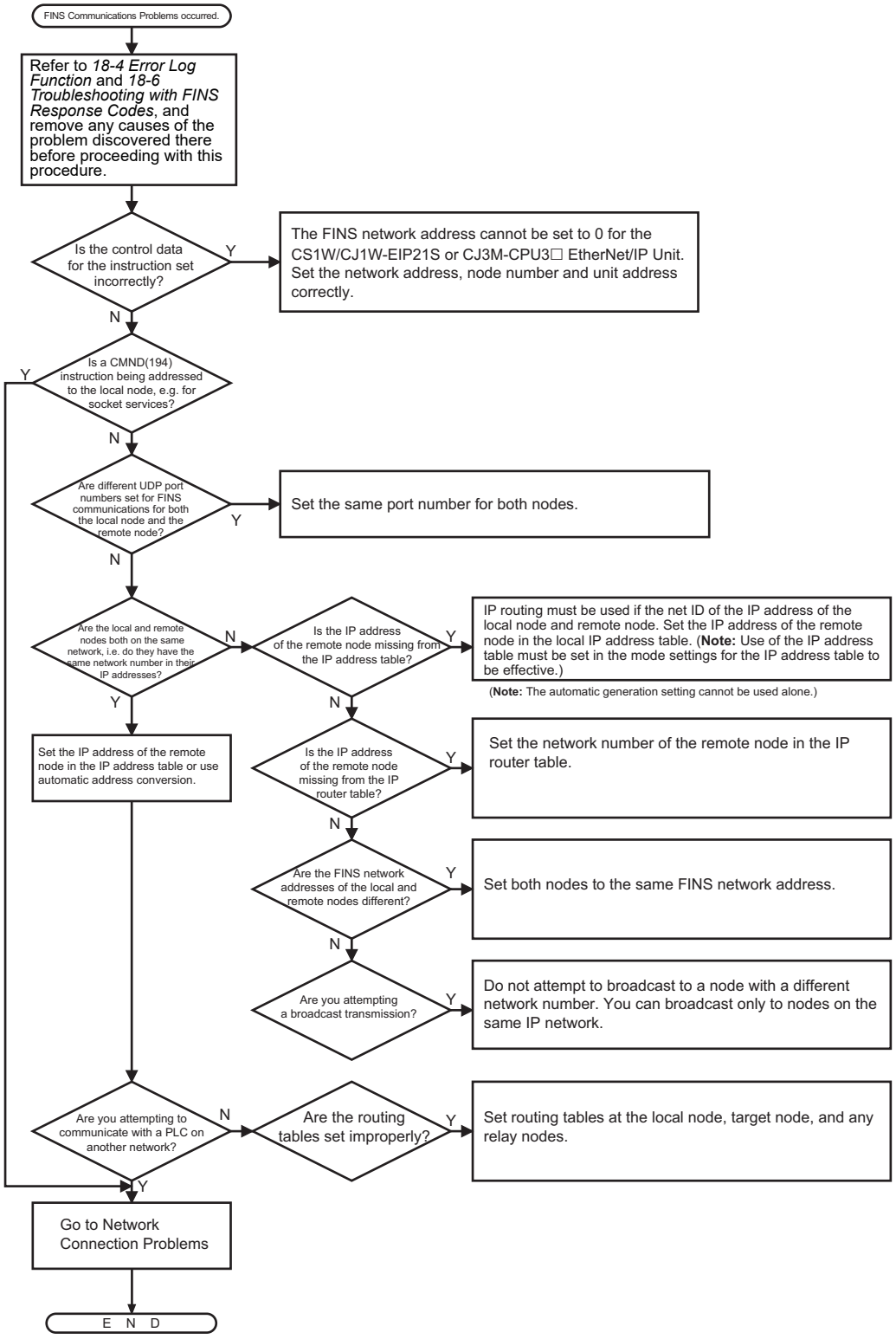
18-5-4 Tag Data Link Problems

The tag data isn't simultaneous.	Observe the following precautions when writing application programs: • Maintain the simultaneity of data in connection-units between the PLC and EtherNet/IP Unit or built-in EtherNet/IP port. • If another company's device is being used, refer to that device's user's manual for details.
At startup, the received data is OFF unexpectedly.	• When received data is used in the ladder program, use the All Tag Data Links Operating Flag in Communications Status 1, or the Target Node PLC Operating Flag as a condition. If the Target Node PLC Operating Flag is used, the PLC status must be included in tag sets of both the sending and receiving nodes. • If the Output OFF function (Output Inhibit) is enabled in the output (produce) tag settings, all of the output data will be OFF if a fatal error occurs in the CPU Unit or the Output OFF Bit is turned ON. Check the status of the output (producer) PLC.
The tag data links start and stop communicating intermittently.	• Check whether the baud rate is set to 10 Mbps, or a 10M or 100M repeater hub is being used. The tag data link performance is based on the use of switching hubs. The bandwidth listed in the specifications (CJ2M-EIP21: 3,000 pps, other CPU Units: 12,000 pps) is achieved when the Unit auto-negotiates to full-duplex at 100 Mbps. • Refer to *18-1 Checking Status with the Network Configurator* for details on checking the error counters on the Monitor Device Window's *Ethernet Information* Tab Page. The error and discarded packet counters indicate problems such as noise in the communications path, the use of substandard cables, damaged cables/connectors, loose connectors, abnormally high communications load, or incorrect wiring (loops) in the switching hub wiring. • Contact the switching hub manufacturer to determine whether there are any problems with the transfer capacity of the switching hubs in the communications path. If switching hubs are arranged in a cascade connection, there may be a heavy load concentrated at a mid-level switching hub. In the EtherNet/IP Unit or built-in EtherNet/IP port itself, processing is performed with a higher priority than message communications, so specifications provide for a 3,000 pps bandwidth for the CJ2M-EIP21 and a 12,000 pps bandwidth for other CPU Units in tag data link performance only. • Refer to *18-1 Checking Status with the Network Configurator* for details on checking the connection status on the Monitor Device Window's *Connection* Tab Page. Eliminate any errors, which can be identified in the tables in *18-3 Connection Status Codes and Error Processing*.

18-5-5 Message Timeout Problems

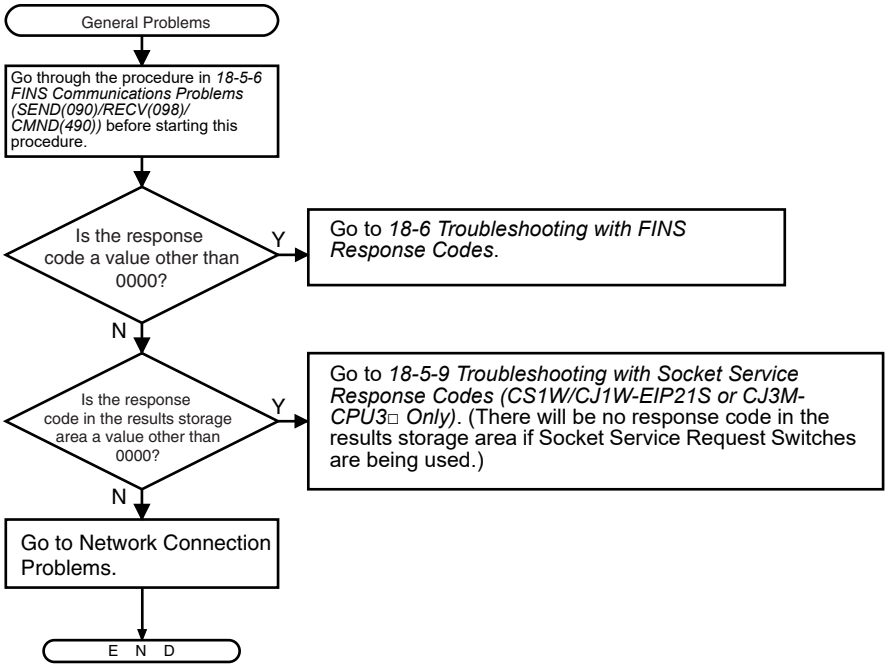
Timeout errors occur frequently in message services (CIP UCMM, CIP Class 3, or FINS).	• When there is a high load in the tag data link, and the CPU Unit's cycle time is relatively long or there are messages coming in from many nodes, the message service response time may be delayed and messages may be discarded occasionally. • In this case, the communications load must be reduced by increasing (slowing) the tag data link's RPI, reducing the message load, or increasing the timeout value. • The tag data link's bandwidth usage can be checked on the Monitor Device Window's *Ethernet Information* Tab Page. Refer to *18-1 Checking Status with the Network Configurator* for details. • The error log error codes that indicate discarded messages (insufficient memory) due to heavy communications loads are 0117, 0119, 0123, 0125, 03C2 (detail code □□08, □□09, or □□0A), 03C3, and 03D2. Refer to *18-1 Checking Status with the Network Configurator* for details on reading the error codes on the *Error History* Tab Page. • For information on preventing high loads in FINS communications, refer to *8-7 Precautions on High Traffic in FINS Communications*.

18-5-6 FINS Communications Problems (SEND(090)/RECV(098)/ CMND(490))



18-5-7 UDP Socket Problems (CS1W/CJ1W-EIP21S or CJ3M-CPU3□ Only)

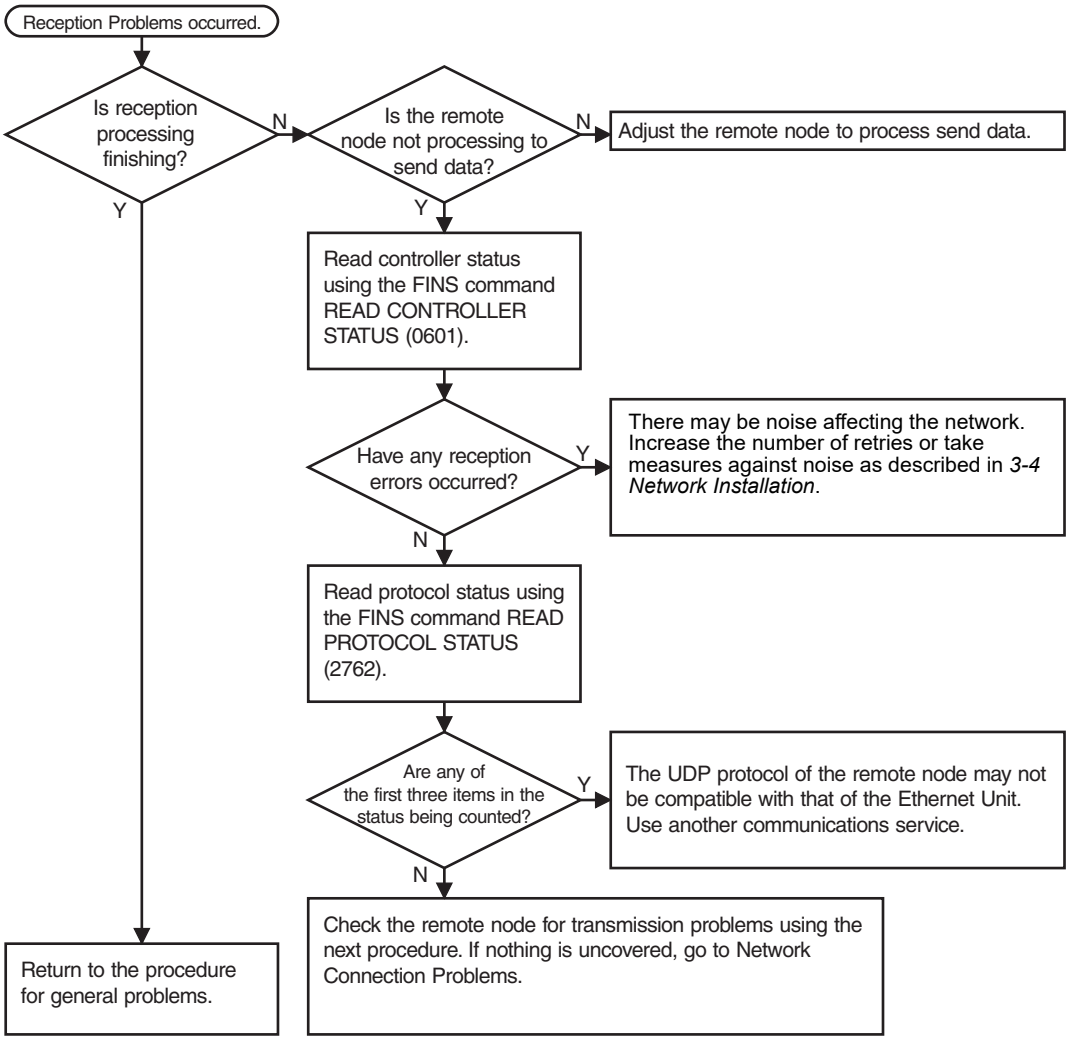
General Problems



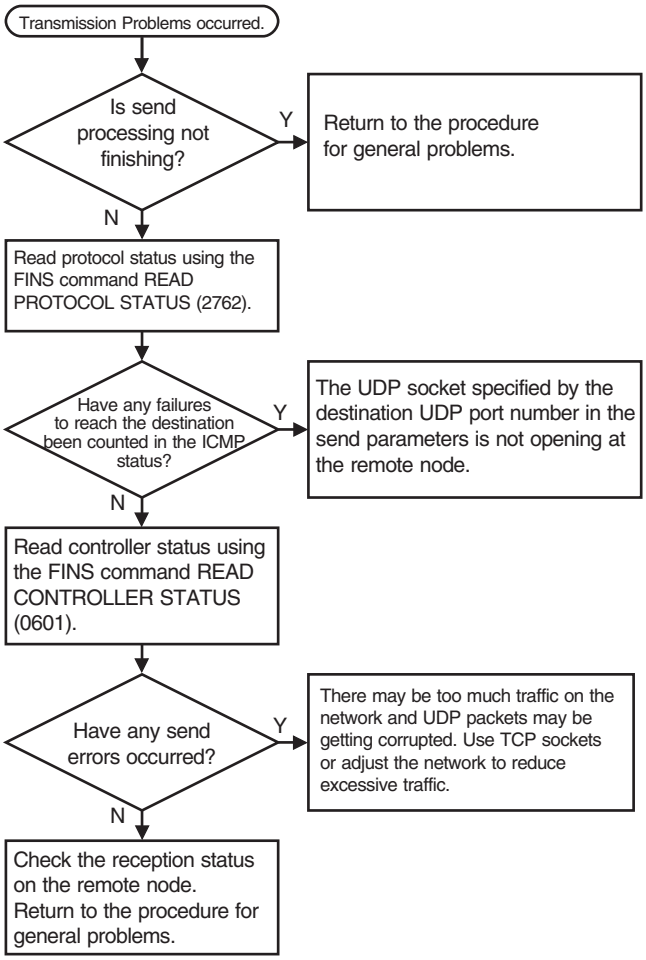
Opening and Closing Problems

Refer to *General Problems* above.

Reception Problems

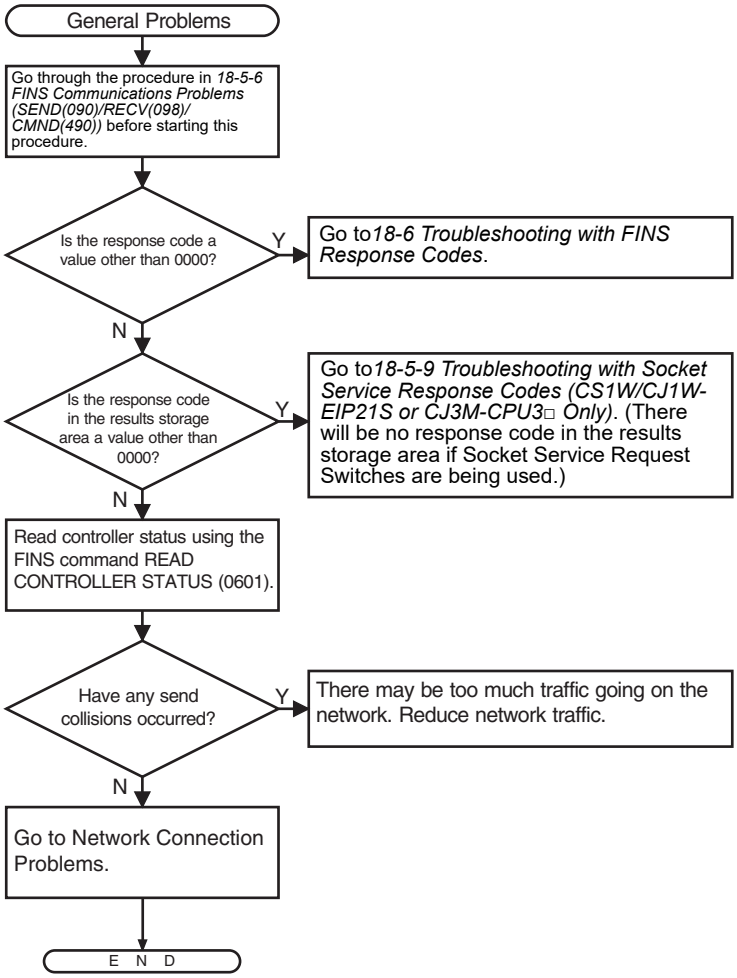


Transmission Problems

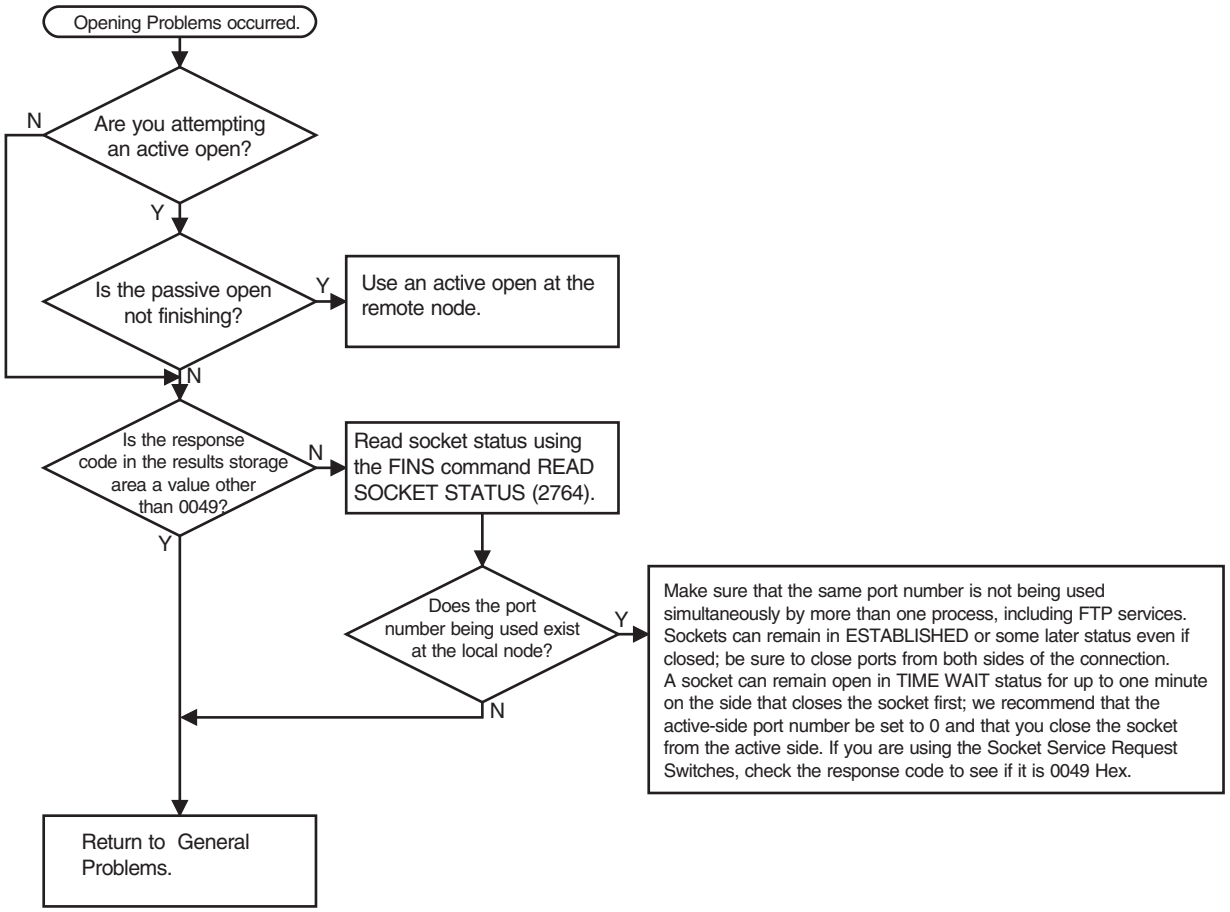


18-5-8 TCP Socket Problems (CS1W/CJ1W-EIP21S or CJ3M-CPU3□ Only)

General Problems



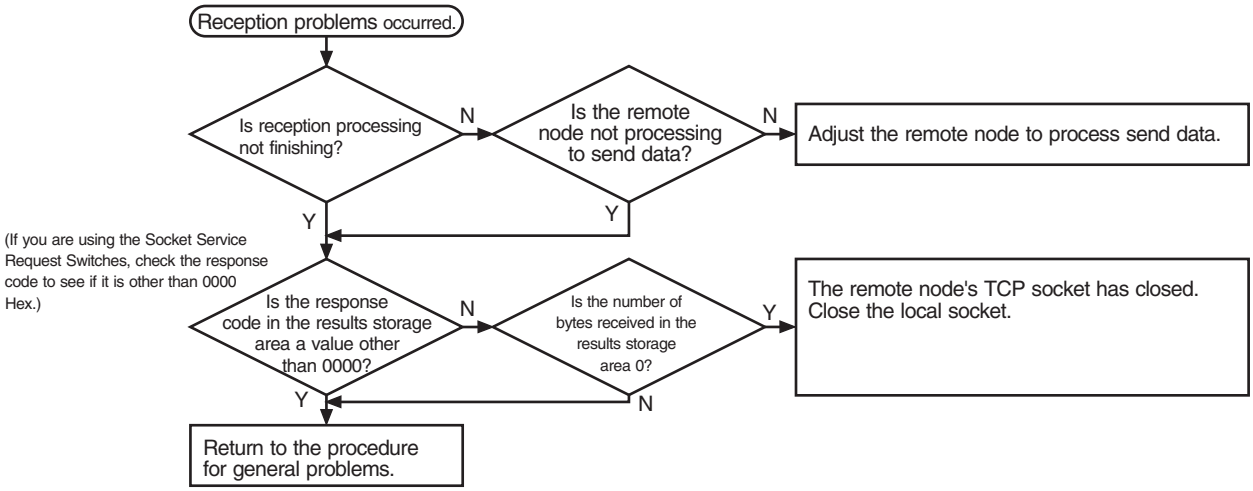
Opening Problems



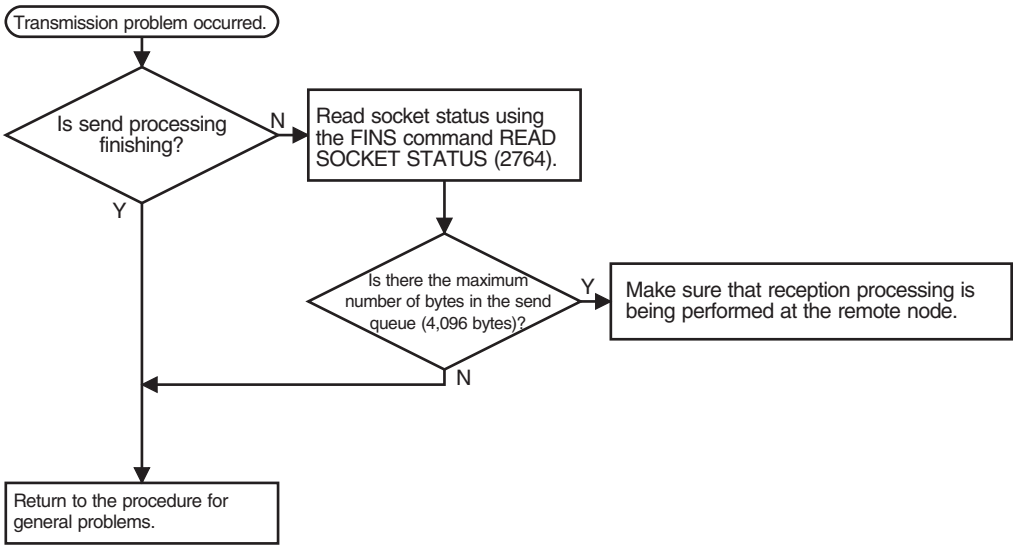
Closing Problems

Refer to *General Problems* on page 567.

Reception Problems



Transmission Problems



18-5-9 Troubleshooting with Socket Service Response Codes (CS1W/CJ1W-EIP21S or CJ3M-CPU3□ Only)

The response codes stored in the Results Storage Area can be used to troubleshoot socket service problems. Refer to *Socket Service Parameter Area 1 to 8 (EtherNet/IP Unit to CPU Unit)* on page 116 in *4-3-2 Details of the Allocated DM Area Words* for the location of the response codes stored in the Results Storage Area.

The UNIX socket service error messages corresponding to the response codes are given in the following table. Refer to the documentation for the devices involved when communicating between a CS1W/CJ1W-EIP21S or CJ3M-CPU3□ and other devices.

Response code	UNIX error message	Description	Probable remedy
0003	ESRCH	No such process	Close the local socket and try reopening it.
0006	ENXIO	No such device or address	
0009	EBADF	Bad file number (incorrect socket specification)	
000D	EACCES	Permission denied (Broadcast address specified for remote IP address for active TCP open)	Check the IP address of the remote node and try to reconnect.
000E	EFAULT	Bad address (copy failed between kernel and user area)	Close the local socket and try reopening it.
0011	EEXIST	File exists	
0016	EINVAL	Invalid argument (socket library argument error)	
0018	EMFILE	Too many open files (More than 32 sockets)	
0020	EPIPE	Broken pipe (remote node closed socket)	Close the local socket.
003C	EPROTONO-SUPPORT	Protocol not supported (protocol other than UDP, TCP, or RAW specified)	Close the local socket and try reopening it.
003D	EPROTOTYPE	Protocol wrong type for socket	
003E	ENOBUFS	No buffer space available	There is too much load (traffic) on the CS1W/CJ1W-EIP21S EtherNet/IP Unit. Check your user applications.
003F	EISCONN	Socket is already connected (connection attempted to open socket)	Close the local socket and try reopening it.
0040	ENOTCONN	Socket is not connected (send attempted to closed socket)	
0041	EALREADY	Operation already in progress (connection attempted to existing non-block connection)	
0042	EMSGSIZE	Message too long	Check the length of send data. UDP or TCP: 1 to 1,982 bytes UDP broadcasts: 1 to 1,472 bytes

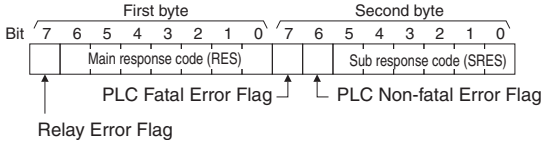
Response code	UNIX error message	Description	Probable remedy
0043	EDESTADDRREQ	Destination address required (destination address not specified)	Close the local socket and try reopening it.
0044	ENOPROTOOPT	Protocol not available (unsupported option specified)	
0045	ECONNABORTED	Software caused connection abort (another task closed socket)	
0046	EINPROGRESS	Operation now in progress (non-block connection ended during processing)	
0047	ENOTSOCK	Socket operation on non-socket	
0048	EOPNOTSUPP	Operation not supported on socket	
0049	EADDRINUSE	Address already in use (UDP or TCP open request sent for port already in use)	Check the port number. TCP ports can remain unusable for 1 min after closing.
004A	ECONNREFUSED	Connection refused (TCP socket (active open) processing refused by remote node)	Passively open a remote TCP socket, checking the remote IP address and remote TCP port number.
004B	ECONNRESET	Connection reset by peer (TCP socket closed by remote node)	Close the local socket and try reconnecting.
004C	EADDRNOTAVAIL	Can't assign requested address (mistake in remote IP address)	Check the setting of the remote IP address and try reconnecting.
004D	EAFNOSUPPORT	Address family not supported by protocol family	Close the local socket and try reopening it.
004E	ENETUNREACH	Network is unreachable	Set the path to the remote node in the IP router table.
004F	EHOSTDOWN	Host is down	Check the remote host and communications path.
0050	EWOULDBLOCK	Operation would block	Close the local socket and try reopening it.
0051	EHOSTUNREACH	No route to host	The specified node does not exist on the designated IP network segment. Check the communications path.
0053	ETIMEDOUT	Connection timed out (TCP timed out)	• Check the remote host and communications path. • Check that communications are permitted by IP packet filtering for the local or remote node.
0063	ESELABORT	Used for internal processing of CS1W/CJ1W-EIP21S EtherNet/IP Unit	Close the local socket and try reopening it.
0066	(None)	Internal memory cannot be allocated for processing; the service cannot be provided.	Traffic is too high at the CS1W/CJ1W-EIP21S EtherNet/IP Unit. Correct the user application to reduce traffic at the Ethernet Unit.
0080	(None)	Timed out for passive TCP open request	• Either the remote node is not executing an active TCP open or there is a block on the network. • Check that communications are permitted by IP packet filtering for the local or remote node.
0081	(None)	Closed by close command during socket servicing	No action is necessarily called for.
0082	(None)	Connection with remote node not achieved for passive TCP open request	The remote IP address and TCP port number settings differ from those of the remote socket (active side).

18-6 Troubleshooting with FINS Response Codes

The cause of errors that occur when using the SEND(090), RECV(098), or CMND(490) instructions can be identified from the response codes. (Refer to the description of *Communications Port Completion Codes* in *8-6-4 Writing Programs* for the storage locations of response codes generated by the SEND, RECV, or CMND instructions.)

This section describes the completion codes produced by EtherNet/IP Units. For details on completion codes produced by CPU Units, other CPU Bus Units, or computers equipped with FINS services, refer to the device's operation manual.

The 6th, 7th, and 15th bits of the response codes have specific functions. The 6th bit will be ON when a non-fatal error has occurred in the PLC at the remote node; the 7th bit will be ON when a fatal error has occurred in the PLC at the remote node; and the 15th bit will be ON when a network relay error has occurred. The following table explains the meaning of the completion codes.



Main response code		Sub response code		Item to check	Likely cause	Corrective action
Value and meaning		Value and meaning				
00	Normal completion	00	---	---	---	---
01	Local node error	03	Local node send error	---	Lack of available space in internal buffers	The load (traffic) on the Ethernet Unit is too heavy. Check your user applications.
		05	Node address setting error	Local IP address	The network cannot be used because the IP address setting is incorrect.	Correct the local IP address.
		07	Local node busy (send failed)	System load	Lack of available space in internal buffers	The load (traffic) on the Ethernet Unit is too heavy. Check your user applications.

Main response code		Sub response code		Item to check	Likely cause	Corrective action
Value and meaning		Value and meaning				
02	Remote node error	01	Remote node not in network	IP address table and IP router table	IP address of remote node not set correctly.	Set IP address of remote node into IP address table and, if internetwork transmission is required, into the IP router table.
		02	No Unit with specified unit address	Instruction's control data	There is no Unit with the specified unit address.	Check the remote node's unit address.
		05	Response timeout	Transfer conditions (Use FINS status read commands.)	Message packet was corrupted by transmission error.	Increase the number of transmit retry attempts.
				Instruction's control data	The response monitoring time is too short.	Set a longer response monitoring time.
				Read the error log.	The transmission frame may be corrupted or the internal reception buffer full.	Read out the error log and correct the system as required.
				Remote node's FINS settings	FINS is disabled in the FINS settings for the remote node.	Check that FINS is enabled in the FINS settings for the remote node.
				Remote node's packet filter settings	FINS is not permitted in the packet filter settings for the remote node.	Check that FINS is permitted in the packet filter settings for the remote node.
03	Unit error (Controller error)	01	Communications controller error	Affected controller's ERC indicator	Error occurred in the communications controller.	Take corrective action, referring to troubleshooting procedures in this section.
		02	PLC error	Affected node's LED indicators	CPU Unit error occurred in the PLC at the remote node.	Clear the error in the CPU Unit. (Refer to the PLC's operation manuals.)
		04	Unit number setting error	Unit number	The unit number setting is incorrect.	Confirm that the unit number set on the switch is within the specified range and that the same unit number is not used twice in the same network.
04	Service not supported	01	Unsupported command	Command code	The specified command code is not supported by the destination Unit.	Check the command code.
				FINS header frame length	A short frame (4 bytes) is being used for the FINS header frame.	The EtherNet/IP Unit does not support short headers.
05	Routing error	01	Routing table setting error	Routing tables	Remote node is not set in the routing tables.	Set the destination address in the routing tables.
		02	Routing tables not registered	Routing tables	Destination is unknown because there are no routing tables.	Set routing tables at the local node, remote node, and any relay nodes.
		03	Routing table error	Routing tables	Routing table error	Set the routing tables correctly.
		04	Too many relay points	Network configuration	The maximum number of network levels (3) was exceeded in the command.	Redesign the network, or reconsider the routing tables to reduce the number of relay nodes in the command.

Main response code		Sub response code		Item to check	Likely cause	Corrective action
Value and meaning		Value and meaning				
10	Command format error	01	Command too long	Command data	The command is too long.	Check the command format of the command and set it correctly.
					The command exceeded 1,473 bytes when broadcasting.	
		02	Command too short	Command data	The command is too short.	
		03	Number of items does not match amount of data	Command data	The specified number of items does not match the amount of write data.	Check the number of items and amount of data, and make them agree.
		05	Header parameter error	Command data	Data for another node on the same network was received from the network.	Check the command format of the command and set it correctly.
					Attempted to send response data for a broadcast address.	
11	Parameter error	00	Parameter error	Parameters in command data	The specified parameters are incorrect.	Check the command data and set the parameters correctly.
					The UDP/TCP socket number was not within the proper range.	Be sure the socket number is between 1 and 8.
					The local UDP port number might be set to 0.	Set the local UDP port number correctly.
		01	No data area code	Variable type in command data	A correct memory area code has not been used or EM Area is not available.	Check the command's data area code in the Results Storage Area and set the appropriate code.
		03	Address out-of-range error	First word address in command data	The first word is in an inaccessible area.	Check the data area range, and set a first word that is in an accessible area.
					The specified bit number is not 00.	Check the command's data area code in the Results Storage Area. The bit address must be 00 for EtherNet/IP Units.
		04	Address range overflow	Command data	The address range specified in the command is not correct.	Set the address in the command data so that the start address plus the number of words does not exceed accessible memory.
		0B	Response too long	Command data	The response frame is longer than allowed.	Correct the number of data elements or other parameters in the command data for which the response is being returned.
		0C	Parameter error	Parameters in command data	The specified parameters are incorrect.	Check the command data and set the parameters correctly.
21	Cannot write	08	Cannot change	IP address conversion method	A FINS message was received from an IP address that differed from the ones in the Unit Setup with FINS node addresses that could not be dynamically changed.	Correct the relationships between IP addresses and FINS node addresses. Refer to *SECTION 5 Determining IP Addresses* for details.

Main response code		Sub response code		Item to check	Likely cause	Corrective action
Value and meaning		Value and meaning				
22	Status error (operating mode disagreement)	0F	Cannot execute because service is being processed.	Socket status area	The same socket service is already in progress at the specified socket number.	Use the corresponding socket status flag in PLC memory to be sure that socket service has finished before starting services again.
		10	Socket not open	Socket status area	The specified socket is not open.	Open the socket. (For TCP sockets, wait until the connection is made.)
		11	Local node busy (send failed)	System load	Lack of available space in internal buffers	The load (traffic) on the Ethernet Unit is too heavy. Check your user applications.
		20	FINS/TCP not connected	Unit Setup	Not opened due to system settings.	Correctly set the Unit Setup, FINS/TCP connection number, remote IP address, and remote port number.
		21			Not opened due to a change command from the FINS/TCP connection's remote node.	
		22			Closed by remote node; opening again.	
		23			Opening again because of a reception error.	
		24			Opening again because of a send error.	
		25			Opening again because of an RST response in keep-alive.	
		26			Opening again because there was no response in keep-alive.	
		30	Establishing connection	Command data	A connection is already established with the specified remote node.	Correct the settings for the FINS/TCP connection number, the remote IP address, and the remote port number.
		31	Cannot change connection	Unit Setup and command data	The specified connection number is not set as a FINS/TCP client in the Unit Setup.	Correct the settings for the Unit Setup, the FINS/TCP connection number, the remote IP address, and the remote port number.
		32	Cannot execute because service was interrupted	Command data	While a remote node change was being processed for the specified connection number, a request for a change was received and the processing was stopped.	Correct the settings for the FINS/TCP connection number, the remote IP address, and the remote port number.
23	No such Unit (Environment error)	05	Parameters	Unit Setup	IP address conversion failed.	Check the IP address and subnet mask in the Unit Setup, and correct if necessary.
		07	Configuration error	IP address conversion in Unit Setup	IP address conversion is set for automatic conversion only.	Check the IP address conversion setting in the Unit Setup. This error will be generated for the IP ADDRESS TABLE READ command only.

18-7 What to Do If Communications Are Not Possible Due to Security Functions

CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ EtherNet/IP Units provide security functions that are intended to prevent unauthorized access from outside.

This may prevent Support Software or external devices to communicate with the CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ if the security settings are insufficient or incorrect.

This section describes what you should do if a CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ EtherNet/IP Unit cannot communicate with Support Software or external devices due to the security settings on a use case basis.

Note that the description here applies to the case where CS1W/CJ1W-EIP21S EtherNet/IP Units exist in an Ethernet network.

The following abbreviations are used for terms used in tables in this section.

Term	Abbreviation
CX-Programmer	CX-P
CS/CJ-series CPU Unit	CS/CJ CPU
CS1W/CJ1W-EIP21S or CJ3M-CPU3☐ EtherNet/IP Unit	EIP21S
NA-series Programmable Terminal	NA
NB-series Programmable Terminal	NB
NS-series Programmable Terminal	NS

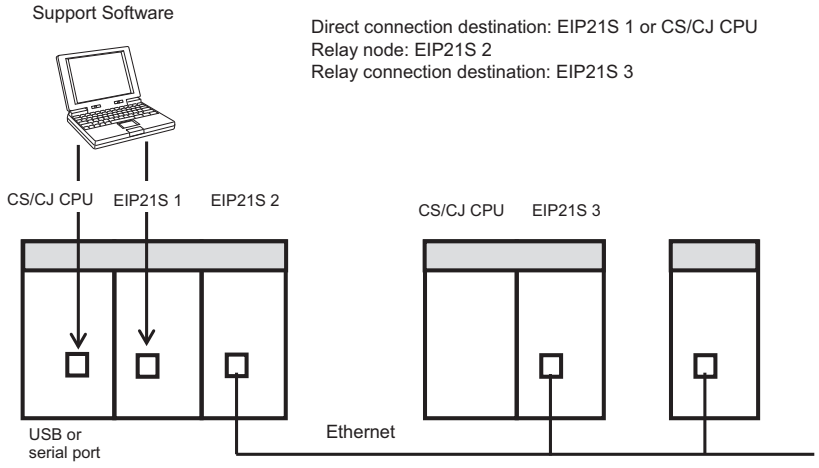
18-7-1 Connection with Support Software

This section describes what you should do if an error occurs in connection with Support Software.

A description is provided for each network type that you select when connecting Support Software to an Ethernet network.

Definition of Connection Formats

The description for each network type is further divided by connection format, i.e., direct connection destination, relay node, and relay connection destination. The meaning of each connection format is defined as follows.



Secure Comm

The connection format in this case is direct connection destination only.

Target built-in EtherNet/IP Unit

Built-in EtherNet/IP Unit
CS1W-EIP21S, CJ1W-EIP21S, CJ3M-CPU3□

CPU Units that support EtherNet/IP Unit or built-in EtherNet/IP port

CPU Unit	Model
CJ3 CPU Unit	CJ3M-CPU□□
CJ2 CPU Unit (See note.)	CJ2H-CPU6□(-EIP), CJ2M-CPU□□
CJ1G-P CPU Unit	CJ1G-CPU4□P
CS1H-H CPU Unit	CS1G/CS1H-CPU□□H
CS1D CPU Unit	CS1D-CPU□□H/HA, CS1DCPU□□SA/S, CS1D-CPU□□P
CP1H CPU Unit	CP1H-X□40D□-□, CP1H-Y20DT-D

Note The built-in EtherNet/IP port of the CJ2H-CPU6□-EIP/CJ2M-CPU3□ does not support connections using secure communications.

Target Support Software

The target Support Software is shown as below.

Support Software	Version	
	CS1W-EIP21S CJ1W-EIP21S	**CJ3M-CPU3□**
CX-Programmer	Ver. 9.81 or higher	Ver. 9.90 or higher
PLC Backup Tool	Ver. 1.03 or higher	Ver. 1.06 or higher
EIP21S User Management Tool (See note.)	Ver. 1.0 or higher	Ver. 1.01 or higher

Note If the OS of your PC is earlier than Windows 10, you cannot either install the EIP21S User Management Tool or select Secure Comm in the CX-Programmer and the PLC Backup Tool.
If the Windows 10 version is earlier than 1803, you cannot either go online by Secure Comm or use the function derived from Secure Comm.
In this section, the above supported Support Software is mentioned by name without version information.

■ **Secure Comm**

Direct connection destination

Operation	Support Software status	Setting error description	What to do
Connecting online	Timeout display	The computer's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the computer's IP address setting is incorrect Change the computer's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted and set the source IP address to permit the computer's IP address. The following is an example of the settings. Source IP address: Computer's IP address Protocol filter: Disabled
		TCP/443 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted and set the protocol filter to permit TCP/443. The following is an example of the settings. Source IP address: Any Protocol: TCP Source port: Not specified Destination port: 443
Entering values that are different from the user name and password settings for the EIP21S in the User Authentication Dialog Box	User authentication error	---	Enter the correct user name and password that are set for the EIP21S. If the user name and password are unknown, ask the administrator to add an account or reset the password.
Entering an expired password in the User Authentication Dialog Box	User authentication error	---	Use the EIP21S User Management Tool to change the password.

Other Than Secure Comm - Case 1

Target Support Software

The target Support Software is shown as below.

- CX-Programmer
- SwitchBox
- PLC Backup Tool
- CX-Protocol
- CX-Motion
- CX-Motion-MCH
- CX-Motion-NCF
- CX-Position
- CX-FLnet
- CX-Integrator
- CX-Net

■ **EtherNet/IP**

The connection format in this case is direct connection destination only.

Direct connection destination

Operation	Support Software status	Setting error description	What to do
Connecting online	Timeout display	*Use CIP message server* is not set in the CIP message server setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use the CIP message server.
		The computer's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the computer's IP address setting is incorrect Change the computer's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted and set the source IP address to permit the computer's IP address. The following is an example of the settings. Source IP address: Computer's IP address Protocol filter: Disabled
		Any of the following is not permitted for the protocol filter in the IP Packet Filter Setting. • TCP/44818 • ICMP	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit TCP/44818 and ICMP. The following is an example of the settings. Source IP address, Protocol, Source port, Destination port TCP: Any, TCP, Not specified, 44818 ICMP: Any, ICMP, Not specified, Not specified

■ **USB**

The connection format available in this case is relay connection destination only.

Relay connection destination

Operation	Support Software status	Setting error description	What to do
Connecting online	Timeout display	*Use CIP message server* is not set in the CIP message server setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use the CIP message server.
		The relay unit's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the relay unit's IP address setting is incorrect Change the relay unit's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the source IP address to permit the relay unit's IP address. The following is an example of the settings. Source IP address: Relay unit's IP address Protocol filter: Disabled
		TCP/44818 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit TCP/44818. The following is an example of the settings. Source IP address: Any Protocol: TCP Source port: Not specified Destination port: 44818

■ **NJ-Thru (USB Port)**

The connection format available in this case is relay connection destination only.

Relay connection destination

Operation	Support Software status	Setting error description	What to do
Connecting online	Timeout display	*Not use FINS/UDP service* is set in the FINS/UDP setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use FINS/UDP service.
		The relay unit's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the relay unit's IP address setting is incorrect Change the relay unit's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the source IP address to permit the relay unit's IP address. The following is an example of the settings. Source IP address: Relay unit's IP address Protocol filter: Disabled
		UDP/9600 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit UDP/9600. The following is an example of the settings. Source IP address: Any Protocol: UDP Source port: Not specified Destination port: 9600 (See note 1.)

Note (1) If you enter a port number value that is not the default, the value will be set.

■ **Ethernet or FinsGateway (When Using FINS/UDP)**

Direct connection destination

Operation	Support Software status	Setting error description	What to do
Connecting online	Timeout display	*Not use FINS/UDP service* is set in the FINS/UDP setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use FINS/UDP service.
		The computer's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the computer's IP address setting is incorrect Change the computer's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted and set the source IP address to permit the computer's IP address. The following is an example of the settings. Source IP address: Computer's IP address Protocol filter: Disabled
		UDP/9600 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit UDP/9600. The following is an example of the settings. Source IP address: Any Protocol: UDP Source port: Not specified Destination port: 9600 (See note 1.)

Note (1) If you enter a port number value that is not the default, the value will be set.

Relay connection destination

Operation	Support Software status	Setting error description	What to do
Connecting online	Timeout display	*Not use FINS/UDP service* is set in the FINS/UDP setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use FINS/UDP service.
		The relay unit's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the relay unit's IP address setting is incorrect Change the relay unit's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the source IP address to permit the relay unit's IP address. The following is an example of the settings. Source IP address: Relay unit's IP address Protocol filter: Disabled
		UDP/9600 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit UDP/9600. The following is an example of the settings. Source IP address: Any Protocol: UDP Source port: Not specified Destination port: 9600 (See note 1.)

Note (1) If you enter a port number value that is not the default, the value will be set.

Relay node

Operation	Support Software status	Setting error description	What to do
Connecting online	Communications error display	*Not use FINS/UDP service* is set in the FINS/UDP setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use FINS/UDP service.

■ **Ethernet (FINS/TCP) or FinsGateway (When Using FINS/TCP)**

Direct connection destination

Operation	Support Software status	Setting error description	What to do
Connecting online	Timeout display	*Not use FINS/TCP service* is set in the FINS/TCP setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use FINS/TCP service.
		The computer's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the computer's IP address setting is incorrect Change the computer's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted and set the source IP address to permit the computer's IP address. The following is an example of the settings. Source IP address: Computer's IP address Protocol filter: Disabled
		TCP/9600 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit TCP/9600. The following is an example of the settings. Source IP address: Any Protocol: TCP Source port: Not specified Destination port: 9600 (See note 1.)

Note (1) If you enter a port number value that is not the default, the value will be set.

Relay connection destination

Operation	Support Software status	Setting error description	What to do
Connecting online	Timeout display	*Not use FINS/TCP service* is set in the FINS/TCP setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use FINS/TCP service.
		The relay unit's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the relay unit's IP address setting is incorrect Change the relay unit's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the source IP address to permit the relay unit's IP address. The following is an example of the settings. Source IP address: Relay unit's IP address Protocol filter: Disabled
		TCP/9600 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit TCP/9600. The following is an example of the settings. Source IP address: Any Protocol: TCP Source port: Not specified Destination port: 9600 (See note 1.)

Note (1) If you enter a port number value that is not the default, the value will be set.

Relay node

Operation	Support Software status	Setting error description	What to do
Connecting online	Communications error display	*Not use FINS/TCP service* is set in the FINS/TCP setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use FINS/TCP service.

■ **Toolbus, Toolbus (USB Port), or Device Name**

Relay connection destination

Operation	Support Software status	Setting error description	What to do
Connecting online	Timeout display	One of the following is true. • *Not use FINS/UDP service* is set in the FINS/UDP setting and *Not use FINS/TCP service* is set in the FINS/TCP setting. • The FINS/UDP and/or FINS/TCP settings are inconsistent between the EIP21S relay node and the EIP21S relay connection destination.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the settings of the EIP21S relay node and the EIP21S relay connection destination so that they are consistent. • To use FINS/UDP service Change the settings of both the EIP21S relay node and the EIP21S relay connection destination to use FINS/UDP service. • To use FINS/TCP service Change the settings of both the EIP21S relay node and the EIP21S relay connection destination to use FINS/TCP service.
		The relay unit's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the relay unit's IP address setting is incorrect Change the relay unit's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the source IP address to permit the relay unit's IP address. The following is an example of the settings. Source IP address: Relay unit's IP address Protocol filter: Disabled
		UDP/9600 or TCP/9600 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit UDP/9600 or TCP/9600. The following is an example of the settings. Source IP address: Any Protocol: UDP or TCP Source port: Not specified Destination port: 9600 (See note 1.)

Note (1) If you enter a port number value that is not the default, the value will be set.

Relay node

Operation	Support Software status	Setting error description	What to do
Connecting online	Timeout display	One of the following is true. • *Not use FINS/UDP service* is set in the FINS/UDP setting and *Not use FINS/TCP service* is set in the FINS/TCP setting. • The FINS/UDP and/or FINS/TCP settings are inconsistent between the EIP21S relay node and the EIP21S relay connection destination.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the settings of the EIP21S relay node and the EIP21S relay connection destination so that they are consistent. • To use FINS/UDP service Change the settings of both the EIP21S relay node and the EIP21S relay connection destination to use FINS/UDP service. • To use FINS/TCP service Change the settings of both the EIP21S relay node and the EIP21S relay connection destination to use FINS/TCP service.

■ **NS-Thru (USB Port)**

The connection format available in this case is relay connection destination only.

Relay connection destination

Operation	Support Software status	Setting error description	What to do
Connecting online	Timeout display	*Not use FINS/UDP service* is set in the FINS/UDP setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use FINS/UDP service.
		The Relay NS Unit's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the relay NS Unit's IP address setting is incorrect Change the relay NS Unit's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the source IP address to permit the relay NS Unit's IP address. The following is an example of the settings. Source IP address: Relay NS Unit's IP address Protocol filter: Disabled
		UDP/9600 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit UDP/9600. The following is an example of the settings. Source IP address: Any Protocol: UDP Source port: Not specified Destination port: 9600 (See note 1.)

Note (1) If you enter a port number value that is not the default, the value will be set.

Other Than Secure Comm - Case 2

In this case, the target Support Software is shown as below.

- CX-ConfiguratorFDT
  Applicable when the communications DTM is OMRON EtherNet/IP
- NX-IO Configurator

■ **CJ2 USB/Serial Port or CS/CJ1 Serial Port -> EIP Unit I/F**

The connection format available in this case is relay node only.

Relay node

Operation	Support Software status	Setting error description	What to do
Scanning after connecting online	No target device display	*Use CIP message server* is not set in the CIP message server setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use the CIP message server.

■ **Ethernet I/F**

Direct connection destination

Operation	Support Software status	Setting error description	What to do
Updating the connected network port when online	No EIP21S display	*Use CIP message server* is not set in the CIP message server setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use the CIP message server.
		The computer's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the computer's IP address setting is incorrect Change the computer's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted and set the source IP address to permit the computer's IP address. The following is an example of the settings. Source IP address: Computer's IP address Protocol filter: Disabled
		Any of the following is not permitted for the protocol filter in the IP Packet Filter Setting. • UDP/44818 • TCP/44818 • ICMP	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit a protocol that is consistent with the Support Software. The following is an example of the settings. Source IP address, Protocol, Source port, Destination port UDP: Any, UDP, Not specified, 44818 TCP: Any, TCP, Not specified, 44818 ICMP: Any, ICMP, Not specified, Not specified

Relay node

Operation	Support Software status	Setting error description	What to do
Scanning after connecting online	No target device display	*Use CIP message server* is not set in the CIP message server setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use the CIP message server.

Other Than Secure Comm - Case 3

In this case, the target Support Software is shown as below.

• Network Configurator

■ **CJ2 USB/Serial Port or CS/CJ1 Serial Port -> EIP Unit I/F**

Relay node

Operation	Support Software status	Setting error description	What to do
Executing update after going online	No target device display under EIP21S relay node	*Use CIP message server* is not set in the CIP message server setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use the CIP message server.

Relay connection destination

Operation	Support Software status	Setting error description	What to do
Executing update after going online	No target EIP21S display in Select Connect Network Port Dialog Box	*Use CIP message server* is not set in the CIP message server setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use the CIP message server.
		The relay unit's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the relay unit's IP address setting is incorrect Change the relay unit's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the source IP address to permit the relay unit's IP address. The following is an example of the settings. Source IP address: Relay unit's IP address Protocol filter: Disabled
		Any of the following is not permitted for the protocol filter in the IP Packet Filter Setting. • UDP/44818 • TCP/44818 • ICMP	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit a protocol that is consistent with the Support Software. The following is an example of the settings. Source IP address, Protocol, Source port, Destination port UDP: Any, UDP, Not specified, 44818 TCP: Any, TCP, Not specified, 44818 ICMP: Any, ICMP, Not specified, Not specified

■ **Ethernet I/F**

Direct connection destination

Operation	Support Software status	Setting error description	What to do
Executing update after going online	No target EIP21S display in Select Connect Network Port Dialog Box	*Use CIP message server* is not set in the CIP message server setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use the CIP message server.
		The computer's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the computer's IP address setting is incorrect Change the computer's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the source IP address to permit the computer's IP address. The following is an example of the settings. Source IP address: Computer's IP address Protocol filter: Disabled
		Any of the following is not permitted for the protocol filter in the IP Packet Filter Setting. • UDP/44818 • TCP/44818 • ICMP	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit a protocol that is consistent with the Support Software. The following is an example of the settings. Source IP address, Protocol, Source port, Destination port UDP: Any, UDP, Not specified, 44818 TCP: Any, TCP, Not specified, 44818 ICMP: Any, ICMP, Not specified, Not specified

Relay node

Operation	Support Software status	Setting error description	What to do
Executing update after going online	No target device display under EIP21S relay node	*Use CIP message server* is not set in the CIP message server setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use the CIP message server.

Relay connection destination

Operation	Support Software status	Setting error description	What to do
Executing update after going online	No target EIP21S display in Select Connect Network Port Dialog Box	*Use CIP message server* is not set in the CIP message server setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use the CIP message server.
		The relay unit's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the relay unit's IP address setting is incorrect Change the relay unit's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the source IP address to permit the relay unit's IP address. The following is an example of the settings. Source IP address: Relay unit's IP address Protocol filter: Disabled
		Any of the following is not permitted for the protocol filter in the IP Packet Filter Setting. • UDP/44818 • TCP/44818 • ICMP	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit a protocol that is consistent with the Support Software. The following is an example of the settings. Source IP address, Protocol, Source port, Destination port UDP: Any, UDP, Not specified, 44818 TCP: Any, TCP, Not specified, 44818 ICMP: Any, ICMP, Not specified, Not specified

18-7-2 Communications with External Devices

This section describes what you should do if an error occurs in communications with external devices for each usage.

Tag Data Link

Status	Error cause		What to do
	Setting error	Setting error description	
The following occurs in the originator. Verification error (target nonexistent) 7-segment display: d5 Error code: None	Local node (originator) setting error	In the case of multicast, IGMP is not permitted in *Protocol filter* in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit IGMP. The following is an example of the settings. Source IP address: Any Protocol: IGMP Source port: Not specified Destination port: Not specified
	Remote node (target) setting error	*Use CIP message server* is not set in the CIP message server setting.	Change the setting to use the CIP message server.
		The originator's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	Change the source IP address setting to permit the originator's IP address.
		TCP/44818 is not permitted for the protocol filter in the IP Packet Filter Setting.	Change the protocol filter setting to permit the following. Protocol: TCP Destination port: 44818
An error occurs in another company's PLC (originator). • General Status: 01 hex • Additional Status: 0204 hex	Target (OMRON node) setting error	*Use CIP message server* is not set in the CIP message server setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use the CIP message server.
		The originator's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the source IP address to permit the originator's IP address. The following is an example of the settings. Source IP address: Originator's IP address Protocol filter: Disabled
		TCP/44818 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit TCP/44818. The following is an example of the settings. Source IP address: Any Protocol: TCP Source port: Not specified Destination port: 44818

CIP Message (FINS2810) This is applicable to cases where the following instruction is used.

FINS command *CIP UCMM MESSAGE SEND(2810)* used in the CMND(490) instruction

Status	Error cause		What to do
	Setting error	Setting error description	
The instruction ends normally. However, the response to the CIP message is as follows. General Status: 01 hex Additional Status: 0204 hex	With relay node Relay node setting error	*Use CIP message server* is not set in the CIP message server setting.	Change the setting to use the CIP message server.
		The client's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	Change the source IP address setting to permit the client's IP address.
		TCP/44818 is not permitted for the protocol filter in the IP Packet Filter Setting.	Change the protocol filter setting to permit the following. Protocol: TCP Destination port: 44818
	Remote node (server) setting error	*Use CIP message server* is not set in the CIP message server setting.	Change the setting to use the CIP message server.
		Both are IP packet filter settings. Without relay node • The client's IP address is not permitted. With relay node • The relay node's IP address is not permitted.	• Without relay node Change the source IP address setting to permit the client's IP address. • With relay node Change the source IP address setting to permit the relay node's IP address.
		TCP/44818 is not permitted for the protocol filter in the IP Packet Filter Setting.	Change the protocol filter setting to permit the following. Protocol: TCP Destination port: 44818

CIP Message (FINS2801)

This is applicable to cases where the following instruction is used.

- FINS command *EXPLICIT MESSAGE SEND(2801)* used in the CMND(490) instruction
- EXPLT
- EGATR

Status	Error cause		What to do
	Setting error	Setting error description	
The instruction ends normally. However, the response to the CIP message is as follows. General Status: 01 hex Additional Status: 0204 hex	Remote node (server) setting error	*Use CIP message server* is not set in the CIP message server setting.	Change the setting to use the CIP message server.
		The client's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	Change the source IP address setting to permit the client's IP address.
		TCP/44818 is not permitted for the protocol filter in the IP Packet Filter Setting.	Change the protocol filter setting to permit the following. Protocol: TCP Destination port: 44818

FINS Message

This is applicable to cases where the following instruction is used.

- SEND
- RECV
- CMND

Status	Error cause		What to do
	Setting error	Setting error description	
With response Instruction will end abnormally. FINS completion code: 0205 hex (Response timeout)	Local node (client) setting error	*Not use FINS/UDP service* is set in the FINS/UDP setting and *Not use FINS/TCP service* is set in the FINS/TCP setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use FINS/UDP or FINS/TCP service.
	Remote node (server) setting error	*Not use FINS/UDP service* is set in the FINS/UDP setting and *Not use FINS/TCP service is* set in the FINS/TCP setting.	Change the setting to use FINS/UDP or FINS/TCP service.
		The client's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	Change the source IP address setting to permit the client's IP address.
		UDP/9600 or TCP/9600 is not permitted for the protocol filter in the IP Packet Filter Setting.	Change the protocol filter setting to permit the following. Protocol: UDP or TCP Destination port: 9600 (See note 1.)

Note (1) If you enter a port number value that is not the default, the value will be set.

FTP Client

Status	Error cause		What to do
	Setting error	Setting error description	
FTP client cannot establish FTP connections.	EIP21S setting error	The FTP client's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the source IP address to permit the FTP client's IP address. The following is an example of the settings. Source IP address: FTP client's IP address Protocol filter: Disabled
		TCP/20, 21 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and change the protocol filter settings to permit the following. Protocol: TCP Destination port: 20, 21 (See note 1.)

Note (1) If you enter a port number value that is not the default, the value will be set.

SNMP Agent

Status	Error cause		What to do
	Setting error	Setting error description	
SNMP agent cannot establish FTP connections.	EIP21S setting error	The SNMP agent's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the source IP address to permit the SNMP agent's IP address. The following is an example of the settings. Source IP address: SNMP agent's IP address Protocol filter: Disabled
		UDP/161 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit UDP/161. The following is an example of the settings. Source IP address: Any Protocol: UDP Source port: Not specified Destination port: 161 (See note 1.)

Note (1) If you enter a port number value that is not the default, the value will be set.

Socket Service

Status	Error cause		What to do
	Setting error	Setting error description	
• TCP socket passive open request time-out (Completion code: 0080 hex) • UDP/TCP socket receive request time-eout (Completion code: 0080 hex)	Local node setting error	The remote node's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the source IP address to permit the remote node's IP address. The following is an example of the settings. Source IP address: Remote node's IP address Protocol filter: Disabled
		The TCP port opened by the local node is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit the opened UDP/TCP port. The following is an example of the settings. Source IP address: Any Protocol: Protocol for the opened port Source port: Not used Destination port: Port number of the opened port
TCP socket active open request communications error (Completion code: 0053 hex)	If the remote node is EIP21S Remote node setting error	The active open request node's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the source IP address to permit the active open request node's IP address. The following is an example of the settings. Source IP address: Active open request node's IP address Protocol filter: Disabled
		The TCP port opened by the local node is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit the opened TCP port. The following is an example of the settings. Source IP address: Any Protocol: TCP Source port: Not specified Destination port: Port number of the opened port

Sysmac Gateway

Status	Error cause		What to do
	Setting error	Setting error description	
Tag data link timeout	EIP21S setting error	*Use CIP message server* is not set in the CIP message server setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use the CIP message server.
		The originator's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the source IP address to permit the originator's IP address. The following is an example of the settings. Source IP address: Originator's IP address Protocol filter: Disabled
		TCP/44818 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit TCP/44818. The following is an example of the settings. Source IP address: Any Protocol: TCP Source port: Not specified Destination port: 44818

CX-Compolet

Status	Error cause		What to do
	Setting error	Setting error description	
Timeout	EIP21S setting error	*Use CIP message server* is not set in the CIP message server setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use the CIP message server.
		The CX-Compolet's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the source IP address to permit the CX-Compolet's IP address. The following is an example of the settings. Source IP address: CX-Compolet's IP address Protocol filter: Disabled
		TCP/44818 or UDP/44818 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit TCP/44818 or UDP/44818. The following is an example of the settings. Source IP address: Any Protocol: TCP or UDP Source port: Not specified Destination port: 44818

BOOTP

Status	Error cause		What to do
	Setting error	Setting error description	
Server connection error 7-segment display: E3 Error code: 03C4 hex Detailed code: First byte: 06 hex, second byte: 03 hex	EIP21S setting error	The BOOTP server's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	Connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted and set the source IP address to permit the BOOTP server's IP address. The following is an example of the settings. Source IP address: BOOTP server's IP address Protocol filter: Disabled
		UDP/68 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted and set the protocol filter to permit UDP/68. The following is an example of the settings. Source IP address: Any Protocol: UDP Source port: Not specified Destination port: 68

18-7-3 Communications with HMIs

This section describes what you should do if an error occurs in communications with HMIs.

■ If Using an NA-series Programmable Terminal as HMI

When the connection method is EtherNet/IP

Status of NA Series	Error cause		What to do
	Setting error	Setting error description	
Timeout display	EIP21S setting error	*Use CIP message server* is not set in the CIP message server setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use the CIP message server.
	NA Series setting error, or EIP21S setting error	The NA Unit's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the NA Unit's IP address setting is incorrect Change the NA Unit's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted and set the source IP address to permit the NA Unit's IP address. The following is an example of the settings. Source IP address: NA Unit's IP address Protocol filter: Disabled
	EIP21S setting error	TCP44818 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit TCP/44818. The following is an example of the settings. Source IP address: Any Protocol: TCP Source port: Not specified Destination port: 44818

When the connection method is Ethernet

Status of NA Series	Error cause		What to do
	Setting error	Setting error description	
Timeout display	EIP21S setting error	*Not use FINS/UDP service* is set in the FINS/UDP setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use FINS/UDP service.
	NA Series setting error, or EIP21S setting error	The NA Unit's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the NA Unit's IP address setting is incorrect Change the NA Unit's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted and set the source IP address to permit the NA Unit's IP address. The following is an example of the settings. Source IP address: NA Unit's IP address Protocol filter: Disabled
	EIP21S setting error	UDP/9600 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit UDP/9600. The following is an example of the settings. Source IP address: Any Protocol: UDP Source port: Not specified Destination port: 9600 (See note 1.)

Note (1) If you enter a port number value that is not the default, the value will be set.

■ **If Using an NB-series Programmable Terminal as HMI**

The connection method available in this case is Ethernet only.

When the connection method is Ethernet

Status of NB Series	Error cause		What to do
	Setting error	Setting error description	
Timeout display	EIP21S setting error	*Not use FINS/UDP service* is set in the FINS/UDP setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use FINS/UDP service.
	NB Series setting error, or EIP21S setting error	The NB Unit's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the NB Unit's IP address setting is incorrect Change the NB Unit's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted and set the source IP address to permit the NB Unit's IP address. The following is an example of the settings. Source IP address: NB Unit's IP address Protocol filter: Disabled
	EIP21S setting error	UDP/9600 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit UDP/9600. The following is an example of the settings. Source IP address: Any Protocol: UDP Source port: Not specified Destination port: 9600 (See note 1.)

Note (1) If you enter a port number value that is not the default, the value will be set.

■ If Using an NS-series Programmable Terminal as HMI

When the connection method is EtherNet/IP

Status of NS Series	Error cause		What to do
	Setting error	Setting error description	
Timeout display	EIP21S setting error	*Use CIP message server* is not set in the CIP message server setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use the CIP message server.
	NS Series setting error, or EIP21S setting error	The NS Unit's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the NS Unit's IP address setting is incorrect Change the NS Unit's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted and set the source IP address to permit the NS Unit's IP address. The following is an example of the settings. Source IP address: NS Unit's IP address Protocol filter: Disabled
	EIP21S setting error	TCP44818 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit TCP/44818. The following is an example of the settings. Source IP address: Any Protocol: TCP Source port: Not specified Destination port: 44818

When the connection method is Ethernet

Status of NS Series	Error cause		What to do
	Setting error	Setting error description	
Timeout display	EIP21S setting error	*Not use FINS/UDP service* is set in the FINS/UDP setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of CPU on which the EIP21S is mounted, and change the setting to use FINS/UDP service.
	NS Series setting error, or EIP21S setting error	The NS Unit's IP address is not permitted for the source IP address in the IP Packet Filter Setting.	• If the NS Unit's IP address setting is incorrect Change the NS Unit's IP address to the one permitted for the IP packet filter. • If the EIP21S Unit's settings are incorrect Connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted and set the source IP address to permit the NS Unit's IP address. The following is an example of the settings. Source IP address: NS Unit's IP address Protocol filter: Disabled
	EIP21S setting error	UDP/9600 is not permitted for the protocol filter in the IP Packet Filter Setting.	Connect the CX-P directly to the EIP21S using Secure Comm or connect the CX-P online via the USB or serial port of the CPU on which the EIP21S is mounted, and set the protocol filter to permit UDP/9600. The following is an example of the settings. Source IP address: Any Protocol: UDP Source port: Not specified Destination port: 9600 (See note 1.)

Note (1) If you enter a port number value that is not the default, the value will be set.

Appendix A
CS/CJ-series Ethernet Unit Function Comparison

Item	Support for function			
	Ethernet Unit CS1W-ETN21 CJ1W-ETN21	Built-in EtherNet/IP port CS1W-EIP21S CJ1W-EIP21S CJ3M-CPU3☐	Built-in EtherNet/IP port CS1W-EIP21, CJ1W-EIP21, CJ2H-CPU6☐-EIP, CJ2M-CPU3☐	
			Unit version 1.0	Unit version 2.0 or later
Tag data link communications service	No	Yes	Yes	Yes
CIP message communications service	No	Yes	Yes	Yes
FINS/UDP service	Yes	Yes	Yes	Yes
FINS/TCP service	Yes	Yes	Yes	Yes
Socket service	Yes	Yes	No	No
Modbus Server Functions	No	Yes (See note 3.)	No	No
Modbus Client Functions	No	Yes (See note 4.)	No	No
File transfer (FTP)	Yes	Yes	No	Yes
Mail send/receive	Yes	No	No	No
Web functions	Yes	No	No	No
Automatic adjustment of PLC's internal clock	Yes	Yes	No	Yes
Simple backup function	Yes	Yes	Yes	Yes
Error log	Yes	Yes	Yes	Yes
Response to PING command	Yes	Yes	Yes	Yes
SNMP/SNMP trap	No	Yes	No	Yes
LLDP function	No	Yes (See note 3.)	No	No
CIDR function for IP addresses	Yes (See note 1.)	Yes	No	Yes
Online connection by EtherNet/IP using CX-One	No	Yes	No	Yes
Online connection by Ethernet (FINS) using CX-One	Yes	Yes	Yes	Yes
Online connection by EtherNet/IP using Network Configurator	No	Yes	Yes	Yes
Secure communications (See note 2.)	No	Yes	No	No
User authentication (See note 2.)	No	Yes	No	No
Opening and closing the port	No	Yes	No	No
IP packet filtering	No	Yes	No	No
Operation log (See note 2.)	No	Yes	No	No

Note (1) This function is supported by unit version 1.5 or later.

(2) When connected to the CP1H CPU Units, the CX-Programmer and PLC backup tools cannot use the corresponding functions.

(3) This is enabled for CJ3M-CPU3☐ only.

(4) This function is supported by the CJ1W-EIP21S connected to the CJ2/CJ3 CPU Unit, or CJ3M-CPU3☐.

Appendix B
Ethernet Network Parameters

Parameter	Value		Description
	CS1WCJ1W-EIP21 CJ2H-CPU6□-EIP CJ2M-CPU3□	CS1WCJ1W-EIP21S CJ3M-CPU3□	
TCP send buffer	4,096 bytes	22,528 bytes	Maximum capacity of the TCP send buffer
TCP receive buffer	4,096 bytes	32,768 bytes	Maximum capacity of the TCP receive buffer
UDP send buffer	9,000 bytes	41,600 bytes	Maximum capacity of the UDP send buffer
UDP receive buffer	9,016 bytes	9,216 bytes	Maximum capacity of the UDP receive buffer
FINS receive buffer	16,383 bytes		Maximum capacity of the FINS receive buffer
Modbus server receive buffer	-	2,080 bytes	Maximum capacity of the TCP receive buffer (CJ3M-CPU3□ only)
	-	66,560 bytes	Maximum capacity of the UDP send buffer (CJ3M-CPU3□ only)
RAW send buffer	2,048 bytes	8,192 bytes	Maximum capacity of the RAW send buffer
RAW receive buffer	2,048 bytes	8,192 bytes	Maximum capacity of the RAW receive buffer
Hold timer	75 s (See note 1.)		The hold timer is used for active open processing of TCP sockets. An ETIMEDOUT error will occur if connection is not completed within 75 s.
Resend timer	Initial value: 1 s Maximum value: 64 s		The resend timer is used to monitor completion of reception of arrival confirmations when transferring data via TCP sockets. If the timer setting is exceeded before arrival confirmation is received, data is resent. Resends are performed from the first timeout (1 s) through the 12th timeout (64 s). An ETIMEDOUT error will occur after the 12th timeout.
Continue timer	Initial value: 1 s Maximum value: 60 s	Initial value: 5 s Maximum value: 60 s	The continue timer starts if preparations have been completed to send data but the send window is too small (either 0 or too small) to send the data and the remote node has not requested that communications be restarted. Confirmation of the window size is requested from the remote node when the continue timer times out. The confirmation processing will continue consecutively with increasingly longer times until the maximum time of 60 s is reached.
2MSL timer	60 s		The 2MSL timer starts at the TCP socket that first closes the socket and will run for 60 s in the TIME_WAIT status.
IP reassemble timer	12 s	60 s	If a fragmented IP packet cannot be reassembled when the length of IP reassemble timer is exceeded, the IP packet is discarded.
ARP timer	20 min/3 min	20 min/ 20 s	If a complete ARP table entry (with an Ethernet address) is not referred to for 20 minutes, it is removed from the table. An incomplete ARP table entry (no response yet returned to the ARP request) is removed from the table after 3 minutes or 20 seconds.
Fragment size	1,500 bytes		Data packets are fragmented into 1,500-byte IP packets. UDP data is separated into 1,472-byte fragments before sending.
Segment size	1,024 bytes	1,460 bytes	TCP data is separated into the segment size units. However, when the segments are different, it is separated into 536-byte units.
TTL (Time to Live)	30 (See note 2.)	64 (See note 2.)	Decremented each time an IP router is passed.
Keep-alive timer	First time: 5 min Resend: 5 s × 5 times	First time: 5 min (See note 3.) Resend: 5 s × 6 times	The keep-alive timer is used for the keep-alive function with TCP connections. It must be used with UCMM, Class 3.
LLDP timer	-	30 s	LLDP frame transmission interval

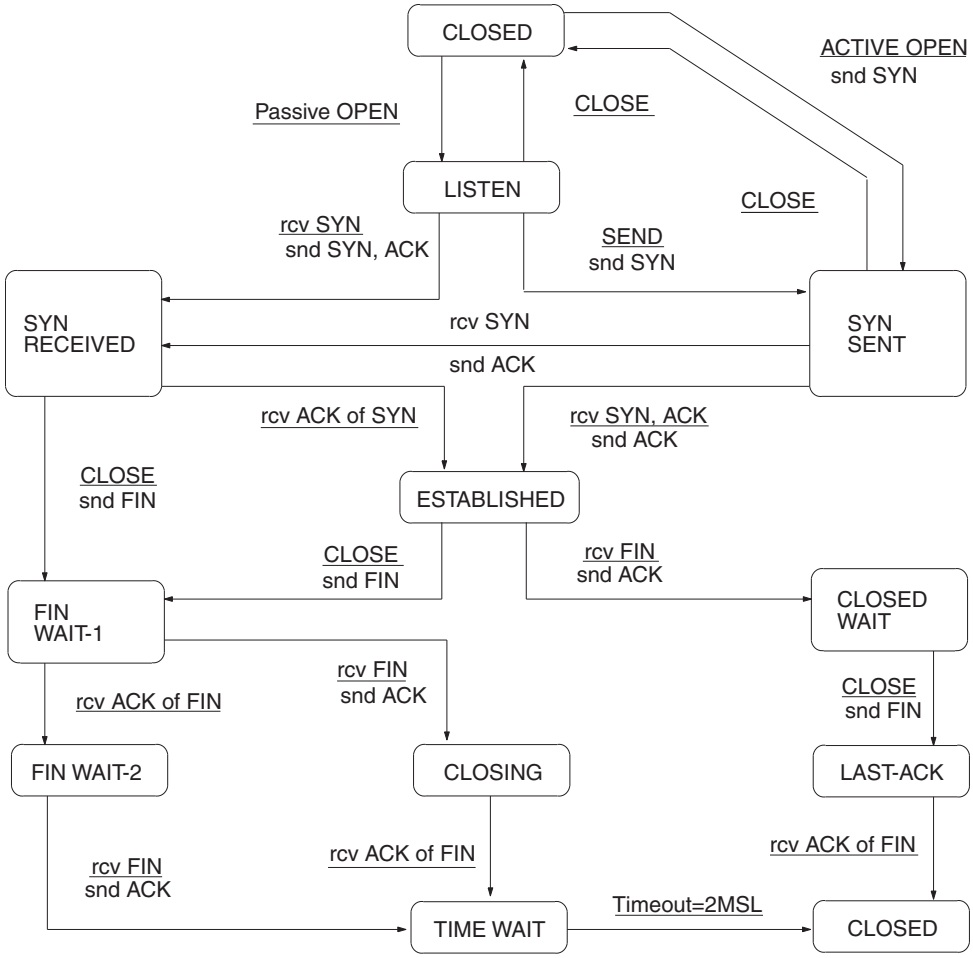
Note (1) The hold time is 3 s for the UCMM service, Class 3 service, and tag data link open/close processing.

(2) This value is 1 if the multicast connection is selected in the connection type in the tag data link connection settings.

(3) Initial value. You can change this value in the *TCP/IP keep-alive* setting in the TCP/IP Tab Page of the Edit Parameters Dialog Box.

Appendix C
TCP Status Transitions

The TCP socket status can be confirmed using the socket status data returned for the FINS command SOCKET STATUS READ (27 64).



Status	Meaning
CLOSED	Connection closed.
LISTEN	Waiting for connection.
SYN SENT	SYN sent in active status.
SYN RECEIVED	SYN received and sent.
ESTABLISHED	Already established.
CLOSE WAIT	FIN received and waiting for completion.
FIN WAIT 1	Completed and FIN sent.
CLOSING	Completed and exchanged FIN. Awaiting ACK.
LAST ACK	FIN sent and completed. Awaiting ACK.
FIN WAIT 2	Completed and ACK received. Awaiting FIN.
TIME WAIT	After closing, pauses twice the maximum segment life (2MSL).

Appendix D
CIP Message Communications

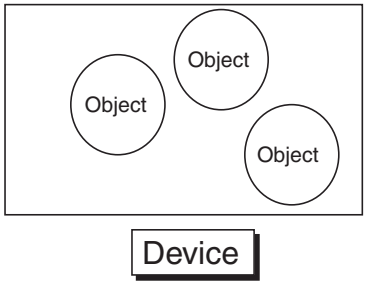
This appendix describes CIP message communications.

The basic concepts of CIP message communications are described in this appendix from *CIP Object* on page 611 through *Example of CIP Message Creation* on page 616. Read these sections to improve your understanding of CIP message communications.

CIP Object

Object Model

In the CIP (Common Industrial Protocol) system, each device is modeled as a group of “Objects.” An Object abstractly represents a related group of the device’s data values.



When accessing the device from the outside, access an Object.

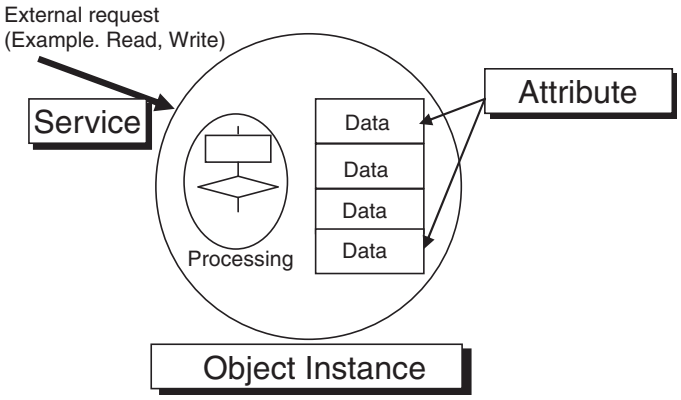
An Object represents the abstracted device function, processing, and the resulting data.

A request from the outside of Object, such as Read Data, is called “Service.”

Data belonging to the Object is called “Attribute.”

The actual entity of Object is called “Instance” or “Object Instance.”

When Object is generalized, it is called “Class.” For example, “Japan” is one of Instances (Object Instances) of Class “Nation.”



Terminology

In CIP specifications, “Object,” “Class,” “Instance,” “Attribute” and “Service” are defined as follows:

Term	Meaning
Object	An abstract representation of a particular component within a product.
Class	A set of objects that all represent the same kind of system component. A class is a generalization of an object. All objects in a class are identical in form and behavior, but may contain different attribute values.
Instance	A specific and real (physical) occurrence of an object. For example: New Zealand is an instance of the object class Country. The terms Object, Instance, and Object Instance all refer to a specific Instance.
Attribute	A description of an externally visible characteristic or feature of an object. Typically, attributes provide status information or govern the operation of an Object. For example: the ASCII name of an object; and the repetition rate of a cyclic object.
Service	A function supported by an object and/or object class. CIP defines a set of common services and provides for the definition of Object Class and/or Vendor Specific services.

Specifying an Object Address (Request Path)

This is the basic concept involved in accessing an Object or Attribute.

Each Object Class has a “Class ID”.

There are two types of “Class ID”; one is standardized by ODVA and the other is decided independently by each device vendor.

Each Object Instance also has ID. This is called “Instance ID.” Different Instance ID is assigned to each Object. As for Object Class standardized by ODVA, Instance ID is given to it according to the ODVA method. On the other hand, vendor's own Instance ID is decided independently by the vendor.

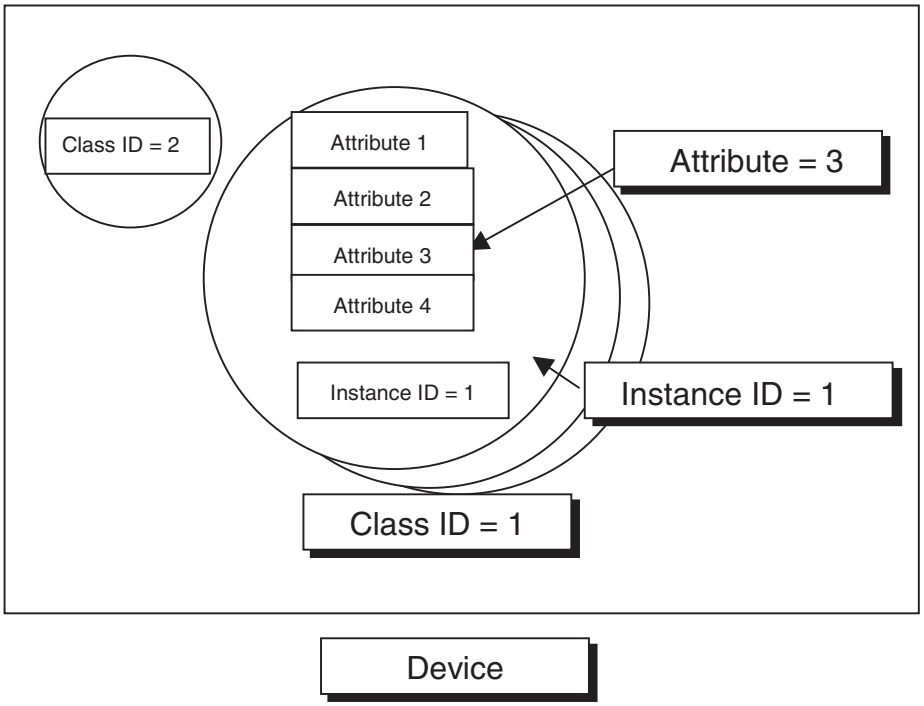
Each Attribute also has “Attribute ID.”

Each Object is accessed to by using “Class ID,” “Instance ID,” and “Attribute ID.”

In the device, you can designate Object by specifying these three IDs.

When requesting “Service,” you should specify “Class ID,” “Instance ID,” and “Attribute ID.” (Instance ID and Attribute ID may not be required, depending on the Service.)

The “Class ID,” “Instance ID,” and “Attribute ID” identify a location in the device and are known as the request path.



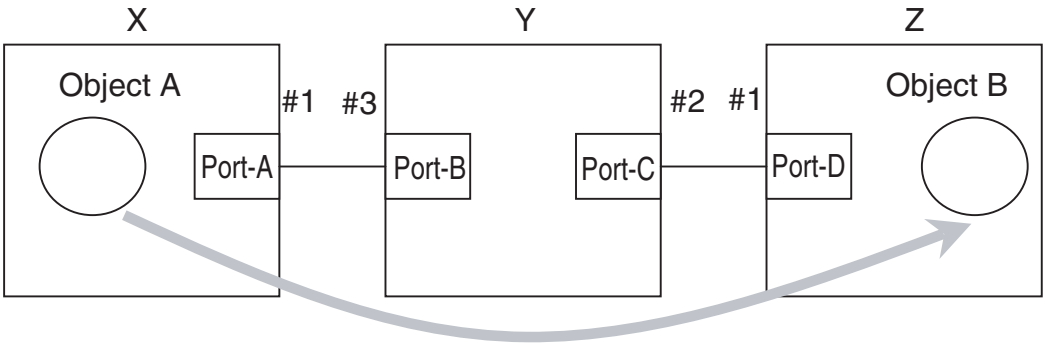
Route Path

Route Path

In the CIP, unlike the internet protocol, the transmission frame contains a complete relay route from the transmission node to the reception node. The described route is called the “route path.” The route path is described as “EPATH type.”

The basic concept of the route path is as follows:

First of all, specify a network port of the transmission node with the destination network, and specify a node address (called the Link Address) on that network. For the relay node, similarly, specify a network port with the destination network and node address on that network. Then, repeat the same procedure to the final destination.



When sending data from X to Z.

Route Path = Port A: #3, Port C: #1

Send data from the network port of X (Port-A) to #3 on that circuit, and the data reaches Y. Then, send it from the network port of Y (Port-C) to #1 on that circuit. Through this procedure, the destination node Z can be designated.

Description by EPATH Type

In CIP, the EPATH type is used to describe the route path and request path.

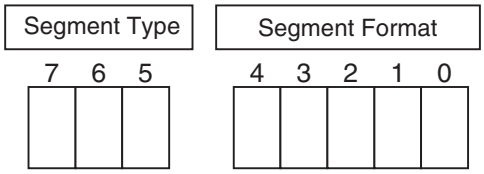
With this method, the route path and request path are divided into segments and a value is assigned to each segment, so the route path description shows the path to the final destination when the data segments are joined together.

The segment includes the segment type information and the segment data.

Segment 1	Segment 2	Segment 3	Segment 4	· · · ·

Details of Segment Type

The interpretation method of a segment is included in the first 1 byte, which consists of two parts; a 3-bit “Segment Type” and a 5-bit “Segment Format.”



According to CIP Specifications, the Segment Type specifications are decided as follows:

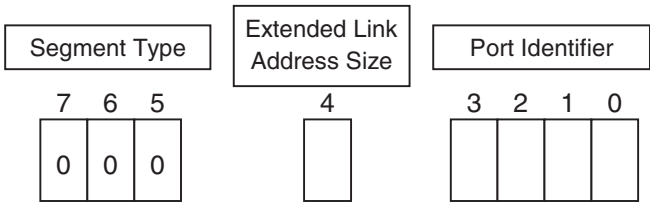
Segment Type			Description
7	6	5	
0	0	0	Port Segment
0	0	1	Logical Segment
0	1	0	Network Segment
0	1	1	Symbolic Segment
1	0	0	Data Segment
1	0	1	Data Type
1	1	0	Data Type
1	1	1	Reserved

The specifications of Segment Format are different for each Segment Type.

The following sections describe Port Segment, Logical Segment, and Data Segment which are needed to use the CIP message communications instructions.

Port Segment

The Port Segment is used to specify the path described above.



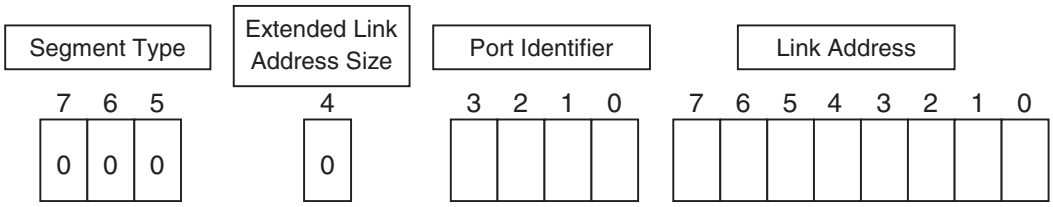
Set the ID of the port in Port Identifier.

The Port Identifier is 4 bits, so it can have a value between 0 and 15. A port identifier of “0” is reserved and not available. A port identifier of “1” indicates the backplane port.

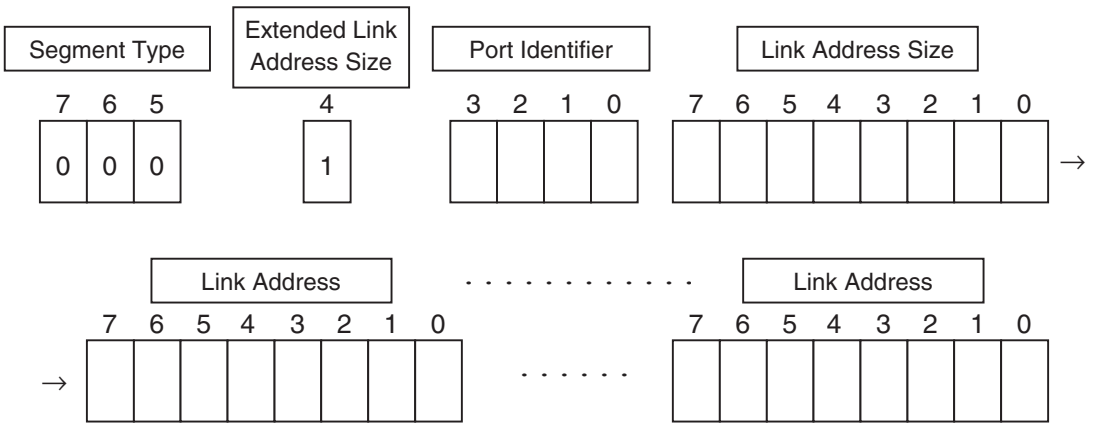
A port identifier of “15” has a special meaning, which indicates that the size of Port Identifier is larger than 1 byte, and the 4-bit port identifier (15) is followed by 2-byte Port Identifier. The port identifier does not exceed 1 byte when using the EtherNet/IP Unit or built-in EtherNet/IP port, so this special case is not explained here.

Set the Extended Link Address Size to “1” when that port’s Link Address is larger than 1 byte.

The following diagram shows the Port Segment value when the Extended Link Address Size is set to “0.”



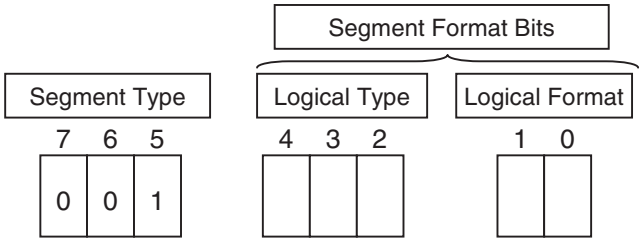
Specify the size of Link Address when the Extended Link Address Size is set to “1.” The following diagram shows the Port Segment value in this case.



Always set the Link Address to an even number of bytes. If there is an odd number of bytes, pad the Link Address with “00” so that it has an even number of bytes.

Logical Segment

The Logical Segment is used to specify the request path.



Logical Type			Description
4	3	2	
0	0	0	Class ID
0	0	1	Instance ID
0	1	0	Member ID
0	1	1	Connection Point
1	0	0	Attribute ID
1	0	1	Special (Do not use the logical addressing definition for the Logical Format.)
1	1	0	Service ID (Do not use the logical addressing definition for the Logical Format.)
1	1	1	Reserved

Logical Format		Description
1	0	
0	0	8-bit logical address
0	1	16-bit logical address
1	0	32-bit logical address
1	1	Reserved

The 32-bit logical address format is reserved and cannot be used.

The 8-bit and 16-bit logical address can be used for the Class ID and Instance ID, which specify the request path.

The 8-bit logical address can be used for the Attribute ID. Use the Attribute ID when requesting a Service of a particular Object of a particular device.

Example of CIP Message Creation

Setting the Route Path

Port Number

The following description explains the network port, which is used to specify the route path. In the CJ2/CJ3 Series, the Backplane is also considered part of the network when specifying the Link Address.

CPU Unit

CJ2/CJ3 (Not supported by CS1/CJ1 CPU Units.)

Each CPU Unit has one backplane port. By convention, the built-in EtherNet/IP port on a CJ2H-CPU6□-EIP or a CJ2M-CPU3□, CJ3M-CPU3□ CPU Unit functions as a CPU Bus Unit or Special I/O Unit.

Port	Port Number
Backplane	1

The Backplane port is the Backplane. CPU Unit communications routed through CPU Bus Units always travel through the backplane.

EtherNet/IP Unit or Built-in Port

The EtherNet/IP Unit has two ports. A CPU Unit also has two EtherNet/IP ports. One is a Backplane port and the other is an Ethernet port.

The Backplane port is the Backplane. Communications routed through the CPU Unit, a Special I/O Unit, or another CPU Bus Unit always travel through the backplane.

Port	Port Number
Backplane	1
Ethernet	2

Link Address

The Link Address is a node address on the network, which is used to specify the route path.

The method to set the Link Address is different for each network.

In the CS/CJ Series, the Backplane is also considered part of the network when specifying the Link Address.

Backplane

- **CPU Bus Unit or Special I/O Unit**
  In the CS/CJ Series, the base unit is recognized as a backplane port.
  CPU Bus Units, such as the EtherNet/IP Unit, are also recognized as nodes on the backplane port.
  The Link Address of a CPU Bus Unit on the Backplane is the “unit number + 10 hex.” For example, when the unit number is 0, the Link Address is 10 hex. When the unit number is F, the Link Address is 1F hex.
  The Link Address of a Special I/O Unit on the Backplane is the “unit number + 20 hex.” For example, when the unit number is 0, the Link Address is 20 hex.

Network

- **EtherNet/IP**
  The Ethernet port’s Link Address is described by the IP address.
  The IP address must be described entirely in ASCII.
  For example, IP address of 192.168.200.200 will be [31] [39] [32] [2E] [31] [36] [38] [2E] [32] [30] [30] [2E] [32] [30] [30].

Response Codes

General Status Code

The General Status Code is stored in the response data after execution of the CMND instruction has been completed.

General Status Code (hex)	Status Name	Description of Status
00	Success	Service was successfully performed by the object specified.
01	Connection failure	A connection related service failed along the connection path.
02	Resource unavailable	Resources needed for the object to perform the requested service were unavailable.
03	Invalid parameter value	See Status Code 20 hex, which is the preferred value to use for this condition.
04	Path segment error	The path segment identifier or the segment syntax was not understood by the processing node. Path processing shall stop when a path segment error is encountered.
05	Path destination unknown	The path is referencing an object class, instance or structure element that is not known or is not contained in the processing node. Path processing shall stop when a path destination unknown error is encountered.
06	Partial transfer	Only part of the expected data was transferred.
07	Connection lost	The messaging connection was lost.
08	Service not supported	The requested service was not implemented or was not defined for this Object Class/Instance.
09	Invalid attribute value	Invalid attribute data detected.
0A	Attribute list error	An attribute in the Get_Attribute_List or Set_Attribute_List response has a non-zero status.
0B	Already in requested mode/state	The object is already in the mode/state being requested by the service.
0C	Object state conflict	The object cannot perform the requested service in its current mode/state.
0D	Object already exists	The requested instance of object to be created already exists.
0E	Attribute not settable	A request to modify a non-modifiable attribute was received.
0F	Privilege violation	A permission/privilege check failed.
10	Device state conflict	The device's current mode/state prohibits the execution of the requested service.
11	Reply data too large	The data to be transmitted in the response buffer is larger than the allocated response buffer
12	Fragmentation of a primitive value	The service specified an operation that is going to fragment a primitive data value, i.e. half a REAL data type.
13	Not enough data	The service did not supply enough data to perform the specified operation.
14	Attribute not supported	The attribute specified in the request is not supported.
15	Too much data	The service supplied more data than was expected.
16	Object does not exist	The object specified does not exist in the device.
17	Service fragmentation sequence not in progress	The fragmentation sequence for this service is not currently active for this data.
18	No stored attribute data	The attribute data of this object was not saved prior to the requested service.
19	Store operation failure	The attribute data of this object was not saved due to a failure during the attempt.
1A	Routing failure (request packet too large)	The service request packet was too large for transmission on a network in the path to the destination. The routing device was forced to abort the service.
1B	Routing failure (response packet too large)	The service response packet was too large for transmission on a network in the path from the destination. The routing device was forced to abort the service.
1C	Missing attribute list entry data	The service did not supply an attribute in a list of attributes that was needed by the service to perform the requested behavior.

General Status Code (hex)	Status Name	Description of Status
1D	Invalid attribute value list	The service is returning the list of attributes supplied with status information for those attributes that were invalid.
1E	Embedded service error	An embedded service resulted in an error.
1F	Vendor specific error	A vendor specific error has been encountered. The Additional Code Field of the Error Response defines the particular error encountered. Use of this General Error Code should only be performed when none of the Error Codes presented in this table or within an Object Class definition accurately reflect the error.
20	Invalid parameter	A parameter associated with the request was invalid. This code is used when a parameter does not meet the requirements of this specification and/or the requirements defined in an Application Object Specification.
21	Write-once value or medium already written	An attempt was made to write to a write-once medium (e.g. WORM drive, PROM) that has already been written, or to modify a value that cannot be changed once established.
22	Invalid Reply Received	An invalid reply is received (e.g. reply service code does not match the request service code, or reply message is shorter than the minimum expected reply size). This status code can serve for other causes of invalid replies.
23-24		Reserved by CIP for future extensions
25	Key Failure in path	The Key Segment that was included as the first segment in the path does not match the destination module. The object specific status shall indicate which part of the key check failed.
26	Path Size Invalid	The size of the path which was sent with the Service Request is either not large enough to allow the Request to be routed to an object or too much routing data was included.
27	Unexpected attribute in list	An attempt was made to set an attribute that is not able to be set at this time.
28	Invalid Member ID	The Member ID specified in the request does not exist in the specified Class/ Instance/Attribute.
29	Member not settable	A request to modify a non-modifiable member was received.
2A	Group 2 only server general failure	This error code may only be reported by DeviceNet group 2 only servers with 4K or less code space and only in place of Service not supported, Attribute not supported and Attribute not settable.
2B-CF	---	Reserved by CIP for future extensions
D0-FF	Reserved for Object Class and service errors	This range of error codes is to be used to indicate Object Class specific errors. Use of this range should only be performed when none of the Error Codes presented in this table accurately reflect the error that was encountered.

Example of Additional Status in case that General Status Is 01 Hex. (Status of Connection Manager Object)

General Status (hex)	Additional Status (hex)	Explanation
01	0100	Connection in Use or Duplicate Forward Open.
01	0103	Transport Class and Trigger combination not supported
01	0106	Ownership Conflict
01	0107	Connection not found at target application.
01	0108	Invalid Connection Type. Indicates a problem with either the Connection Type or Priority of the Connection.
01	0109	Invalid Connection Size
01	0110	Device not configured
01	0111	RPI not supported. May also indicate problem with connection time-out multiplier, or production inhibit time.
01	0113	Connection Manager cannot support any more connections
01	0114	Either the Vendor Id or the Product Code in the key segment did not match the device
01	0115	Product Type in the key segment did not match the device
01	0116	Major or Minor Revision information in the key segment did not match the device
01	0117	Invalid Connection Point
01	0118	Invalid Configuration Format
01	0119	Connection request fails since there is no controlling connection currently open.
01	011A	Target Application cannot support any more connections
01	011B	RPI is smaller than the Production Inhibit Time.
01	0203	Connection cannot be closed since the connection has timed out
01	0204	Unconnected Send timed out waiting for a response.
01	0205	Parameter Error in Unconnected Send Service
01	0206	Message too large for Unconnected message service
01	0207	Unconnected acknowledge without reply
01	0301	No buffer memory available
01	0302	Network Bandwidth not available for data
01	0303	No Tag filters available
01	0304	Not Configured to send real-time data
01	0311	Port specified in Port Segment Not Available
01	0312	Link Address specified in Port Segment Not Available
01	0315	Invalid Segment Type or Segment Value in Path
01	0316	Path and Connection not equal in close
01	0317	Either Segment not present or Encoded Value in Network Segment is invalid.
01	0318	Link Address to Self Invalid
01	0319	Resources on Secondary Unavailable
01	031A	Connection already established
01	031B	Direct connection already established
01	031C	Miscellaneous
01	031D	Redundant connection mismatch
01	031F	No connection resources exist for target path
01	0320-07FF	Vendor specific

Priority/Time Ticks and Time Out Ticks

Format of the Priority/Time Tick

Time tick	Base value (ms)	Maximum time-out time (ms) that can be set in the time out ticks
0000 hex	1	255
0001 hex	2	510
0010 hex	4	1,020
0011 hex	8	2,040
0100 hex	16	4,080
0101 hex	32	8,160
0110 hex	64	16,320
0111 hex	128	32,640
1000 hex	256	65,280
1001 hex	512	130,560
1010 hex	1,024	261,120
1011 hex	2,048	522,240
1100 hex	4,096	1,044,480
1101 hex	8,192	2,088,960
1110 hex	16,389	4,177,920
1111 hex	32,768	8,355,840

Appendix E
FINS Commands Addressed to EtherNet/IP Units or Built-in EtherNet/IP Ports

Command Code List

Command code		Function name	Remarks
MRC	SRC		
04	03	RESET	---
05	01	CONTROLLER DATA READ	---
06	01	CONTROLLER STATUS READ	---
08	01	INTERNODE ECHO TEST	---
	02	BROADCAST TEST RESULTS READ	---
	03	BROADCAST DATA SEND	---
21	02	ERROR LOG READ	---
	03	ERROR LOG CLEAR	---
27	01	UDP OPEN REQUEST*1	---
	02	UDP RECEIVE REQUEST*1	---
	03	UDP SEND REQUEST*1	---
	04	UDP CLOSE REQUEST*1	---
	10	PASSIVE TCP OPEN REQUEST*1	---
	11	ACTIVE TCP OPEN REQUEST*1	---
	12	TCP RECEIVE REQUEST*1	---
	13	TCP SEND REQUEST*1	---
	14	TCP CLOSE REQUEST*1	---
	20	PING	---
	30	FINS/TCP CONNECTION REMOTE NODE CHANGE REQUEST	---
	31	FINS/TCP CONNECTION STATUS READ	---
	50	IP ADDRESS TABLE WRITE	---
	57	IP ADDRESS WRITE	---
	60	IP ADDRESS TABLE READ	---
	61	IP ROUTER TABLE READ	---
	62	PROTOCOL STATUS READ	---
	63	MEMORY STATUS READ*2	---
	64	SOCKET STATUS READ	---
	65	ADDRESS INFORMATION READ	---
	67	IP ADDRESS READ	---
28	01	EXPLICIT MESSAGE SEND	---
	10	CIP UCMM MESSAGE SEND	---

*1 These commands are supported by the CS1W/CJ1W-EIP21S or CJ3M-CPU3□.

*2 This command is supported by EtherNet/IP Units or built-in EtherNet/IP ports excluding the CS1W/CJ1W-EIP21S or CJ3M-CPU3□.

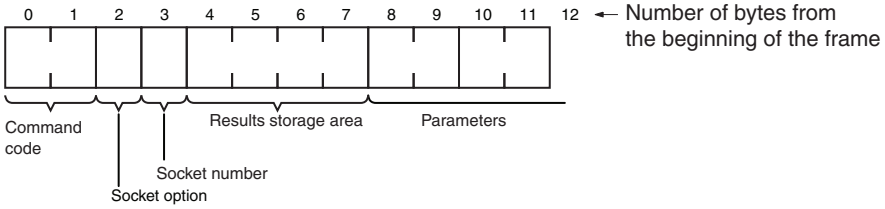
Socket Applications

The format of the following FINS commands partially differs when the sockets are used.

Command code		Name
MRC	SRC	
27	01	UDP OPEN REQUEST
	02	UDP RECEIVE REQUEST
	03	UDP SEND REQUEST
	04	UDP CLOSE REQUEST
	10	PASSIVE TCP OPEN REQUEST
	11	ACTIVE TCP OPEN REQUEST
	12	TCP RECEIVE REQUEST
	13	TCP SEND REQUEST
	14	TCP CLOSE REQUEST

Format

The basic format of these commands is shown in the diagram below.



Command Code

Specifies the requested process.

Socket Option

For the TCP OPEN REQUEST (ACTIVE or PASSIVE), specifies whether or not the keep-alive function is to be used. For all other commands it is disabled. (Set to 0).

Socket Number

Specifies the socket number for which the process is requested, from 1 to 8.

Results Storage Area

Specifies the area to store the results of the requested process.

Parameters

Specifies the parameters for the command code. Parameters depend on the command being executed; for details, refer to the following pages.

PLC Memory Areas

The memory areas of the PLC that can be specified for results storage when executing commands from the PC are listed in the table below. The *Variable type* is set in the first byte of the results storage area. The remaining three bytes contain the address for communications.

Addresses in the *Addresses for communications* column are not the same as the actual memory addresses.

Memory area	Data type		Word addresses	Addresses for communications	Variable type	Bytes
Bit Areas	Current value of word	CIO	CIO 0000 to CIO 6143	000000 to 17FF00	B0 (80)*	2
		HR	H000 to H511	000000 to 01FF00	B2	
		AR	A448 to A959	01C000 to 03BF00	B3	
DM Area		DM	D00000 to D32767	000000 to 7FFF00	82	2
EM Area		Bank 0	E0_E00000 to E0_E32767	000000 to 7FFF00	A0 (90)*	2
		Bank 1	E1_E00000 to E1_E32767	000000 to 7FFF00	A1 (91)*	
		Bank 2	E2_E00000 to E2_E32767	000000 to 7FFF00	A2 (92)*	
		Bank 3	E3_E00000 to E3_E32767	000000 to 7FFF00	A3 (93)*	
		Bank 4	E4_E00000 to E4_E32767	000000 to 7FFF00	A4 (94)*	
		Bank 5	E5_E00000 to E5_E32767	000000 to 7FFF00	A5 (95)*	
		Bank 6	E6_E00000 to E6_E32767	000000 to 7FFF00	A6 (96)*	
		Bank 7	E7_E00000 to E7_E32767	000000 to 7FFF00	A7 (97)*	
		Bank 8	E8_E00000 to E8_E32767	000000 to 7FFF00	A8	2
		Bank 9	E9_E00000 to E9_E32767	000000 to 7FFF00	A9	2
		Bank A	EA_E00000 to EA_E32767	000000 to 7FFF00	AA	2
		Bank B	EB_E00000 to EB_E32767	000000 to 7FFF00	AB	2
		Bank C	EC_E00000 to EC_E32767	000000 to 7FFF00	AC	2
		Current bank	E00000 to E32767	000000 to 7FFF00	98	2

Note The variable types (area designations) given in parentheses can also be used.

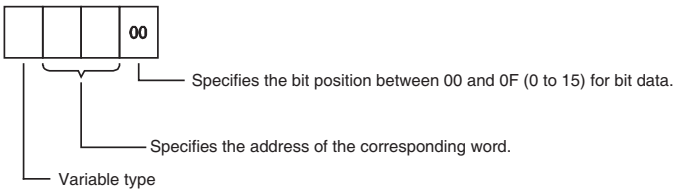
Word and Bit Addresses

Three bytes of data are used to express data memory addresses of PLCs. The most significant two bytes give the word address and the least significant byte gives the bit number between 00 and 15.

The word address combined with the bit number expresses the bit address.

Address for Communications

The three bytes of the address for communications is composed as follows.



Word addresses for specific memory area words can be calculated by converting the normal decimal word address to hexadecimal and adding it to the first word in the *Addresses for communications* column in the above table. For example, the address for communications for D00200 would be 0000 (from above table) plus C8 (decimal 200 converted to hexadecimal), or 00C8.

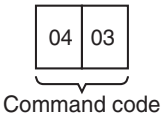
FINS Command Reference for EtherNet/IP Units or Built-in EtherNet/IP Ports

Details of the FINS commands addressed to EtherNet/IP Units and the responses are described for each command.

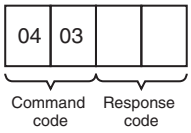
RESET

Resets the EtherNet/IP Unit or built-in EtherNet/IP port.

Command Block



Response Block



Precautions

- No response will be returned if the command ends normally. A response will be returned only if an error occurs.
- In some cases, send requests (SEND(192)/RECV(193) instructions) made from the PLC to the EtherNet/IP Unit or built-in EtherNet/IP port just before execution of the RESET command may not be executed.
- TCP ports used for CIP communications, socket services, or FTP are closed immediately before resetting.

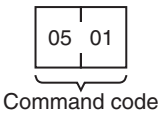
Response Codes

Response code	Description
1001	Command too large

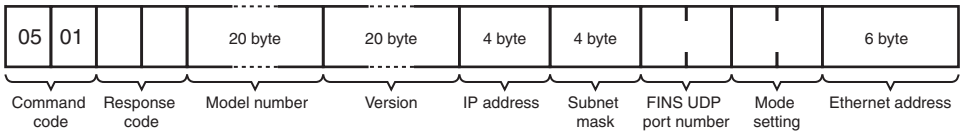
CONTROLLER DATA READ

Reads the following data from the EtherNet/IP Unit or built-in EtherNet/IP port: Model number, version, IP address, subnet mask, FINS UDP port number, mode settings, Ethernet address.

Command Block



Response Block



Parameters

Model number, Version (Response)

The model number and version of the EtherNet/IP Unit or built-in EtherNet/IP port are returned as ASCII characters occupying 20 bytes each (i.e., 20 characters each). If all bytes are not used, the remaining bytes will be all spaces (ASCII 20 Hex).

Example Model: CS1W-EIP21, CJ1W-EIP21, CJ2B-EIP21, or CJ2M-EIP21
Example Version: V2.00

The model number of the built-in EtherNet/IP port on a CJ2H-CPU□□-EIP CPU Unit is CJ2B-EIP21.

The model number of the built-in EtherNet/IP port on a CJ2M-CPU3□ CPU Unit is CJ2M-EIP21.

IP Address, Subnet Mask (Response)

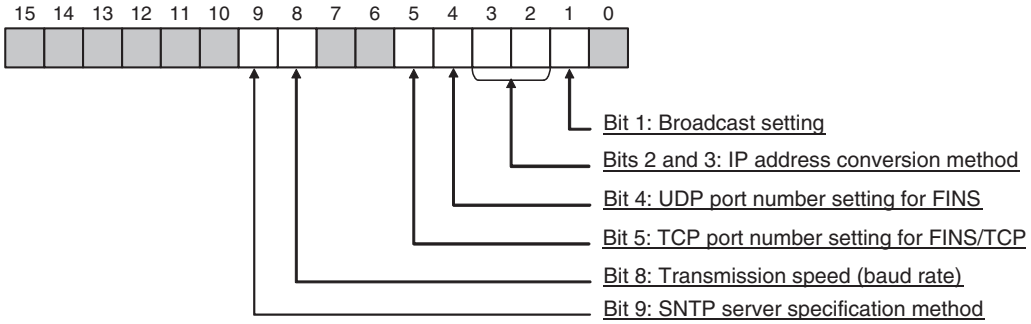
The IP address and subnet mask of the EtherNet/IP Unit or built-in EtherNet/IP port are returned as 4 bytes each.

FINS UDP Port Number (Response)

The UDP port number of the EtherNet/IP Unit or built-in EtherNet/IP port for FINS is returned as 2 bytes.

Mode Setting (Response)

The mode setting in the system setup is returned.



Broadcast Address Setting

Bit 1	Meaning
0	Broadcast with host number set to all ones (4.3BSD specifications)
1	Broadcast with host number set to all zeroes (4.2BSD specifications)

Communications Partner IP Address Conversion Method Setting

Bit 3	Bit 2	Meaning
0	0	Automatic generation method (dynamic)
0	1	Automatic generation method (static)
1	0	IP address table reference method
1	1	Combined method (IP address table reference + automatic generation (dynamic))

FINS/UDP Port Number Setting

Bit 4	Meaning
0	Default (9600)
1	Unit Setup value

FINS/TCP Port Number Setting

Bit 5	Meaning
0	Default (9600)
1	Unit Setup value

Baud Rate Setting

Bit 8	Meaning
0	Automatic detection
1	100BASE-TX or 10BASE-T

SNTP Server Specification Method

Bit 9	Meaning
0	IP address
1	Host name

Ethernet Address (Response)

The Ethernet address of the EtherNet/IP Unit or built-in EtherNet/IP port is returned.

Note This Ethernet address is listed on the label on the side of the EtherNet/IP Unit or (for a built-in EtherNet/IP port), on the CPU Unit.

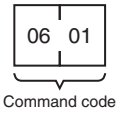
Response Codes

Response code	Description
0000	Normal end
1001	Command too large

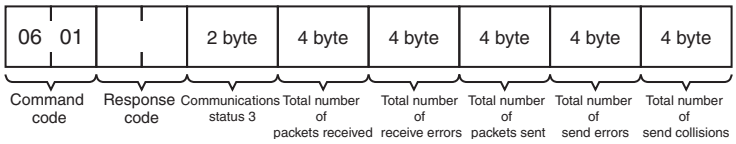
CONTROLLER STATUS READ

Reads the controller status.

Command Block

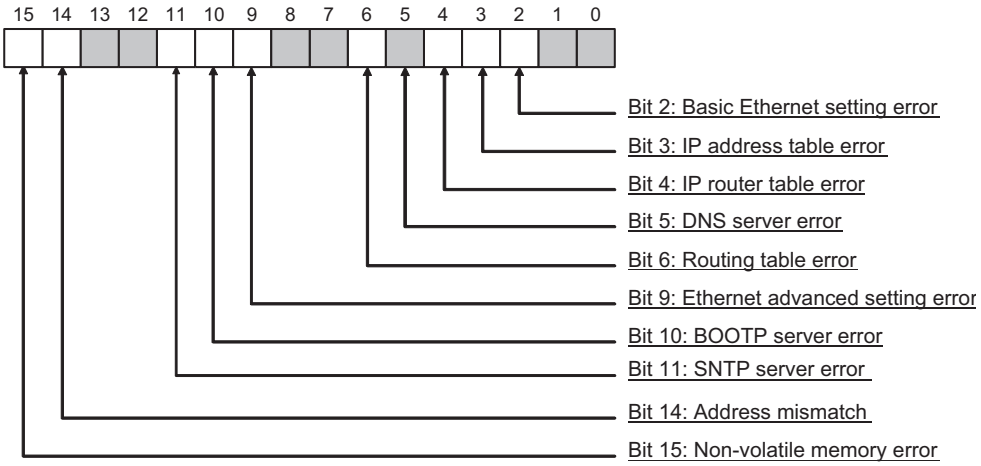


Response Block



Parameters

Communications Status 3 (Response)



Basic Ethernet Setting Error

Bit 2	Meaning
0	No error
1	An error (such as an invalid IP address) was detected during the validity check of parameters related to the TCP/IP Interface Object and Ether Link Object.

IP Address Table Error

Bit 3	Meaning
0	No error
1	Error detected (More than 32 records, invalid IP address, or invalid FINS node address).

IP Router Table Error

Bit 4	Meaning
0	No error
1	Error detected (More than 8 records, or invalid IP address).

DNS Server Error

Bit 5	Meaning
0	No error
1	Error detected (The IP address setting of the DNS server is not correct, or a time-out occurred during communications with the DNS server.)

Routing Table Error

Bit 6	Meaning
0	No error
1	Error detected in routing table check.

Ethernet Advanced Setting Error

Bit 9	Meaning
0	No error
1	An error was detected during the validity check of vendor-specific parameters for the TCP/IP Interface Object and Ether Link Object.

BOOTP Server Error

Bit 10	Meaning
0	No error
1	Error detected. (A time-out occurred during communications with the BOOTP server).

SNTP Server Error

Bit 10	Meaning
0	No error
1	Error detected. (The setting of the host specification (IP address or host name) of the SNTP server is not correct, or communications with the SNTP server timed out.)

Address Mismatch

Bit 14	Meaning
0	No error
1	Error detected. (The address conversion method was set for automatic generation, but the host ID of the local IP address does not match the local node address (FINS node address).

Non-volatile Memory Error

Bit 15	Meaning
0	No error
1	Error detected. (The non-volatile memory's service life has expired, or the memory has failed).

Total Number of Packets Received (Response)

The total number of packets received by the EtherNet/IP Unit or built-in EtherNet/IP port is returned.

Total Number of Receive Errors (Response)

The total number of packet errors detected while the EtherNet/IP Unit or built-in EtherNet/IP port was receiving is returned.
The following types of error are detected:

- Short packet errors
- Alignment errors
- CRC errors
- Frame length errors (received frame: 1,515 bytes or more)
- Communications controller overflow errors

Total Number of Packets Sent (Response)

The total number of packets sent by the EtherNet/IP Unit or built-in EtherNet/IP port is returned.

Total Number of Errors Sent (Response)

The total number of packet errors detected while the EtherNet/IP Unit or built-in EtherNet/IP port was sending is returned.

Total Number of Send Collisions (Response)

Returns the number of packets damaged by 16 collisions with data from other nodes during EtherNet/IP Unit or built-in EtherNet/IP port transmissions.

Precautions

Counting of the total number of packets received, total number of receive errors, total number of packets sent, total number of errors sent, and total number of send collisions is discontinued when the counted value reaches the maximum value.

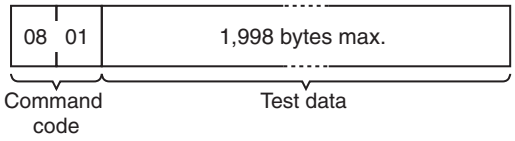
Response Codes

Response code	Description
0000	Normal end
1001	Command too large

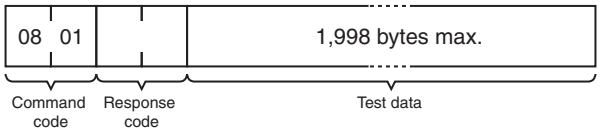
INTERNODE ECHO TEST

Performs an echoback test (internode communications test) between specified nodes.

Command Block



Response Block



Parameters

Test Data (Command, Response)

This command specifies the data to be sent to the specified nodes. Up to 1,998 bytes can be specified. The response sends back data identical to the data specified in the command. An abnormality is assumed if the data returned in the response differs from the test data sent.

Precautions

- The test destination node is the destination node specified in the CMND instruction operands.
- Always specify the unit address of the EtherNet/IP Unit or built-in EtherNet/IP port in the CMND instruction.

Response Codes

Response code	Description
0000	Normal end
1001	Command too large
1002	Command too small (No test data)

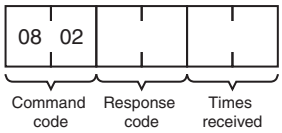
BROADCAST TEST RESULTS READ

Reads the results (number of times data received) of the broadcast test.

Command Block



Response Block



Parameters

Times Received (Response)

The number of times the data has been received normally during the broadcast send test is returned as a hexadecimal number. The number of times received is cleared each time the result is read.

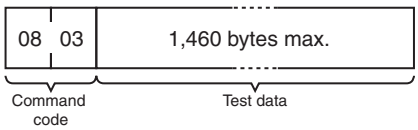
Response Codes

Response code	Description
0000	Normal end
1001	Command too large

BROADCAST DATA SEND

Sends test data simultaneously to all nodes on the network.

Command Block



Parameters

Test Data (Command)

This command specifies the data to be sent to the specified nodes. Up to 1,460 bytes can be specified.

Precautions

- No response is made to this command.
- When using this command, set the FINS header parameters (or the control data for the CMND instruction) as follows:

  Destination node address:FF (broadcast data)

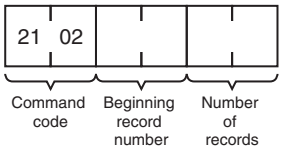
  Destination unit address:FE (EtherNet/IP Unit or built-in EtherNet/IP port)

  Response/no response flag:1 (no response)

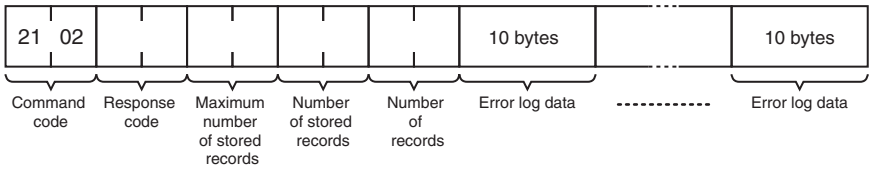
ERROR LOG READ

Reads the error log.

Command Block



Response Block



Parameters

Beginning Record Number (Command)

The first record to be read. The first record number can be specified in the range between 0000 and 003F (0 to 63 decimal) where 0000 is the oldest record.

Number of Records (Command, Response)

The number of records to read is specified between 0001 and 0040 (1 to 64 decimal) in the command. The response returns the actual number of records read.

Maximum Number of Stored Records (Response)

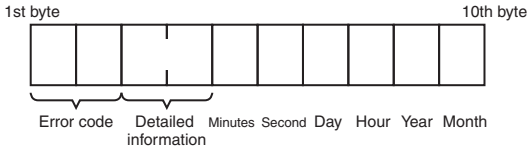
Indicates the maximum number of records that can be stored in the error log. The maximum number of error log records depends on the model of CPU Unit or CPU Bus Unit being used. In an EtherNet/IP Unit or built-in EtherNet/IP port, the maximum number of stored records is fixed at 40 (64 decimal).

Number of Stored Records (Response)

The number of records stored at the time the command is executed is returned.

Error Log Data (Response)

The specified number of error log records from the beginning record number is returned sequentially. The total number of bytes in the error log is calculated as the number of records x 10 bytes/record. Each error log record thus comprises 10 bytes, configured as follows:



Error Code, Detailed Information

Details of the error stored in the record. Refer to *18-4-4 Error Log Error Codes* for details.

Minute, Second, Day, Hour, Year, Month

Indicate the time at which the error stored in the record occurred.

Precautions

- If the error log contains fewer records than the number specified in the number of records parameter, all records stored in the error log at the time the command is executed will be returned and the command executed will end normally.

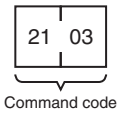
Response Codes

Response code	Description
0000	Normal end
1001	Command too large
1002	Command too small
1103	Beginning record number is out of range
110C	The number of read records is 0.

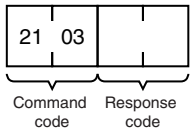
ERROR LOG CLEAR

Clears the error log for the EtherNet/IP Unit or built-in EtherNet/IP ports, and resets the *number of stored records* to 0.

Command Block



Response Block



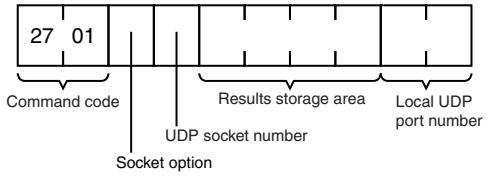
Response Codes

Response code	Description
0000	Normal end
1001	Command too large

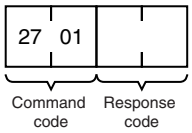
UDP OPEN REQUEST

Requests processing to open a socket.

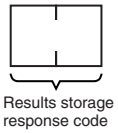
Command Block



Response Block



Results Storage Format



Parameters

Socket Option (Command)

The socket option specified as 1 byte. The setting is not valid for this command. Set to 0.

UDP Socket Number (Command)

The UDP socket number to be opened specified as 1 byte between 1 and 8.

Results Storage Area (Command)

The area in which the results of the command execution are stored. The first byte specifies the memory area and data type (variable type). The 2nd to 4th bytes specify the beginning address of the results storage area. Refer to *PLC Memory Areas* in *Socket Applications* for details about the variable types and addresses that can be specified.

Local UDP Port Number (Command)

The UDP port number for communications with the socket is specified as 2 bytes (0 cannot be specified). Packets received at this port are distributed to the socket specified in the UDP socket number, and send packets are distributed from the UDP socket to this port.

The following ports for the CS1W/CJ1W-EIP21S EtherNet/IP Unit's communications services cannot be specified.

- UDP port No. used for FINS (Default: 9600)
- UDP port No. used for DNS server access (Default: 53)
- UDP port No. used for SNTP server access (Default: 123)

Response Codes

Response code	Description
0000	Normal
0105	Local IP address setting error
0302	CPU Unit error; execution not possible.
1001	Command too large
1002	Command too small.
1100	UDP socket number is out of range. Local UDP port number is 0.
1101	The variable type for the results storage area is out of range.
1103	Non-zero bit address specified for the results storage area.
220F	Specified socket is already open or is being closed.
2211	High traffic at Unit; cannot execute service.
2240	Mode is incorrect; cannot execute service. (The high-speed socket service option was enabled and a socket service was used with a CMND(490) instruction.) Or, the socket service was executed with a CMND(490) instruction when the layout type of the allocated CIO Area words is set to *Default*.

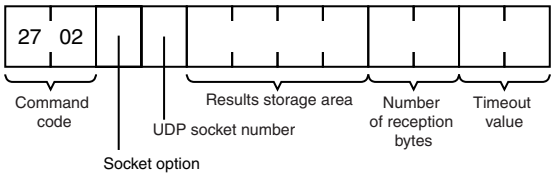
Results Storage Area Response Codes

Response code	Description
0000	Normal
003E	Internal buffer cannot be reserved due to high receive load (ENOBUFS).
0049	Duplicate UDP port number (EADDRINUSE).

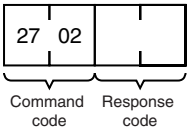
UDP RECEIVE REQUEST

Requests that data be sent from a UDP socket.

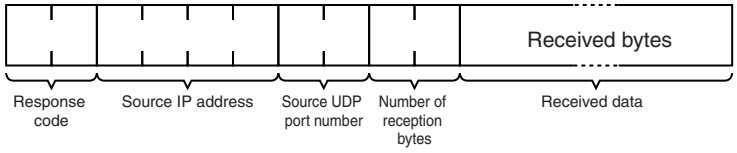
Command Block



Response Block



Results Storage Format



Parameters

Socket Option (Command)

The socket option specified as 1 byte. The setting is not valid for this command. Set to 0.

UDP Socket Number (Command)

The UDP socket number to receive data specified as 1 byte between 1 and 8.

Results Storage Area (Command)

The area in which the results of the command execution are stored. The first byte specifies the memory area and data type (variable type). The 2nd to 4th bytes specify the beginning address of the results storage area. Refer to *PLC Memory Areas* in *Socket Applications* for details about the variable types and addresses that can be specified.

Number of Reception Bytes (Command, Results Storage Area)

The maximum number of bytes of data to be received is given in the command. The number of bytes of data received will be stored in the results storage area. Up to 1,984 bytes can be specified.

Timeout Value (Command)

The maximum control time between receiving the receive request and storing the result. If this set time limit is exceeded, the code for a timeout error will be set as the results storage response code. The value is set in units of 0.1 s. The timeout time will be unlimited if the value is set to 0.

Source IP Address (Results Storage Area)

The IP address of the node sending data is stored in hexadecimal.

Source UDP Port Number (Results Storage Area)

The port number of the node sending data.

Received Data (Results Storage Area)

The data sent from the remote node.

Precautions

If a packet is received which contains more bytes than the number specified in *Number of reception bytes* specified in the command, the specified number of bytes will be stored and the remainder of the bytes will be discarded.

Response Codes

Response code	Description
0000	Normal
0105	IP address setting error
0302	CPU Unit error; execution not possible.
1001	Command too large
1002	Command too small
1100	UDP socket number or number of reception bytes is out of range.
1101	The variable type for the results storage area is out of range.
1103	Non-zero bit address specified for the results storage area.
220F	The specified socket is currently receiving data.
2210	The specified socket is not open.
2211	High traffic at Unit; cannot execute service.
2240	Mode is incorrect; cannot execute service. (The high-speed socket service option was enabled and a socket service was used with a CMND(490) instruction.) Or, the socket service was executed with a CMND(490) instruction when the layout type of the allocated CIO Area words is set to *Default*.

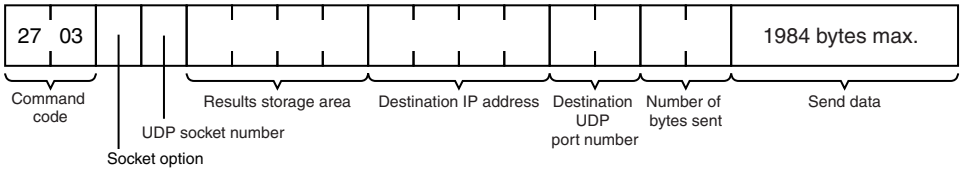
Results Storage Area Response Codes

Response code	Description
0000	Normal
003E	Internal buffer cannot be reserved due to high reception load (ENOBUFS).
0066	Internal memory cannot be allocated; cannot execute service.
0080	A receive request timeout error occurred.
0081	The specified socket was closed while receiving data.

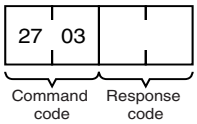
UDP SEND REQUEST

Requests that data be received by a UDP socket.

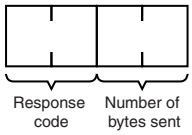
Command Block



Response Block



Results Storage Format



Parameters

Socket Option (Command)

The socket option specified as 1 byte. The setting is not valid for this command. Set to 0.

UDP Socket Number (Command)

The UDP socket number to send the data specified as 1 byte between 1 and 8.

Results Storage Area (Command)

The area in which the result of the command execution is stored. The first byte specifies the memory area and data type (variable type). The 2nd to 4th bytes specify the beginning address of the results storage area. Refer to *PLC Memory Areas* in *Socket Applications* for details about the variable types and addresses that can be specified.

Destination IP Address (Command)

The IP address of the node to which data is being sent is specified in hexadecimal.

Destination UDP Port Number (Command)

The UDP port number of the node to which data is being sent.

Number of Bytes Sent (Command, Results Storage Area)

The number of bytes in the data sent by this command. Up to 1,984 bytes can be specified, or up to 1,472 bytes can be specified if the broadcast address is specified as the send destination. The results storage area stores the actual number of bytes sent.

Send Data (Command)

Specifies the data sent to the remote node.

Response Codes

Response code	Description
0000	Normal
0105	Local IP address setting error
0302	CPU Unit error; execution not possible.
1002	Command too small
1003	The number of bytes sent does not match the sent data length.
1100	UDP socket number or number of bytes sent is out of range. The destination IP address is 0. Local UDP port number is 0.
1101	The variable type for the results storage area is out of range.
1103	Non-zero bit address specified for the results storage area.
220F	Specified socket is currently sending.
2210	The specified socket is not open.
2211	High traffic at Unit; cannot execute service.
2240	Mode is incorrect; cannot execute service. (The high-speed socket service option was enabled and a socket service was used with a CMND(490) instruction.) Or, the socket service was executed with a CMND(490) instruction when the layout type of the allocated CIO Area words is set to *Default*.

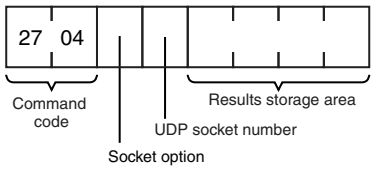
Results Storage Area Response Codes

Response code	Description
0000	Normal
003E	Internal buffer cannot be reserved due to high reception load (ENOBUFS).
0042	The send destination IP address is a broadcast address and the number of bytes sent exceeds 1,472. (EMSGSIZE)
004C	Incorrect network number. Incorrect destination IP address (EADDRNOTAVAIL).
004E	Incorrect destination IP address (ENETUNREACH). No network number in IP router table. Router incorrectly set.
0051	Router incorrectly specified. Incorrect destination IP address (EHOSTUNREACH).

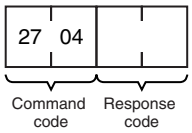
UDP CLOSE REQUEST

Requests processing to close a socket.

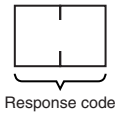
Command Block



Response Block



Results Storage Format



Parameters

Socket Option (Command)

The socket option specified as 1 byte. The setting is not valid for this command. Set to 0.

UDP Socket Number (Command)

The UDP socket number to be closed specified as 1 byte between 1 and 8.

Results Storage Area (Command)

The area in which the results of the command execution are stored. The first byte specifies the memory area and data type (variable type). The 2nd to 4th bytes specify the beginning address of the results storage area. Refer to *PLC Memory Areas* in *Socket Applications* for details about the variable types and addresses that can be specified.

Response Codes

Response code	Description
0000	Normal
0105	Local IP address setting error
0302	CPU Unit error; execution not possible.
1001	Command too large
1002	Command too small
1100	UDP socket number is out of range.
1101	The variable type for the results storage area is out of range.
1103	Non-zero bit address specified for the results storage area.
2210	Specified socket is not open.
2211	High traffic at Unit; cannot execute service.
2240	Mode is incorrect; cannot execute service. (The high-speed socket service option was enabled and a socket service was used with a CMND(490) instruction.) Or, the socket service was executed with a CMND(490) instruction when the layout type of the allocated CIO Area words is set to *Default*.

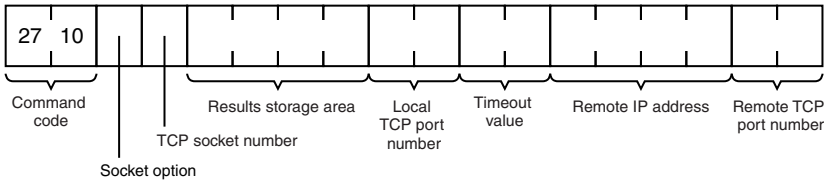
Results Storage Area Response Codes

Response code	Description
0000	Normal

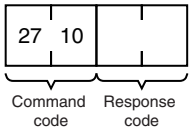
PASSIVE TCP OPEN REQUEST

Requests processing to open a TCP socket. The socket will wait to be connected to another node.

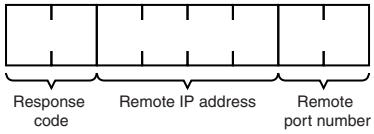
Command Block



Response Block



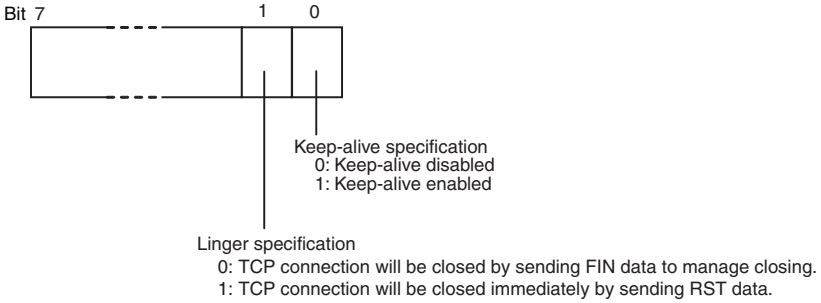
Results Storage Format



Parameters

Socket Option (Command)

The socket option is specified in one byte.



Note (1) If the linger option is not specified and a TCP connection is closed, FIN data will be sent and then approximately 1 minute will be used to confirm the transmission and perform other closing management with the remote node. Therefore, it may not be possible to immediately use TCP sockets with the same port number.

(2) In contrast, when the linger option is specified, RST data will be sent when TCP is closed, and closing will be performed immediately. This enables immediately opening TCP sockets with the same port number. Data that was sent immediately before closing, however, is not checked for transmission to the remote node. If the linger option is specified, ensure the arrival of the send data in the application.

TCP Socket Number (Command)

The TCP socket number to be opened specified as 1 byte between 1 and 8.

Results Storage Area (Command)

The area in which the results of the command execution are stored. The first byte specifies the memory area and data type (variable type). The 2nd to 4th bytes specify the beginning address of the results storage area. Refer to *PLC Memory Areas* in *Socket Applications* for details about the variable types and addresses that can be specified.

Local TCP Port Number (Command)

The TCP port number for communications with the socket is specified as 2 bytes (0 cannot be specified).

The following ports used for the CS1W/CJ1W-EIP21S/CJ3M-CPU3□'s communications services cannot be specified.

- TCP port No. used for FTP server (Default: 20, 21)
- TCP port No. used for DNS server access (Default: 53)

Timeout Value (Command)

The maximum control time between receiving the open request and storing the result. If this set time limit is exceeded, the code for a timeout error will be set as the results storage response code. The value is set in units of 0.1 s. The timeout time is unlimited if the value is set to 0.

Remote IP Address (Command, Results Storage Area)

Specify the remote node's IP address. If all zeroes are set, no remote node is specified and connection is awaited from any node. If any other value is set, connection is awaited from the specified remote node. The IP address of the connected remote node will be stored in the results storage area.

Remote Port Number (Command, Results Storage Area)

Specify the remote TCP port number with this command. If all zeroes are set, no remote TCP port number is specified. If any other value is set, it specifies the TCP port number of the remote node. The TCP port number of the connected remote node will be stored in the results storage area.

Precautions

Processing varies as shown in the table below according to the specified combination of remote IP address and remote TCP port number.

Remote IP address	Remote TCP port	Description
0	0	All connection requests received
0	Not 0	Received only when port number matches.
Not 0	0	Received only when IP address matches.
Not 0	Not 0	Received only when IP address and port number matches.

Response Codes

Response code	Description
0000	Normal
0105	Local IP address setting error
0302	CPU Unit error; execution not possible.
1001	Command too large
1002	Command too small
1100	TCP socket number is out of range. Local TCP port number is 0.
1101	The variable type for the results storage area is out of range.
1103	Non-zero bit address specified for the results storage area.
220F	The specified socket (connection) is already open or is currently being opened.
2211	High traffic at Unit; cannot execute service.
2240	Mode is incorrect; cannot execute service. (The high-speed socket service option was enabled and a socket service was used with a CMND(490) instruction.) Or, the socket service was executed with a CMND(490) instruction when the layout type of the allocated CIO Area words is set to *Default*.

Results Storage Area Response Codes

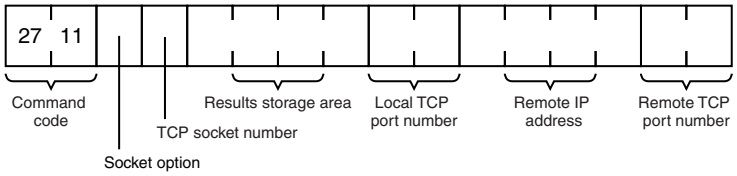
Response code	Description
0000	Normal
003E	Internal buffer cannot be reserved due to high reception load (ENOBUFS).
0042 (see note)	An error occurred (EMSGSIZE).
0045	A communication error occurred with the remote node (ECONNABORTED).
0049	Duplicated port numbers (EADDRINUSE).
004A (see note)	An error occurred (ECONNREFUSED).
004B (see note)	A communication error occurred with the remote node (ECONNRESET).
004E (see note)	A parameter error occurred at the remote IP address (ENETUNREACH).
0051 (see note)	A parameter error occurred at the remote IP address (EHOSTUNREACH).
0053	A communication error occurred with the remote node (ETIMEDOUT). No remote exists.
0066	Internal memory cannot be allocated; cannot execute service.
0080	An open request timeout error occurred.
0081	Socket was closed during opening procedure.
0082	Connection could not be established with the specified remote.

Note These errors occur only in large multilayered networks.

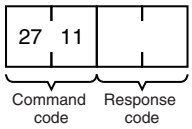
ACTIVE TCP OPEN REQUEST

Requests processing to open a TCP socket. The socket will be connected to another node.

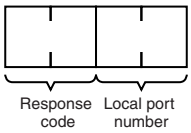
Command Block



Response Block



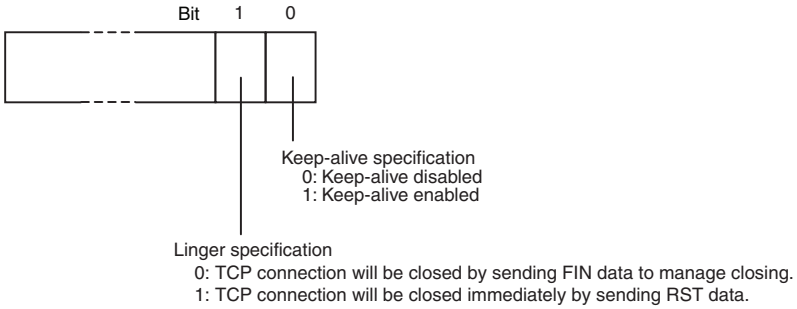
Results Storage Format



Parameters

Socket Option (Command)

The socket option is specified in one byte.



Note (1) If the linger option is not specified and a TCP connection is closed, FIN data will be sent and then approximately 1 minute will be used to confirm the transmission and perform other closing management with the remote node. Therefore, it may not be possible to immediately use TCP sockets with the same port number.

(2) In contrast, when the linger option is specified, RST data will be sent when TCP is closed, and closing will be performed immediately. This enables immediately opening TCP sockets with the same port number. Data that was sent immediately before closing, however, is not checked for transmission to the remote node. If the linger option is specified, ensure the arrival of the send data in the application.

TCP Socket Number (Command)

The TCP socket number to be opened specified as 1 byte between 1 and 8.

Results Storage Area (Command)

The area in which the results of the command execution are stored. The first byte specifies the memory area and data type (variable type). The 2nd to 4th bytes specify the beginning address of the results storage area. Refer to *PLC Memory Areas* in *Socket Applications* for details about the variable types and addresses that can be specified.

Local TCP Port Number (Command, Results Storage Area)

The TCP port number for communications with the socket is specified as 2 bytes. An available TCP port number is automatically assigned if 0 is specified.

The TCP port numbers allocated to the open socket are stored in the Results Storage Area.

The following ports used for the CS1W/CJ1W-EIP21S/CJ3M-CPU3□'s communications services cannot be specified.

- TCP port No. used for FTP server (Default: 20, 21)
- TCP port No. used for DNS server access (Default: 53)

Remote IP Address (Command)

Specify the remote node's IP address (must be non-zero) in hexadecimal.

Remote Port Number (Command)

Specify the remote TCP port number (must be non-zero).

Response Codes

Response code	Description
0000	Normal
0105	Local IP address setting error
0302	CPU Unit error; execution not possible.
1001	Command too large
1002	Command too small
1100	TCP socket number is out of range. Remote IP address or the remote TCP port number is 0.
1101	The variable type for the results storage area is out of range.
1103	Non-zero bit address specified for the results storage area.
220F	The specified socket (connection) is already open or is being opened.
2211	High traffic at Unit; cannot execute service.
2240	Mode is incorrect; cannot execute service. (The high-speed socket service option was enabled and a socket service was used with a CMND(490) instruction.) Or, the socket service was executed with a CMND(490) instruction when the layout type of the allocated CIO Area words is set to *Default*.

Results Storage Area Response Codes

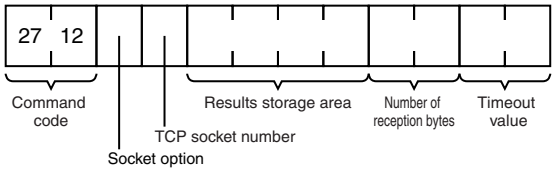
Response code	Description
0000	Normal
000D	A parameter error occurred at the remote IP address (EACCES).
003E	Internal buffer cannot be reserved due to high receive load (ENOBUFS).
0042 (see note)	An error occurred (EMSGSIZE).
0044	Received ICMP data (ENOPROTOOPT).
0045	Local socket closed (ECONNABORTED).
0049	Duplicated port numbers (EADDRINUSE).
004A	An error occurred (ECONNREFUSED). Passive remote is not available.
004B (see note)	A communication error occurred with the remote node (ECONNRESET).
004C	A parameter error occurred at the remote IP address (EADDRNOTAVAIL). A parameter was specified incorrectly. An attempt was made to actively open local TCP port.
004E	Remote IP address parameter error (ENETUNREACH). The network ID is not in the IP router table or router settings are incorrect.
0051	A parameter error occurred at the remote IP address (EHOSTUNREACH). Incorrect router setting.
0053	A communication error occurred with the remote node (ETIMEDOUT). No remote exists.
0081	Socket was closed during opening procedure.

Note These errors occur only in large multilayered networks.

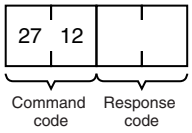
TCP RECEIVE REQUEST

Requests that data be sent from a TCP socket.

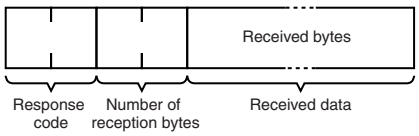
Command Block



Response Block



Results Storage Format



Parameters

Socket Option (Command)

The socket option specified as 1 byte. The setting is not valid for this command. Set to 0.

TCP Socket Number (Command)

The TCP socket number to receive data specified as 1 byte between 1 and 8.

Results Storage Area (Command)

The area in which the results of the command execution are stored. The first byte specifies the memory area and data type (variable type). The 2nd to 4th bytes specify the beginning address of the results storage area. Refer to *PLC Memory Areas* in *Socket Applications* for details about the variable types and addresses that can be specified.

Number of Reception Bytes (Command, Results Storage Area)

The maximum number of bytes of data to be received is given in the command. The number of bytes of data received will be stored in the results storage area. Up to 1,984 bytes can be specified.

Timeout Value (Command)

The maximum control time between receiving the receive request and storing the result. If this set time limit is exceeded, the code for a timeout error will be set as the results storage response code. The value is set in units of 0.1 s. The timeout time is unlimited if the value is set to 0.

Received Data (Results Storage Area)

Stores the received data.

Response Codes

Response code	Description
0000	Normal
0105	Local IP address setting error
0302	CPU Unit error; execution not possible.
1001	Command too large
1002	Command too small
1100	TCP socket number or number of reception bytes is out of range.
1101	The variable type for the results storage area is out of range.
1103	Non-zero bit address specified for the results storage area.
220F	The specified socket is receiving data.
2210	No connection could be established to the specified socket.
2211	High traffic at Unit; cannot execute service.
2240	Mode is incorrect; cannot execute service. (The high-speed socket service option was enabled and a socket service was used with a CMND(490) instruction.) Or, the socket service was executed with a CMND(490) instruction when the layout type of the allocated CIO Area words is set to *Default*.

Results Storage Area Response Codes

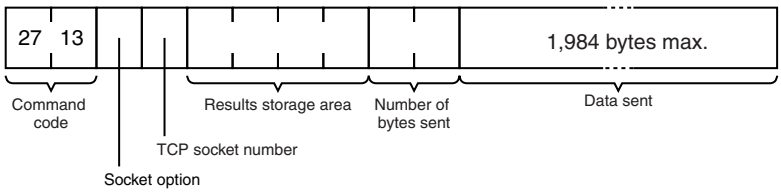
Response code	Description
0000	Normal
003E	Internal buffer cannot be reserved due to high receive load (ENOBUFS).
0042 (see note)	Received ICMP data (EMSGSIZE).
0044 (see note)	Received ICMP data (ENOPROTOOPT).
0045 (see note)	A communication error occurred with the remote node (ECONNABORTED).
004A (see note)	An error occurred (ECONNREFUSED).
004B	A communication error occurred with the remote node (ECONNRESET).
004E (see note)	Received ICMP data (ENETUNREACH).
004F (see note)	Received ICMP data (EHOSTDOWN).
0051 (see note)	Received ICMP data (EHOSTUNREACH).
0053	A communications error occurred with the remote node.
0066	Internal memory cannot be allocated; cannot execute service.
0080	A receive request timeout error occurred.
0081	Socket was closed while receiving.

Note These errors occur only in large multilayered networks.

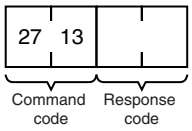
TCP SEND REQUEST

Requests that data be received at a TCP socket.

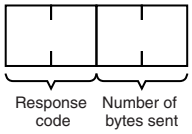
Command Block



Response Block



Results Storage Format



Parameters

Socket Option (Command)

The socket option specified as 1 byte. The setting is not valid for this command. Set to 0.

TCP Socket Number (Command)

The TCP socket number to send the data specified as 1 byte between 1 and 8.

Results Storage Area (Command)

The area in which the results of the command execution are stored. The first byte specifies the memory area and data type (variable type). The 2nd to 4th bytes specify the beginning address of the results storage area. Refer to *PLC Memory Areas* in *Socket Applications* for details about the variable types and addresses that can be specified.

Number of Bytes Sent (Command, Results Storage Area)

The number of bytes in the data sent specified between 0 and 1,984. The results storage area stores the actual number of bytes sent.

Data Sent (Command)

Specifies the data to be sent.

Response Codes

Response code	Description
0000	Normal
0105	Local IP address setting error
0302	CPU Unit error; execution not possible.
1002	Command too small
1003	The number of bytes sent does not match the amount of data.
1100	The TCP socket number or number of bytes sent is out of range.
1101	The variable type for the results storage area is out of range.
1103	Non-zero bit address specified for the results storage area.
220F	The specified socket is sending data.
2210	No connection could be established to the specified socket.
2211	High traffic at Unit; cannot execute service.
2240	Mode is incorrect; cannot execute service. (The high-speed socket service option was enabled and a socket service was used with a CMND(490) instruction.) Or, the socket service was executed with a CMND(490) instruction when the layout type of the allocated CIO Area words is set to *Default*.

Results Storage Area Response Codes

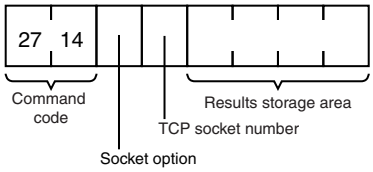
Response code	Description
0000	Normal
0020	Connection to the remote socket was broken during transmission (EPIPE).
003E	Internal buffer cannot be reserved due to high receive load (ENOBUFS).
0042 (see note)	An error occurred (EMSGSIZE).
0044 (see note)	Received ICMP data (ENOPROTOOPT).
0045 (see note)	A communication error occurred with the remote node (ECONNABORTED).
004A (see note)	An error occurred (ECONNREFUSED).
004B (see note)	A communication error occurred with the remote node (ECONNRESET).
004E (see note)	A parameter error occurred at the remote IP address (ENETUNREACH).
004F (see note)	Received ICMP data (EHOSTDOWN).
0051 (see note)	A parameter error occurred at the remote IP address (EHOSTUNREACH).
0053 (see note)	A communication error occurred with the remote node (ETIMEDOUT).
0081	The specified socket was closed during transmission.

Note These errors occur only in large multilayered networks.

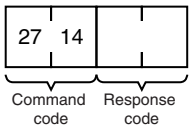
TCP CLOSE REQUEST

Requests processing to close a TCP socket. Other processing being carried out is forcibly ended and a code is recorded in the results storage area.

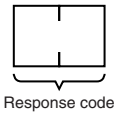
Command Block



Response Block



Results Storage Format



Parameters

Socket Option (Command)

The socket option specified as 1 byte. The setting is not valid for this command. Set to 0.

TCP Socket Number (Command)

The TCP socket number to be closed specified as 1 byte between 1 and 8.

Results Storage Area (Command)

The area in which the results of the command execution are stored. The first byte specifies the memory area and data type (variable type). The 2nd to 4th bytes specify the beginning address of the results storage area. Refer to *PLC Memory Areas* in *Socket Applications* for details about the variable types and addresses that can be specified.

Precautions

Any other processing, such as sending or receiving data, being carried out when this close command is executed will be forcibly ended and a code will be stored in the results storage area to indicate that this processing was forcibly ended.

Response Codes

Response code	Description
0000	Normal
0105	Local IP address setting error
0302	CPU Unit error; execution not possible.
1001	Command too large
1002	Command too small
1100	The TCP socket number is out of range.
1101	The variable type for the results storage area is out of range.
1103	Non-zero bit address specified for the results storage area.
2210	No connection could be established to the specified socket.
2211	High traffic at Unit; cannot execute service.
2240	Mode is incorrect; cannot execute service. (The high-speed socket service option was enabled and a socket service was used with a CMND(490) instruction.) Or, the socket service was executed with a CMND(490) instruction when the layout type of the allocated CIO Area words is set to *Default*.

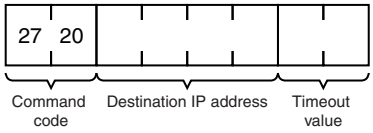
Results Storage Area Response Codes

Response code	Description
0000	Normal

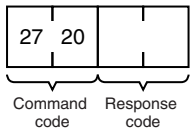
PING

Performs processing equivalent to a UNIX computer's PING command (see below).

Command Block



Response Block



Parameters

Destination IP Address (Command)

The IP address (in hexadecimal) of the destination node for the PING command echo request packet.

Timeout Value (Command)

The wait time for the echo reply packet. The value is set in seconds. The timeout time is set at 20 seconds if the value is specified as 0. If the echo reply packet is not received within the set time limit, the code for a time-out error will be set as the results storage response code.

Remarks

PING Command

The PING command runs the echoback test using the ICMP protocol. When the PING command is executed, an echo request packet is sent to the remote node ICMP. Correct communications are confirmed when the returned response packet is received normally. The echo reply packet is automatically returned by the remote node ICMP.

Response Codes

Response code	Description
0000	Normal end (echo reply received from the remote node)
0205	Timeout error
1001	Command too large
1002	Command too small
1100	Zero destination address
220F	PING command currently being executed
2211	High traffic at Unit; cannot execute service.

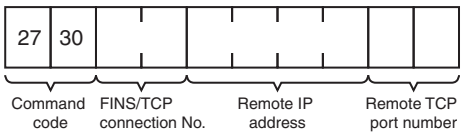
FINS/TCP CONNECTION REMOTE NODE CHANGE REQUEST

Requests a remote node change for the FINS/TCP connection.

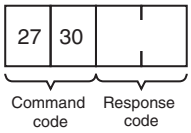
The default destination IP address in a connection in which the EtherNet/IP Unit or built-in EtherNet/IP port is used as a client is the destination IP address set under the FINS/TCP Tab Page in the Unit Setup. By sending this command to the EtherNet/IP Unit or built-in EtherNet/IP port, the destination IP address for the specified connection can be changed to another IP address.

Remote node changes can be made only for connection numbers specified as FINS/TCP clients in the Unit Setup.

Command Block



Response Block



Parameters

FINS/TCP Connection No. (Command)

Specifies, in two bytes, the FINS/TCP connection number (1 to 16) for which the change is to be made.

Remote IP Address (Command)

Specifies the remote node's IP address (must be non-zero) in hexadecimal.

Remote Port Number (Command)

Specifies the remote TCP port number (must be non-zero) with this command.

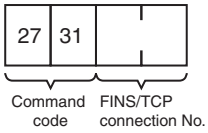
Response Codes

Response code	Description
0000	Normal end
0105	Node address setting error Local IP address setting error
0302	CPU Unit error; execution not possible.
1001	Command too large
1002	Command too small
1100	Connection number not set from 1 to 16 Remote IP address set to 0 Remote TCP port number set to 0
2230	Connection already established with specified remote node
2231	Specified connection number not set as FINS/TCP client in Unit Setup
2232	Remote node change processing for specified connection number aborted because change request received during processing

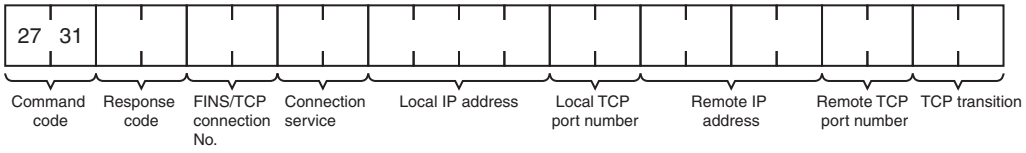
FINS/TCP CONNECTION STATUS READ

Reads the FINS/TCP connection status.

Command Block



Response Block



Parameters

FINS/TCP Connection No. (Command, Response)

Command: Specifies, in two bytes, the FINS/TCP connection number (1 to 16) for which the status is to be read.

Response: Specifies the FINS/TCP connection number (1 to 16) for which the status was read.

Connection Service (Response)

Specifies the service that is being used for the FINS/TCP connection as a number.

0003: FINS/TCP server

0004: FINS/TCP client

Local IP Address (Response)

Specifies the IP address for the local node in hexadecimal.

Local TCP Port Number (Response)

Specifies the TCP port number for the local node.

Remote IP Address (Response)

Specifies the IP address for the remote node in hexadecimal.

Remote TCP Port Number (Response)

Specifies the TCP port number for the remote node.

TCP Transitions (Response)

Specifies the TCP connection status using the following numbers.

For details on TCP status changes, refer to *Appendix C TCP Status Transitions*.

Number	Status	Meaning
00000000	CLOSED	Connection closed.
00000001	LISTEN	Waiting for connection.
00000002	SYN SENT	SYN sent in active status.
00000003	SYN RECEIVED	SYN received and sent.
00000004	ESTABLISHED	Already established.
00000005	CLOSE WAIT	FIN received and waiting for completion.
00000006	FIN WAIT 1	Completed and FIN sent.
00000007	CLOSING	Completed and exchanged FIN. Awaiting ACK.
00000008	LAST ACK	FIN sent and completed. Awaiting ACK.
00000009	FIN WAIT 2	Completed and ACK received. Awaiting FIN.
0000000A	TIME WAIT	After closing, pauses twice the maximum segment life (2MSL).

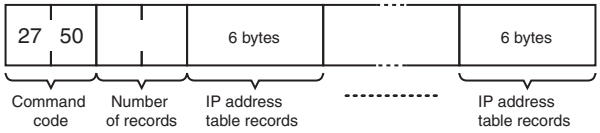
Response Codes

Response code	Description
0000	Normal end
0105	Node address setting error Local IP address setting error
0302	CPU Unit error; execution not possible.
1001	Command too large
1002	Command too small
1100	Connection number not set from 1 to 16

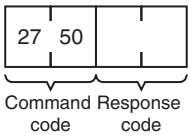
IP ADDRESS TABLE WRITE

Writes the IP address table.

Command Block



Response Block



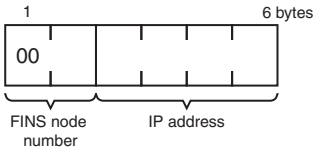
Parameters

Number of Records (Command)

The number of records to write is specified in hexadecimal between 0000 and 0020 (0 to 32 decimal) in the command. If this value is set to 0, the IP address table will be cleared so that no records are registered.

IP Address Table Records (Command)

Specify the IP address table records. The number of records specified must be provided. The total number of bytes in the IP address table records is calculated as the number of records × 6 bytes/record. The configuration of the 6 bytes of data in each record is as shown in the following diagram.



FINS Node Address

Node address for communications via the FINS command (hexadecimal).

IP Address

IP address used by TCP/IP protocol (hexadecimal).

Precautions

- The registered IP address table will not be effective until the PLC or EtherNet/IP Unit or built-in EtherNet/IP port is restarted.
- An error response will be returned if the IP address conversion method in the system mode settings is set for automatic generation on the FINS/UDP Tab Page of the Unit.

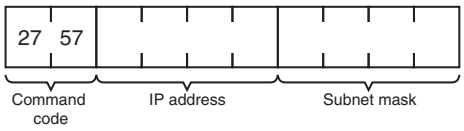
Response Codes

Response code	Description
0000	Normal end (echo reply received from the remote node)
1001	Command too large
1002	Command too small
1003	The number of records specified does not match the sent data length.
110C	The number of records is not between 0 and 32. The FINS node address is not between 1 and 126 The IP address is 0.
2307	IP address conversion method is set for automatic generation.

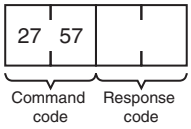
IP ADDRESS WRITE

Write the local IP address and the subnet mask in the CPU Bus Unit System Setup.

Command Block



Response Block

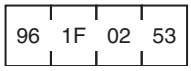


Parameters

IP Address (Command)

Specify the local IP address of the EtherNet/IP Unit or built-in EtherNet/IP port using 4 pairs of 2-digit hexadecimal numbers in the range 00.00.00.00 to FF.FF.FF.FF (0.0.0.0 to 255.255.255.255 decimal). Specify 0.0.0.0 to enable the local IP address set in the allocated DM Area words.

Example: 150.31.2.83



Subnet Mask (Command)

Specify the local IP address of the EtherNet/IP Unit or built-in EtherNet/IP port using 4 pairs of hexadecimal numbers in the range 00.00.00.00 to FF.FF.FF.FF (0.0.0.0. to 255.255.255.255 decimal).

Example: 255.255.255.255



Response Codes

Response code	Description
0000	Normal end
1001	Command too large
1002	Command too small

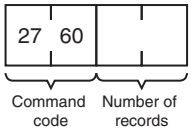
Precautions

- The local IP address and subnet mask set by this command are written to the CPU Bus Unit System Setup for the EtherNet/IP Unit or built-in EtherNet/IP port.
- The new local IP address and subnet mask settings will become effective when the PLC or EtherNet/IP Unit or built-in EtherNet/IP port is restarted.

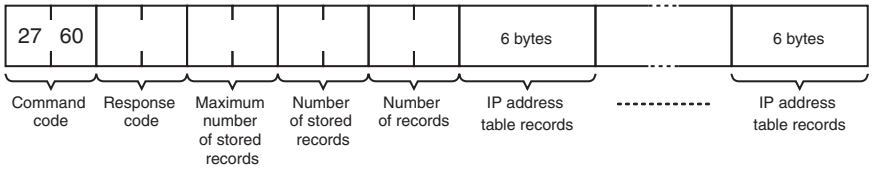
IP ADDRESS TABLE READ

Reads the IP address table.

Command Block



Response Block



Parameters

Number of Records (Command, Response)

The number of records to read is specified between 0000 and 0020 (0 to 32 decimal) in the command. If this value is set to 0, the number of stored records is returned but the IP address table records are not returned. The response returns the actual number of records read.

Maximum Number of Stored Records (Response)

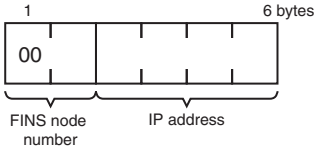
The maximum number of records that can be stored in the IP address table is returned. The maximum number of stored records is fixed at 0020 (32 records).

Number of Stored Records (Response)

The number of IP address table records stored at the time the command is executed is returned as a hexadecimal number.

IP Address Table Records (Response)

The number of IP address table records specified in the number of records parameter is returned. The total number of bytes in the IP address table records is calculated as the number of records × 6 bytes/record. The configuration of the 6 bytes of data in each record is as shown in the following diagram.



FINS Node Address

Node address for communications via the FINS command (in hexadecimal).

IP Address

IP number used by TCP/IP protocol (in hexadecimal).

Precautions

- If the IP address table contains fewer records than the number specified in the *number of records* parameter, all the records contained in the IP address table when the command is executed will be returned and the command execution will end normally.
- An error response will be returned if the IP address conversion method in the system mode settings is set to the automatic generation method on the FINS/UDP Tab Page of the Unit.

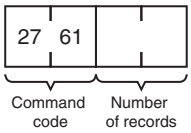
Response Codes

Response code	Description
0000	Normal end
1001	Command too large
1002	Command too small
2307	IP address conversion method is set to the automatic generation method.

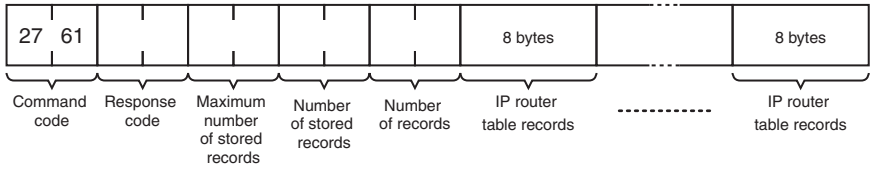
IP ROUTER TABLE READ

Reads the IP router table.

Command Block



Response Block



Parameters

Number of Records (Command, Response)

The number of records to read is specified between 0000 and 0008 (0 to 8 decimal) in the command. If this value is set to 0, the number of stored records will be returned but the IP router table records will not be returned. The response returns the actual number of records read.

Maximum Number of Stored Records (Response)

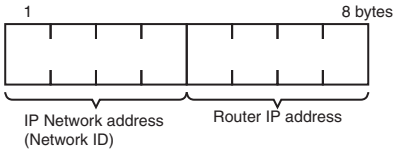
The maximum number of records that can be stored in the IP router table is returned. The maximum number of stored records is fixed at 0008 (8 records).

Number of Stored Records (Response)

The number of IP router table records stored at the time the command is executed is returned in hexadecimal.

IP Router table Records (Response)

The number of IP router table records specified in the *number of records* parameter is returned. The total number of bytes in the IP router table records is calculated as the number of records × 8 bytes/record. The configuration of the 8 bytes of data in each record is shown below.



IP Network Address
The network ID from the IP address in hexadecimal. The network ID part corresponding to the address class (determined by the leftmost 3 bits) set here, is enabled.

Router IP Address
The IP address (in hexadecimal) of a router connected to a network specified with IP addresses.

Precautions

If the IP router table contains fewer records than the number specified in the *number of records* parameter, all the records contained in the IP router table when the command is executed will be returned and the command execution will end normally.

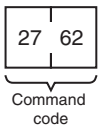
Response Codes

Response code	Description
0000	Normal end
1001	Command too large
1002	Command too small

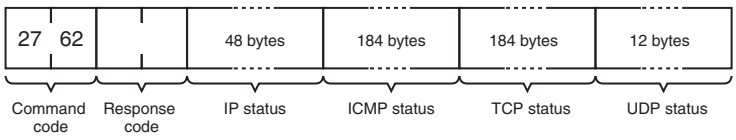
PROTOCOL STATUS READ

Reads the protocol status or the EtherNet/IP Unit or built-in EtherNet/IP port.

Command Block



Response Block



Parameters

IP Status (Response)

Twelve types of IP status information occupying 4 bytes each are returned in the following sequence. Each value is returned as an 8-digit hexadecimal value.

1. Total number of IP packets received.
2. The number of IP packets discarded due to an error with the checksum in the packet header.
3. The number of IP packets discarded because the received packet was larger than the overall packet length value in the packet header.
4. The number of IP packets discarded because the minimum size of the IP header data could not be stored in the first short buffer (See note.) when an attempt was made to store the packet.
5. The number of packets discarded for one of the following reasons:
   - The IP header length value in the IP header was smaller than the smallest size of the IP header.
   - The size of the first short buffer (See note.) was smaller than the IP header length value in the IP header when storing the packet.

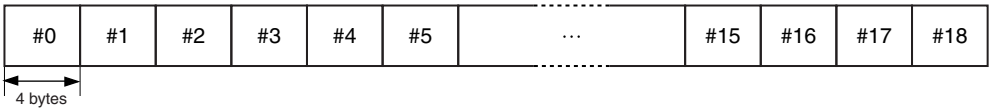
6. The number of IP packets discarded because the IP header length was larger than the overall packet length value in the packet header.
7. The number of fragmented packets received.
8. The number of received fragmented IP packets discarded because a queue for reassembly could not be secured.
9. The number of fragmented IP packets discarded because they could not be reassembled within 12 seconds after being received.
10. Always 0.
11. The number of packets addressed to other networks that have been discarded.
12. Always 0.

Note Refer to *MEMORY STATUS READ* on page 663 for details on the short buffer.

ICMP Status (Response)

Ten types (46 items) of ICMP status information occupying 4 bytes each are returned in the following sequence. Each value is returned as an 8-digit hexadecimal value.

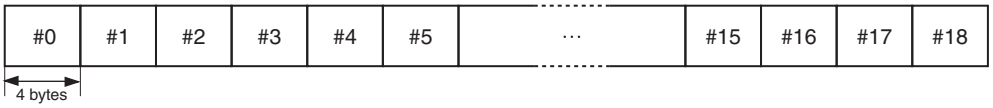
1. The number of times the ICMP error routine was called. The ICMP error routine uses ICMP packets to inform the source about errors. The routine is called when an illegal packet is received (error in IP option processing or error in relay processing) or if the object port does not exist when using UDP.
2. Always 0.
3. Always 0.
4. Total number of outputs of each packet type during ICMP output. The 19 statistical values are returned in the order shown below. Contents are defined for 13 types only; all other types contain 0. Only #0, #3, #14, #16, and #18 are counted by the EtherNet/IP Unit or built-in EtherNet/IP port.



Type number	Description
#0	Echo reply
#1, #2	Undefined, always 0
#3	Destination unreachable
#4	Source quench
#5	Routing redirect
#6, #7	Undefined, always 0
#8	Echo
#9, #10	Undefined, always 0
#11	Time exceeded
#12	Parameter problem
#13	Time stamp
#14	Time stamp reply
#15	Information request
#16	Information request reply
#17	Address mask request
#18	Address mask reply

5. The number of received ICMP packets discarded because the type-indication code was out of range.
6. The number of received ICMP packets discarded because the overall packet length value in the packet header was smaller than the minimum ICMP packet length.
7. The number of received ICMP packets discarded because of an incorrect checksum value in the packet header.

8. The number of received ICMP packets discarded because the ICMP header length value in the packet header did not match the lengths of individual header types.
9. The number of responses returned to received ICMP packets requiring a response.
10. Total number of inputs of each packet type during ICMP input. The 19 statistical values are returned in the order shown below. Contents are defined for 13 types only; all other types contain 0.



Type number	Description
#0	Echo reply
#1, #2	Undefined, always 0
#3	Destination unreachable
#4	Source quench
#5	Routing redirect
#6, #7	Undefined, always 0
#8	Echo
#9, #10	Undefined, always 0
#11	Time exceeded
#12	Parameter problem
#13	Time stamp
#14	Time stamp reply
#15	Information request
#16	Information request reply
#17	Address mask request
#18	Address mask reply

TCP Status (Response)

Three types (46 items) of TCP status information occupying 4 bytes each are returned in the following sequence. Each value is returned as an 8-digit hexadecimal value.

1) Connection Information (60 Bytes)

Fifteen items are returned in the following sequence:

1. The number of times active connections were correctly established.
2. The number of times a SYN packet was received while waiting to establish a passive connection.
3. The number of times active or passive connections were correctly established.
4. The number of times an established connection was cut off.
5. The number of times the connection wait status was cut off.
6. The number of times protocol control blocks or other actively allocated structures were released.
7. The number of segments for the round-trip time (time from segment transmission to ACK).
8. The number of times the round-trip time was changed.
9. The number of times a delayed acknowledgement (ACK) was sent. If the order of the received segments is reversed, ACK is sent with a packet of data separate from ACK (response to input data, etc.) or is immediately sent with the ACK for other data.
10. The number of times the connection was cut off because no ACK was returned after several resend attempts.
11. The number of times no ACK was returned within the resend timer set time. (The resend timer sets the maximum time limit between the data being output and ACK being returned.)

12. The number of times no window advertisement is received within the time set on the duration timer. (The duration timer sets the maximum time limit for a window advertisement to be received if the transmission window is smaller than necessary and the resend timer is not set. If no window advertisement is received within the time limit, the number of segments permitted by the transmission window are sent. If the transmission window is set to 0, a window probe (1 octet of data) is sent before the timer restarts.)
13. The number of times no segment was sent or received within the time set on the hold timer.
14. The number of times the hold packet is resent. (Always 0.)
15. The number of times the hold packet is sent without response before the connection is cut off.

2) Send Information (40 Bytes)

Ten information items are returned in the following sequence:

1. The total number of packets sent.
2. The number of data packets sent.
3. The number of data bytes sent.
4. The number of data packets resent.
5. The number of data bytes resent.
6. The number of ACK packets sent.
7. The number of window probes (1 octet of data) sent.
8. The number of emergency data packets sent. (Always 0.)
9. The number of window advertisement packets sent.
10. The number of control packets (SYN, FIN, RST) sent.

3) Receive Information (84 Bytes)

Twenty-one information items are returned in the following sequence:

1. The total number of packets received.
2. The number of packets received continuously.
3. The number of bytes received continuously.
4. The number of received packets discarded due to an incorrect checksum.
5. The number of packets discarded because the TCP header was smaller than the minimum size for a TCP header or was larger than the IP packet.
6. The number of packets discarded because the TCP header and IP header could not be stored in the first short buffer.
7. The number of resent packets received.
8. The number of bytes in the resend packets.
9. The number of duplicated resend packets received.
10. The number of bytes in the duplicated resend packets received.
11. The number of out-of-range data packets received. (Always 0.)
12. The number of bytes in the out-of-range data packets received. (Always 0.)
13. The number of packets where the data was larger than the window.
14. The number of bytes in the packets where the data was larger than the window.
15. The number of packets received after closing.
16. The number of window probe packets received.
17. The number of resent ACK packets received.
18. The number of ACK packets received with no data set.
19. The number of ACK packets received.
20. The number of ACK packets received for received transmission acknowledgements (ACK).
21. The number of window advertisement packets received.

UDP Status (Response)

Three items of UDP information occupying 4 bytes each are returned in the following sequence. Each value is returned as an 8-digit hexadecimal value.

1. The number of packets discarded because the size of the first short buffer was smaller than the minimum size (28) of the IP header and UDP header when the packet was stored.
2. The number of packets discarded due to an incorrect checksum in the UDP header.
3. The number of packets discarded because the IP overall length in the IP header was shorter than the UDP overall length in the UDP header.

Precautions

All the above values are set to 0 if network operation stops due to incorrect settings in the system setup.

Counting will be stopped when a count reaches the maximum value. The maximum values are as follows:

IP, ICMP, or UDP status: 7FFFFFFF (2,147,483,647 decimal)
TC status: FFFFFFFF (4,294,967,295 decimal)

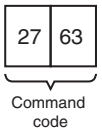
Response Codes

Response code	Description
0000	Normal end
1001	Command too large

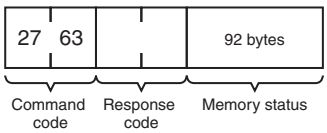
MEMORY STATUS READ

Reads the status of the network memory for the EtherNet/IP Unit or built-in EtherNet/IP port. The network memory contains 2,991 bytes that are used as required as for communications buffers for communications servicing. The network memory consists of 23,928 short buffers (128 bytes each) and 64 long buffers (1,024 bytes each).

Command Block



Response Block



Parameters

Memory Status (Response)

A total of 23 data items in six areas are returned in the following order. Each item consists of 4 bytes.

1) Short Buffer Application: Two items are returned (8 bytes).

1. The number of short buffers currently being used.
2. The number of short buffers in the system (fixed at 23,928 decimal).

2) Short Buffer Application by Type: Thirteen items are returned (52 bytes).

1. The number of short buffers used for storing communications data

2. The number of short buffers used for protocol headers (TCP, UDP, IP, ICMP, ARP)
3. The number of short buffers used in socket structures *1
4. The number of short buffers used as protocol control blocks *1
5. The number of short buffers used for routing tables *1
6. Not used (always 0)
7. Not used (always 0)
8. The number of short buffers used for IP fragment re-assembly queue headers
9. The number of short buffers used for storing socket addresses
10. Not used (always 0)
11. The number of short buffers used for storing socket options
12. The number of short buffers used for storing access rights *1
13. The number of short buffers used for storing interface addresses *1

*1 For the CS1W/CJ1W-EIP21S EtherNet/IP Unit, the following applies.
Not used (always 0)

3) Long Buffer Application: Two items are returned (8 bytes).

1. The number of long buffers currently being used.
2. The number of long buffers in the system (fixed at 64 decimal).

4) Not Used: Always 0. (4 bytes)

5) Network Memory Application: Two items are returned (8 bytes).

1. The number of bytes used (in K bytes)
2. The percentage used

6) Memory Exhaustion Log (12 bytes)

Counts for the following values indicate a high load on the EtherNet/IP Unit or built-in EtherNet/IP port. These high loads may be caused by problems in communications, particularly FINS communications and UDP sockets. If these values are consistently high, check your applications.

1. The number of times an attempt was made to secure a short buffer without WAIT when there were no short buffers available.
2. The number of times an attempt was made to secure a short buffer with WAIT when there were no short buffers available.
3. The number of times an attempt was made to release and secure a short buffer already being used by another socket when there were no short buffers available.

Precautions

All the above values are set to 0 if Ethernet communications functions are stopped due to improper settings in the system setup.

These values are cleared when the EtherNet/IP Unit or built-in EtherNet/IP port is started or reset. Values will be counted only until the maximum values are reached.

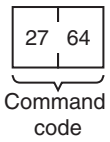
Response Codes

Response code	Description
0000	Normal end
1001	Command too large

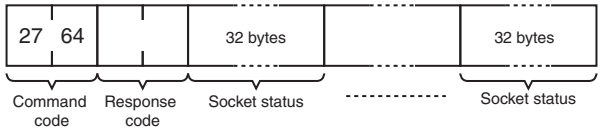
SOCKET STATUS READ

Reads the network socket status of the EtherNet/IP Unit or built-in EtherNet/IP port.

Command Block



Response Block



Parameters

Socket Status (Response)

Returns eight types of information in records of 32 bytes each. A maximum of 62 records can be returned. The format of each record is shown below.

Protocol (4 bytes)
The protocol used for the socket is returned as a number.
00 00 00 06: TCP; 00 00 00 11: UDP

Receive Queue (4 bytes)
The number of bytes in the reception queue.

Send Queue (4 bytes)
The number of bytes in the send queue.

Local IP Address (4 bytes)
The local IP address allocated to the socket.

Local Port Number (4 bytes)
The local port number allocated to the socket.

Remote IP Address (4 bytes)
The remote IP address allocated to the socket.

Remote Port Number (4 bytes)
The remote port number allocated to the socket.

TCP Transitions (4 bytes)
The TCP connection status is returned as one of the numbers shown in the following table. Refer to *Appendix C TCP Status Transitions* for a diagram of transitions.

Number	Stage	Status
00 00 00 00	CLOSED	Closed.
00 00 00 01	LISTEN	Waiting for connection.
00 00 00 02	SYN SENT	SYN sent in active status.
00 00 00 03	SYN RECEIVED	SYN received and sent.
00 00 00 04	ESTABLISHED	Already established.
00 00 00 05	CLOSE WAIT	Received FIN, waiting to close.
00 00 00 06	FIN WAIT 1	Completed and FIN sent.
00 00 00 07	CLOSING	Completed and exchanged FIN. Awaiting ACK.
00 00 00 08	LAST ACK	FIN sent and completed. Awaiting ACK.

Number	Stage	Status
00 00 00 09	FIN WAIT 2	Close completed and ACK received. Awaiting FIN.
00 00 00 0A	TIME WAIT	After closing, pauses twice the maximum segment life (2MSL).

Precautions

All the above values are set to 0 if Ethernet communications functions are stopped due to improper settings in the system setup.

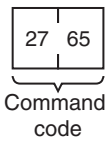
Response Codes

Response code	Description
0000	Normal end
1001	Command too large

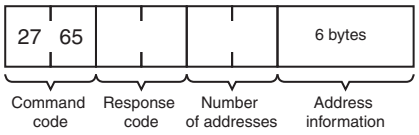
ADDRESS INFORMATION READ

Reads FINS node addresses and IP addresses

Command Block



Response Block



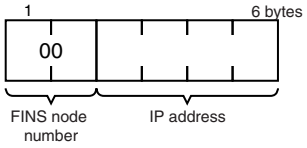
Parameters

Number of Addresses (Response)

Returns the number of pairs of FINS node addresses and IP addresses. With the EtherNet/IP Unit or built-in EtherNet/IP port, this value is always 0001 (1 decimal).

Address Information

Returns the FINS node addresses and IP addresses. Each pair requires 6 bytes and has the following configuration.



FINS Node Address

Node address set in the EtherNet/IP Unit or built-in EtherNet/IP port (hexadecimal).

IP Address

IP address set in the EtherNet/IP Unit or built-in EtherNet/IP port (hexadecimal).

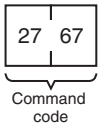
Response Codes

Response code	Description
0000	Normal end
1001	Command too large

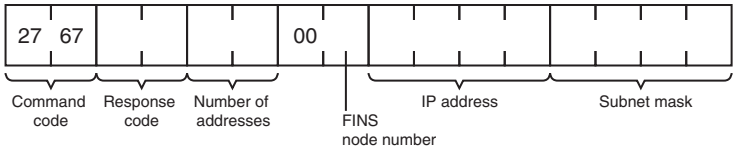
IP ADDRESS READ

Reads the local IP address and subnet mask in the CPU Bus Unit System Setup and the FINS node address. The values read with this command, however, are not necessarily the settings actually used for operation. The settings that are actually used for operation can be confirmed using CONTROLLER DATA READ (page 624) and ADDRESS INFORMATION READ (page 666).

Command Block



Response Block



Parameters

Number of Addresses (Response)

The number of sets of FINS node addresses, IP addresses, and subnet masks being returned. The EtherNet/IP Unit or built-in EtherNet/IP port is always 0001 (1 decimal).

FINS Node Address (Response)

Node address set on the EtherNet/IP Unit or built-in EtherNet/IP port (hexadecimal).

IP Address (Response)

The local IP address set in the CPU Bus Unit System Setup for the EtherNet/IP Unit or built-in EtherNet/IP port is returned in order starting from the leftmost bytes in hexadecimal. If the local IP address set in the allocated words in the DM Area is enabled, 0.0.0.0 is returned.

Subnet Mask (Response)

The subnet mask set in the CPU Bus Unit System Setup for the EtherNet/IP Unit or built-in EtherNet/IP port is returned in order starting from the leftmost bytes in hexadecimal.

Response Codes

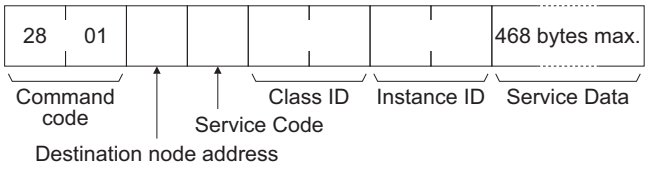
Response code	Description
0000	Normal end
1001	Command too large

EXPLICIT MESSAGE SEND

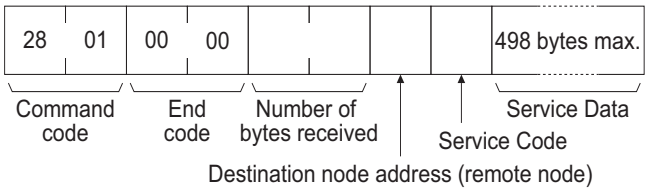
Sends a explicit request message to the specified object, and receives a response.

The rightmost 8 bits of the remote (destination) IP address are used as the remote MAC ID, and the remote IP address is the network ID of the local IP address + the rightmost 8 bits of the remote IP address.

Command Block



Response Block



Response Codes

Response code	Description
0000	Normal end
0101	The local node's network has not started up.
0105	Local node setting error (A BOOTP errors occurs, and the IP address is undetermined.)
0106	Duplicate address error
0201	The remote node's network has not started up.
0204	Remote node busy, cannot send.
0205	No response returned from remote node. Monitoring timer timed out.
1001	Command length exceeds maximum command length.
1002	Command length is less than minimum command length.
1004	Command block format does not match.
1005	Header error
110B	Response length exceeds maximum response length.
2211	Unit is busy.

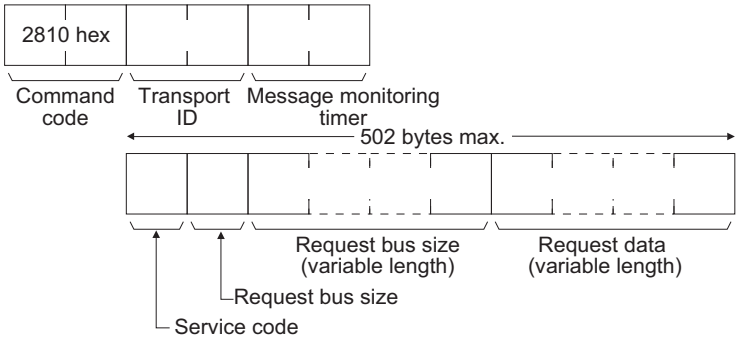
Description

For details, refer to *EXPLICIT MESSAGE SEND (28 01)* on page 280 in *9-1 Sending Explicit Messages*.

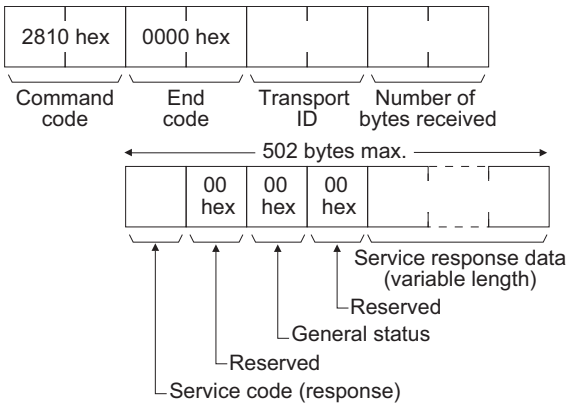
CIP UCMM MESSAGE SEND

Sends a message in the CIP message (UCMM) format.

Command Block



Response Block



Response Codes

Response code	Description
0000	Normal end
0101	The local node's network has not started up.
0106	Duplicate address error
0201	The remote node's network has not started up.
0204	Remote node busy, cannot send.
0205	No response returned from remote node. Monitoring timer timed out.
1001	Command length exceeds maximum command length.
1002	Command length is less than minimum command length.
1004	Command block format does not match.
1005	Header error
110B	Response length exceeds maximum response length.
2211	Unit is busy.

Description

For details, refer to *CIP UCMM MESSAGE SEND (28 10)* on page 276 in *9-1 Sending Explicit Messages*.

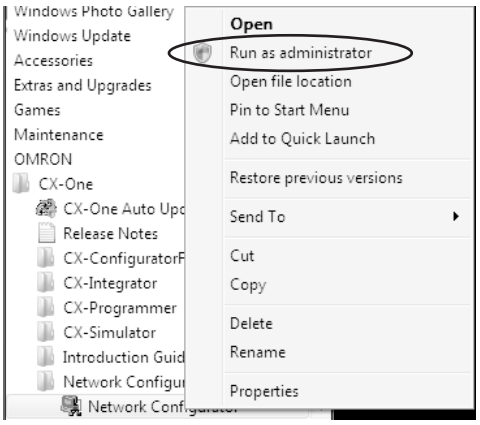
Appendix F
EDS File Management

This section explains the EDS file management functions used in the Network Configurator.

Installing EDS Files

Note We recommend that you start the Network Configurator from *Run as administrator* when you install an EDS file in the Network Configurator. If the EDS file is installed on a Network Configurator that is started in any other way, Windows security user management will cause the installed EDS file to not be recognized when you log in using a different user account. You can run the Network Configurator as the administrator by using the following procedure.

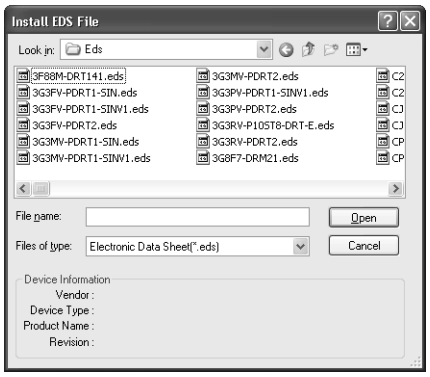
1. Select the Network Configurator from the Start Menu, and then right-click.
2. Select *Run as administrator* from the pop-up menu that is displayed.



EDS File - Install

The Network Configurator can support new devices if the proper EDS files are installed.
To install the EDS file, use the following procedure.

1. Select EDS File and Install.
   The following window will be displayed.



2. The device information will be displayed on the bottom of the window when the EDS file is selected.
3. Select the EDS file to be installed and click the Open Button.
   Next, select the icon file (*.ico), and the EDS file will be added to the Hardware List.
   If the EDS file already exists, the new EDS file will overwrite the previous one.
   If the hardware versions are different, an EDS file will be added to the Hardware List for each version.

Creating EDS Files

EDS File - Create

The EDS files are required by the Network Configurator in order to create a network configuration. To create an EDS file, use the following procedure.

1. Select ***EDS File - Create***.
2. Set the device information and I/O information.
   The device information can be obtained from the device on the network if the network is online.
3. The device can be added to the Hardware List as a new device, just like installing an EDS file.

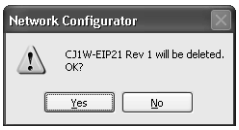
Note Device parameters cannot be set with the Network Configurator's EDS file creation function. Obtain a proper EDS file from the manufacturer of the device to make device parameter settings for the device.

Deleting EDS Files

EDS File - Delete

To delete an EDS file, use the following procedure.

1. Select the device from the Hardware List.
2. Select ***EDS File - Delete***.
   The following confirmation window will be displayed.



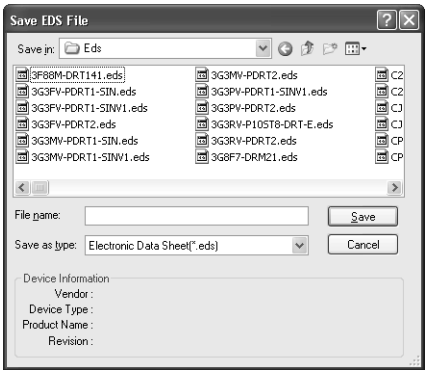
3. Click the **Yes** Button.
   The selected device will be deleted from the Hardware List together with the EDS file.

Saving EDS Files

EDS File - Save

To save the EDS file, use the following procedure.

1. Select the device from the Hardware List.
2. Select ***EDS file - Save As***.
   The following window will be displayed to specify the name of the folder where the EDS file will be saved and the name of the EDS file.



3. Input the folder and file names and click the **Save** Button The EDS file will be saved.

Searching EDS Files

EDS File - Search

To search the devices (EDS files) displayed in the Hardware List, use the following procedure.

1. Select ***EDS file - Find***.
   The following window will be displayed.



2. Input the character string and click the **Find Next** Button.
3. When there is a matching device found, the cursor will move to that position.
4. To quit the search operation, click the **Cancel** Button.

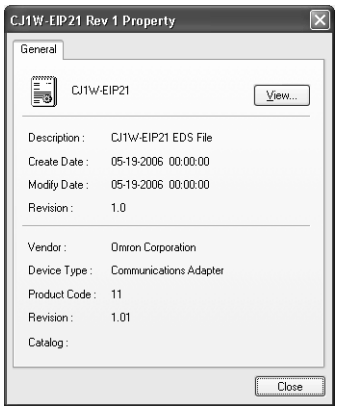
Note (1) The device will be found if it is located below the present cursor position.
(2) To search all the devices, select *Hardware* in the Hardware List before performing the search procedure.

Displaying EDS File Properties

EDS File - Property

To display the properties of the EDS file, use the following procedure.

1. Select the desired hardware (device) from the Hardware List.
2. Select ***EDS File - Property***.
   The following window will be displayed.



   The time and date that the EDS file was created will be displayed, along with the device information.

Creating EDS Index Files

EDS File - Create EDS Index File

To manually add an EDS file or if a device is not displayed correctly in the hardware list, use the following procedure to recreate the EDS index file.

(This applies to Network Configurator version 3.30 or higher.)

1. Select ***EDS File - Create EDS Index File***.
2. Restart the Network Configurator.

Appendix G
Precautions for Using Windows XP or Later Windows OS

Changing Windows Firewall Settings

Better firewall security for Windows XP or later Windows OS has increased the restrictions for data communications on Ethernet ports. When using an EtherNet/IP connection*1 to one of the following PLCs from an Ethernet port on a computer, you must change the settings of the Windows Firewall to enable using CX-Programmer or Network Configurator communications.

Applicable PLCs:

- CJ2H-CPU□□-EIP/CJ2M-CPU3□ or CJ3M-CPU3□
- CS1W/CJ1W-EIP□□/ CS1W/CJ1W-EIP□□S

*1 CX-Programmer

- An EtherNet/IP connection includes the following cases:
- An online connection with the network type set to EtherNet/IP
- An automatic online connection to a PLC on an EtherNet/IP network when ***Auto Online - EtherNet/IP Node Online*** is selected from the PLC Menu

Network Configurator

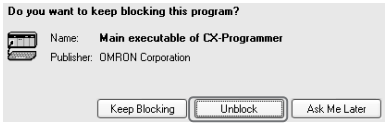
- A connection made by selecting ***Option - Select Interface - Ethernet I/F***

Note Windows Firewall is mainly designed to prevent inappropriate access from external devices (e.g., via the Internet). The changes to the Windows Firewall settings described in this document enable EtherNet/IP connections to be used by the CX-Programmer. If the same computer is being used on a company network or other network, confirm that the changes will not create security problems before proceeding with the changes. The changes described in this document are required only when you connect using EtherNet/IP through an Ethernet port. No changes are necessary if you are connecting through any other port, such as a USB port.

Changing Windows Firewall Settings

Windows XP

1. When you attempt to connect the CX-Programmer or Network Configurator to a PLC on an EtherNet/IP network through an Ethernet port, the Windows Security Alert Dialog Box will be displayed.
2. Click the Unblock Button.



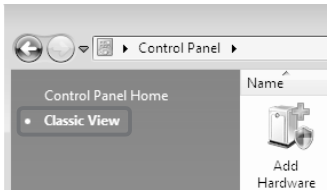
An EtherNet/IP connection will be accepted from CX-Programmer or Network Configurator and EtherNet/IP connections will be enabled in the future as well.

Windows Vista or Windows 7

Use the following procedure to change the settings before attempting to connect from the CX-Programmer or Network Configurator.

The User Account Control Dialog Box may be displayed during this procedure. If it appears, click the **Continue** Button and continue with the procedure.

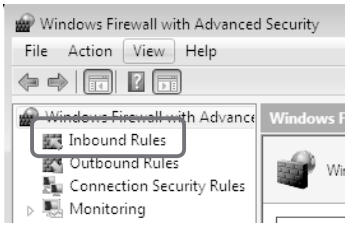
1. Select ***Control Panel*** from the Windows Start Menu and change the display to Classic View.



2. Open the *Administrative Tools* and select *Windows Firewall with Advanced Security* from the dialog box that is displayed.



3. Select *Inbound Rules* under *Windows Firewall with Advanced Security on Local Computer* on the left side of the *Windows Firewall with Advanced Security* Dialog Box.



4. Select *New Rule* under *Inbound Rules* in the Actions Area on the right side of the dialog box.



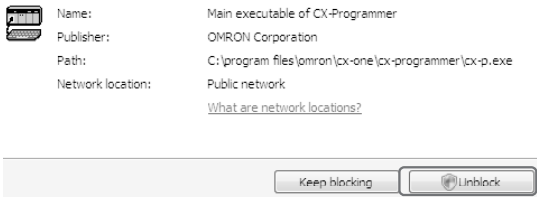
5. Make the following settings for each step in the *New Inbound Rule Wizard* Dialog Box, clicking the **Next** Button to move between steps.

Rule Type	Select Custom.
Program	Select *All Programs.*
Protocol and Ports	Select ICMPv4 as the protocol type. 
Scope	Select *Any IP address* for everything.
Action	Select *Allow the connection*.
Profile	Select *Domain, Private,* and *Public.*
Name	Enter any name, e.g., Omron_EIP.

6. Click the Finish Button. The rule that you defined will be registered in the Inbound Rules (e.g., Omron_EIP). Close the *Windows Firewall with Advanced Security* Dialog Box.



7. When you attempt to connect the CX-Programmer or Network Configurator to a PLC on an EtherNet/IP network through an Ethernet port, the Windows Security Alert Dialog Box will be displayed.
8. Click the **Unblock** Button.



An EtherNet/IP connection will be accepted from CX-Programmer or Network Configurator and EtherNet/IP connections will be enabled in the future as well.

Appendix H

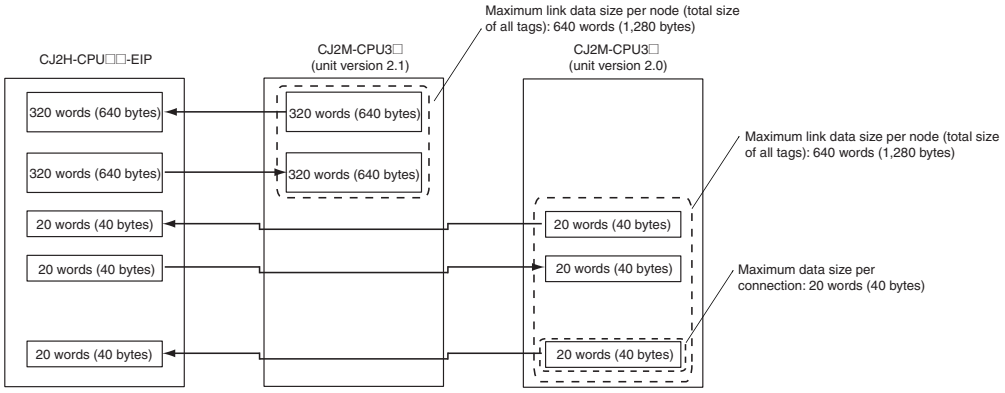
Setting Example for Using Tag Data Links with the CJ2M-CPU3□

The maximum link data size per node for tag data links with built-in EtherNet/IP ports on CJ2M-CPU3□ CPU Units depends on the unit version.

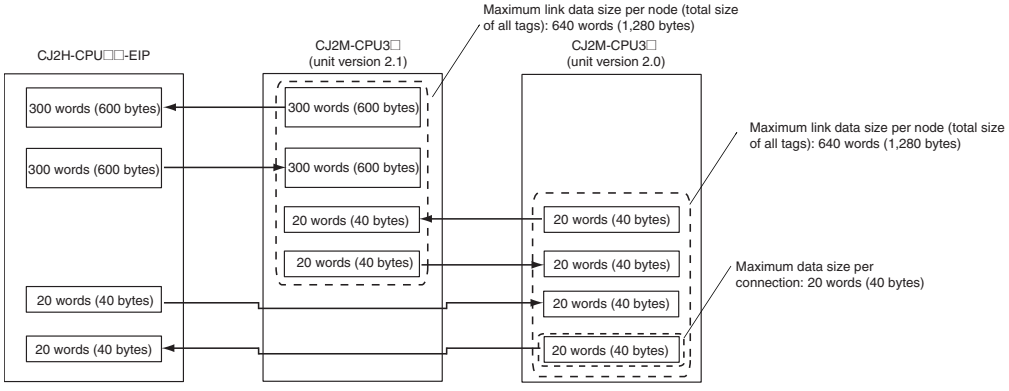
Use the following setting examples as reference.

Correct Tag Data Link Setting Examples

Setting Example 1

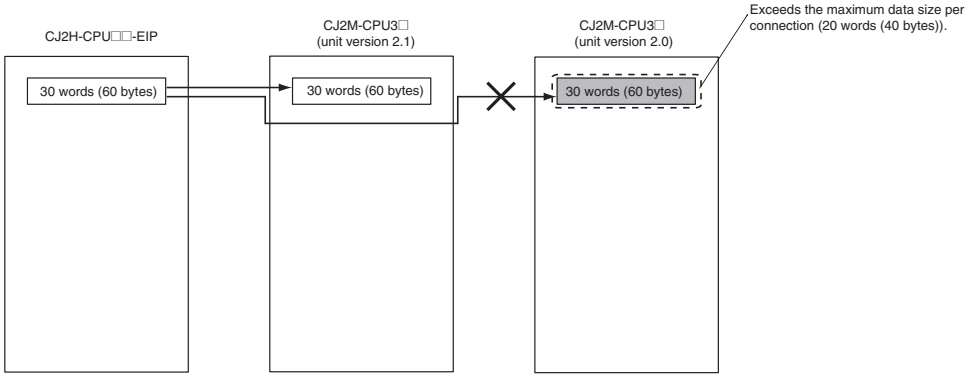


Setting Example 2

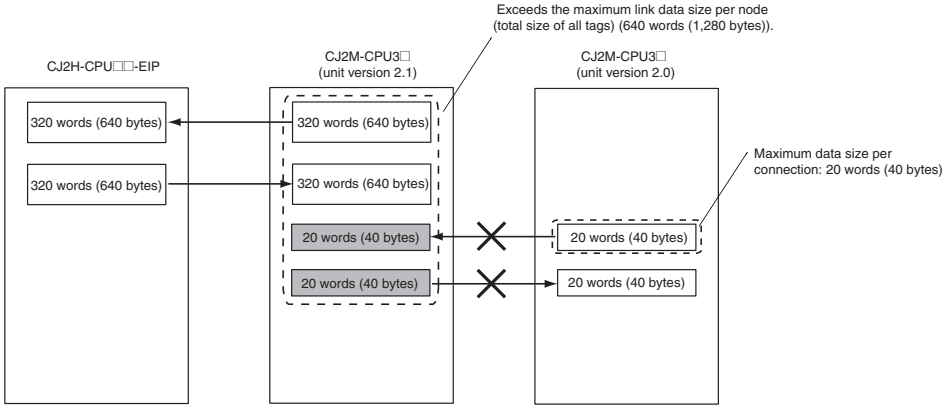


Incorrect Tag Data Link Setting Examples

Setting Example 1



Setting Example 2

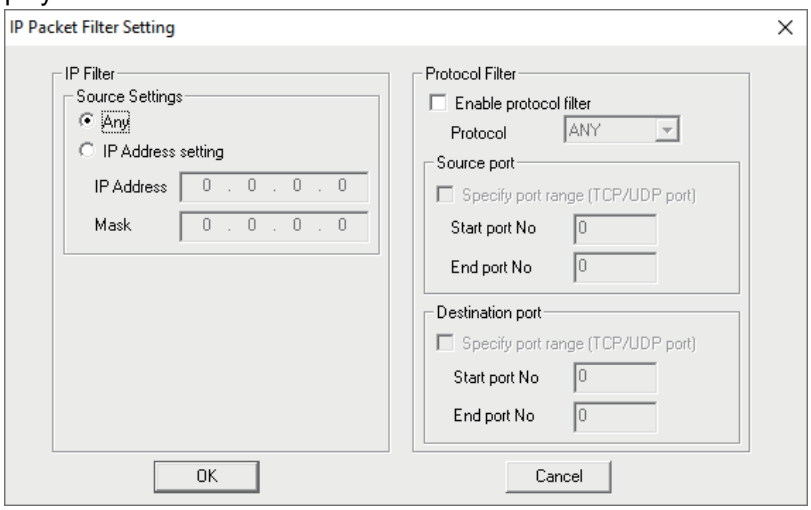


Appendix I
IP Packet Filter Settings

This appendix describes the Protocol Filter settings provided in the IP Packet Filter Setting Dialog Box among the settings described in *13-5 IP Packet Filtering*.

IP Packet Filter Table

Select the *Use IP Packet Filter* Option in the IP Packet Filter Tab Page and then click the **Insert** Button to display the table.



Setting	Contents	Default
IP Filter	Set the conditions for filtering by source IP address.	---
Source Settings	Set the source IP address specification method. Any IP Address setting	Any
IP Address	When the IP address specification method is *IP Address setting*, set the source IP address.	0.0.0.0
Mask	When the IP address specification method is *IP Address setting*, set the mask for the source IP address.	0.0.0.0
Protocol filter	Set the conditions for filtering by protocol.	
Enable protocol filter	Set whether or not to allow for editing the settings in the protocol filter group. Select the check box to allow for editing the settings. If you change the settings in the protocol filter group from the default values, the check box will be selected when the dialog box is displayed next time. Select or clear the check box.	Check box cleared
Protocol	Set the protocol that you want to permit. ANY TCP UDP IGMP (See note 1.) ICMP (See note 2.)	ANY

Setting	Contents	Default
Source port	---	---
Specify port range (TCP/UDP port)	Set whether or not to specify the port range. This setting is required when the protocol filter is TCP/UDP. Select or clear the check box.	Check box cleared
Start port No.	Set the start port. 0 to 65,535	0
End port No.	Set the end port. This setting is required when you specify the port range. 0 to 65,535	0
Destination Port	The contents and default values are the same as those of the source settings.	
Specify port range (TCP/UDP port)		
Start port No.		
End port No.		

Note (1) Select this to perform EtherNet/IP tag data link communications with multicast when the local node is the originator.

(2) Select this to allow ping requests to pass through the IP filter.

How the IP filter settings work

The IP filter settings permits packet reception at the set IP address(es).

If *Any* is set in *Source Settings*, packet reception is permitted for all IP addresses.

If *IP Address setting* is set in *Source Settings*, packet reception is permitted for the IP address specified in the lower-level settings: *IP Address* and *Mask*.

For *IP Address*, set the bits set for the mask in *Mask* and the following bits to *0*s.

Example of setting

- To permit one IP address
  Set the IP address at which to permit reception in *IP Address* and *255.255.255.255* in *Mask*.
  For example, to permit reception at 192.168.250.100, set *192.168.250.100* in *IP Address* and *255.255.255.255* in *Mask*.
- To permit multiple IP addresses
  Set the IP address at which to permit reception in *IP Address* and *Mask*.
  For example, to permit reception at 192.168.***.***, set *192.168.0.0* in *IP Address* and *255.255.0.0* in *Mask*.

How the protocol filter settings work

The protocol filter settings permit packet reception with the set protocol and port.

If *ANY* is set in *Protocol*, reception of IGMP and ICMP packets is permitted for all TCP/UDP ports.

If *IGMP* is set in *Protocol*, reception of IGMP packets is permitted.

If *ICMP* is set in *Protocol*, reception of ICMP packets is allowed.

If *TCP or UDP* is set in *Protocol*, and *Specify port range (TCP/UDP port)* is not selected, reception of TCP or UDP packets is allowed for all ports regardless of the port number settings.

If *TCP* or *UDP* is set in *Protocol*, and *Specify port range (TCP/UDP port)* is selected, reception of TCP or UDP packets is allowed for ports in the range determined by the *Start port No.* and *End port No.* settings.

Example of setting

- To permit one TCP/UDP port number
  Select the *Specify port range (TCP/UDP port)* Check Box, and set the TCP/UDP port numbers for which to permit reception for *Start port No.* and *End port No.*.
  If you set the same port number for both, packet reception is permitted for the set port number only.

- To permit multiple TCP/UDP port numbers
  Select the *Specify port range (TCP/UDP port)* Check Box, and set a range of TCP/UDP port numbers for which to permit reception for *Start port No.* and *End port No.*.
  Packet reception is allowed for the range of port numbers determined by the *Start port No.* and *End port No.* settings.

Appendix J
Security Use Cases

This appendix describes security use cases and the configuration examples and settings for each of them.

Use Cases

The following use cases are described.

Case	Use case	Function to use	Reference
1	Permitting packet reception for specific protocols	Opening and closing the port	*13-7-2 Case 1: Permitting Packet Reception for Specific Protocols*
2	Permitting packet reception from specific source IP addresses	IP packet filtering	*13-7-3 Case 2: Permitting Packet Reception from Specific Source IP Addresses*
3	Permitting packet reception from specific source ports	IP packet filtering	*Case 3: Permitting Packet Reception from Specific Source Ports*
4	Permitting packet reception to specific destination ports	IP packet filtering	*Case 4: Permitting Packet Reception to Specific Destination Ports*

Case 3: Permitting Packet Reception from Specific Source Ports

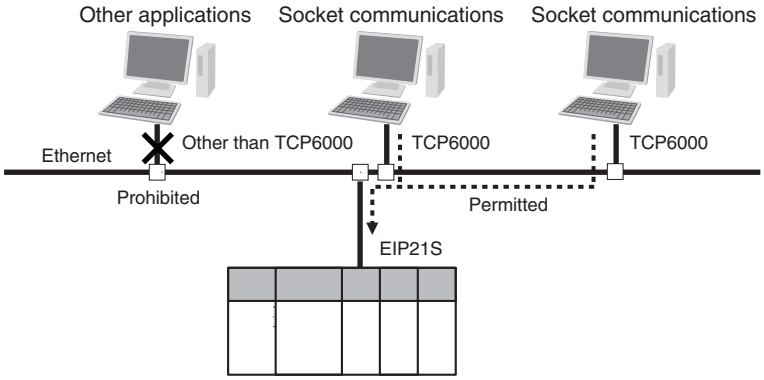
This use case is for permitting packet reception from a specific source port.

Use it when you can distinguish communications by the source port in use.

In this use case, IP packet filtering is used.

Configuration Example

This configuration example permits only socket communications for the TCP 6000 port from the socket communications program on the computer and prohibits communications from other communications ports.



Settings for This Configuration Example

Make the settings in the IP Packet Filter Setting Dialog Box as shown in the following table.

No.	IP Filter			Protocol filter						
	Source Settings			Protocol filter	Source port			Destination Port		
	Setting method	IP Address	Mask		Range specification	Start port No.	End port No.	Range specification	Start port No.	End port No.
1	Any	---	---	TCP	Use	6000	6000	---	---	---

Note Register all protocols and all TCP/UDP ports to use because communications from protocols or ports that are not permitted in the IP Packet Filter Setting are disabled.

Case 4: Permitting Packet Reception to Specific Destination Ports

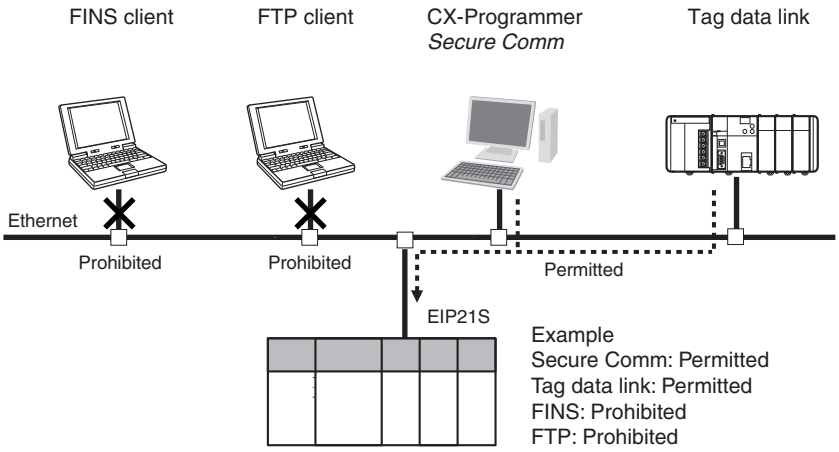
This use case is for permitting reception to a specific destination port.

Use it when you have a specific communications protocol to use and prohibit communications via unused protocols since the destination port is fixed by the communications protocol.

In this use case, IP packet filtering is used.

Configuration Example

This configuration example permits Secure Comm communications with the Support Software and CIP communications with external devices, and prohibits communications from other protocols.



Settings for This Configuration Example

Make the settings in the IP Packet Filter Setting Dialog Box as shown in the following table.

To permit communications with the CX-Programmer using Secure Comm, make the settings in row No. 1.

To permit tag data link communications with other communications devices, make the settings in No. 2 to No. 4 rows.

No.	IP Filter			Protocol filter						
	Source Settings			Protocol filter	Source port			Destination Port		
	Setting method	IP Address	Mask		Range specification	Start port No.	End port No.	Range specification	Start port No.	End port No.
1	Any	---	---	TCP	---	---	---	Use	443	443
2	Any	---	---	TCP	---	---	---	Use	44818	44818
3	Any	---	---	UDP	---	---	---	Use	44818	44818
4	Any	---	---	IGMP	---	---	---	---	---	---

Note Register all protocols and all TCP/UDP ports to use because communications from protocols or ports that are not permitted in the IP Packet Filter Setting are disabled.

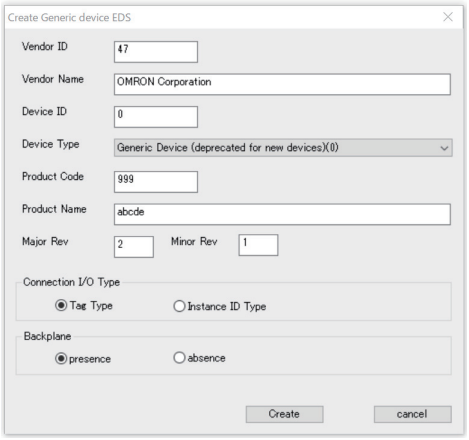
Appendix K
Tag Data Link Settings with Generic Devices

Use the Generic Device if you want to perform tag data links with a device that does not have an EDS file.
Create a Generic Device with the Network Configurator to use a Generic Device.
The procedures to create a Generic Device and the procedures to create a tag or tag set are shown below.

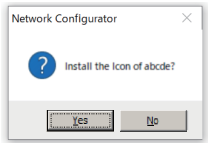
Note The procedures after creating a tag or tag set are the same as for devices that have EDS files. Refer to *6-2 Setting Tag Data Links*.

Creating Generic Devices

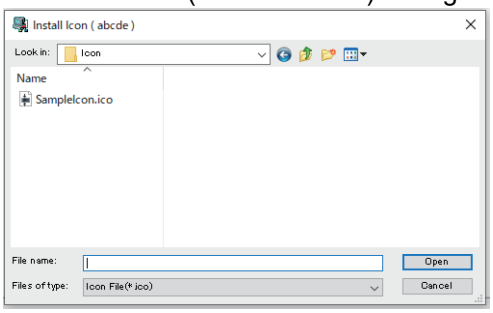
1. Select ***Create Generic Device*** from the ***EDS File*** Menu.
   The Create Generic device EDS Dialog Box is displayed.



2. Set the information for the device and click the **Create** Button.
   A confirmation dialog to install an icon is displayed.

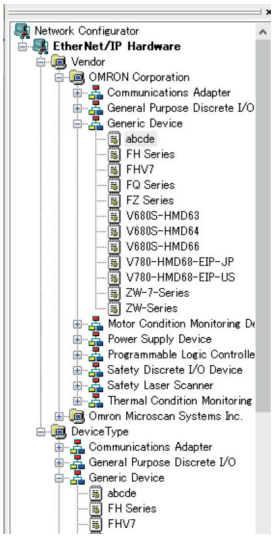


3. Set a device icon.
   - If you click the **Yes** Button:
   The Install Icon (EDS file name) Dialog Box is displayed.



   - If you click the **No** Button:
   A default icon for the Network Configurator is set.

4. Select the icon file (*.ico) to set as the EDS file and click the **Open** Button.
   The created Generic Device is added to the hardware list.



Creating a Tag or Tag Set for Generic Device

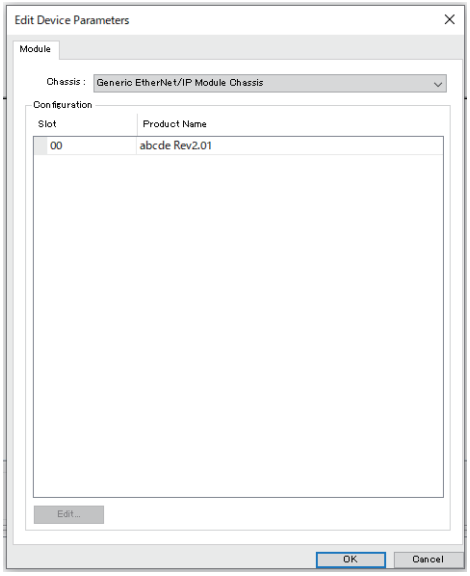
This section describes two types of methods for creating a tag or tag set: tag type and instance ID type. Each procedure is described below.

The type is what you select in ***Connection I/O Type*** when you create a Generic Device.

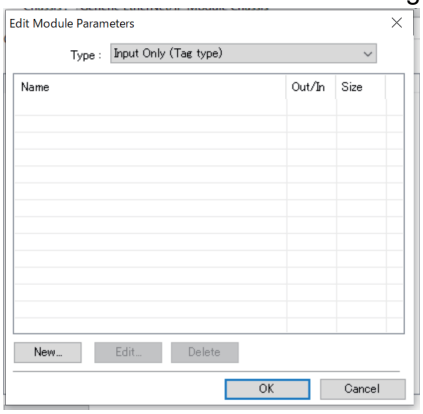
Creation Procedure for Tag Type

1. Add the Generic Device that you created to the network window.

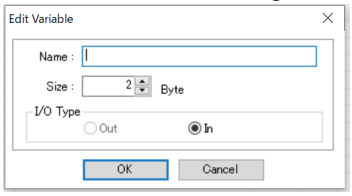
2. Double-click the device icon.
   The Edit Device Parameters Dialog Box is displayed.



3. Select the slot number ***00*** in the ***Configuration*** from the Module Tab Page and then click the **Edit** Button.
   The Edit Module Parameters Dialog Box is displayed.

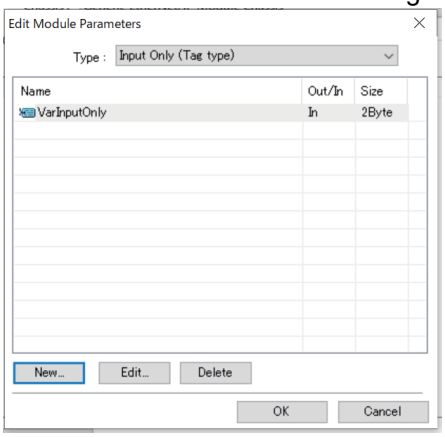


4. Select ***Input Only (Tag type)*** or ***Input & Output (Tag type)*** from ***Type*** and click the **New** Button.
   The Edit Variable Dialog Box is displayed.



5. Set the following parameters for the variable.
   - ***Name***
   Enter the name of the network variable. (Example: VarInputOnly)
   - ***Size***
   Enter the size of the tag in bytes.
   - ***I/O Type***
   If ***Type*** is ***Input & Output (Tag type)***, select ***Out*** or ***In***.

6. Click the **OK** Button.
   The Edit Module Parameters Dialog Box is displayed, and the added variable is displayed.

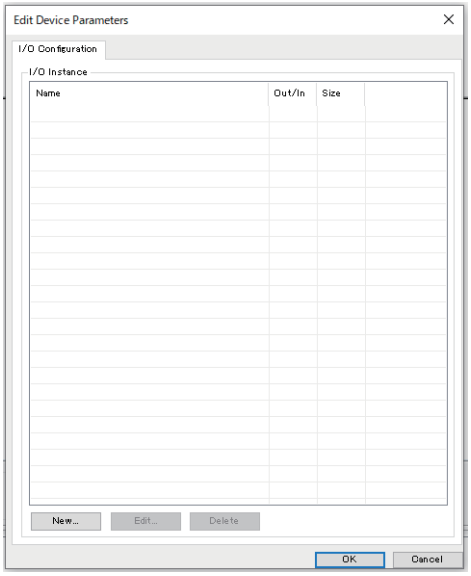


7. Repeat steps 4 through 6 to register the required variables. Click the **OK** Button when the registration is complete.

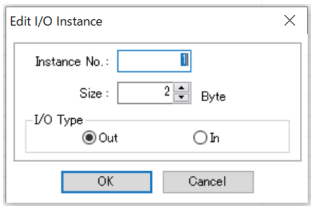
Creation Procedure for Instance ID Type

1. Add the Generic Device that you created to the network window.

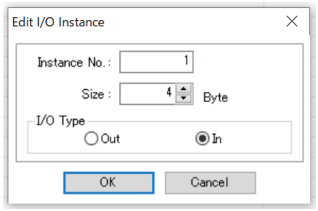
2. Double-click the device icon.
   The Edit Device Parameters Dialog Box is displayed.



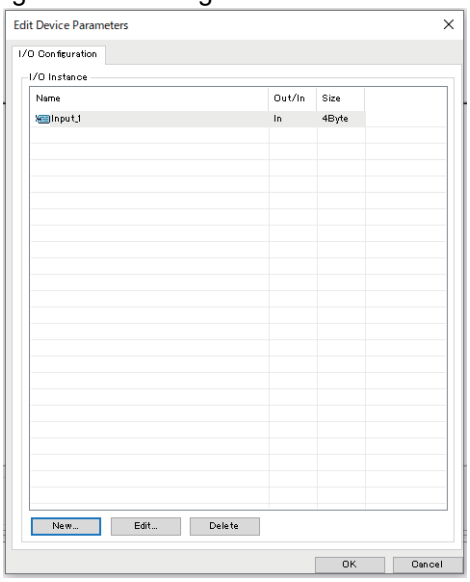
3. Click the **New** Button from the I/O Configuration Tab Page.
   The Edit I/O Instance Dialog Box is displayed.



4. Enter the following parameters.
   - ***Instance No.***
   Enter the instance ID for the I/O instance.
   - ***Size***
   Enter the size of the tag in bytes.
   - ***I/O Type***
   Select Out or In.



5. Click the **OK** Button.
   The Edit Device Parameters Dialog Box is displayed, and the added I/O instance is displayed in the I/O Configuration Tab Page.



6. Repeat steps 3 through 5 to register the required I/O instances. Click the **OK** Button when the registration is complete.

Appendix L
Function Blonk for Socket Service

Function blocks for the socket service are available for TCP and for UDP. The function blocks corresponding to each function are as follows:

- Function Block for Modbus TCP Client

Function	Function Block Name	File Name
Open TCP Socket Passive	_EIPS001_SOCKET_TcpOpenPassive	Lib\FBL\omronlib\programmable controller\\EIP21S_EIPS001_SOCKET_TcpOpen Passive.cxf
Open TCP Socket Active	_EIPS002_SOCKET_TcpOpenActive	Lib\FBL\omronlib\programmable controller\\EIP21S_EIPS002_SOCKET_TcpOpen Active.cxf
Close TCP Socket	_EIPS003_SOCKET_TcpClose	Lib\FBL\omronlib\programmable controller\EIP21S_EIPS003_SOCKET_TcpClose .cxf
Send via TCP Socket	_EIPS004_SOCKET_TcpSend	Lib\FBL\omronlib\programmable controller\EIP21S_EIPS004_SOCKET_TcpSend .cxf
Receive via TCP Socket	_EIPS005_SOCKET_TcpRecv	Lib\FBL\omronlib\programmable controller\EIP21S_EIPS005_SOCKET_TcpRecv .cxf

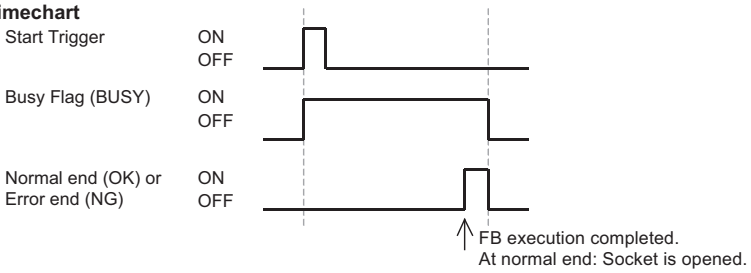
- Function Block for UDP Socket

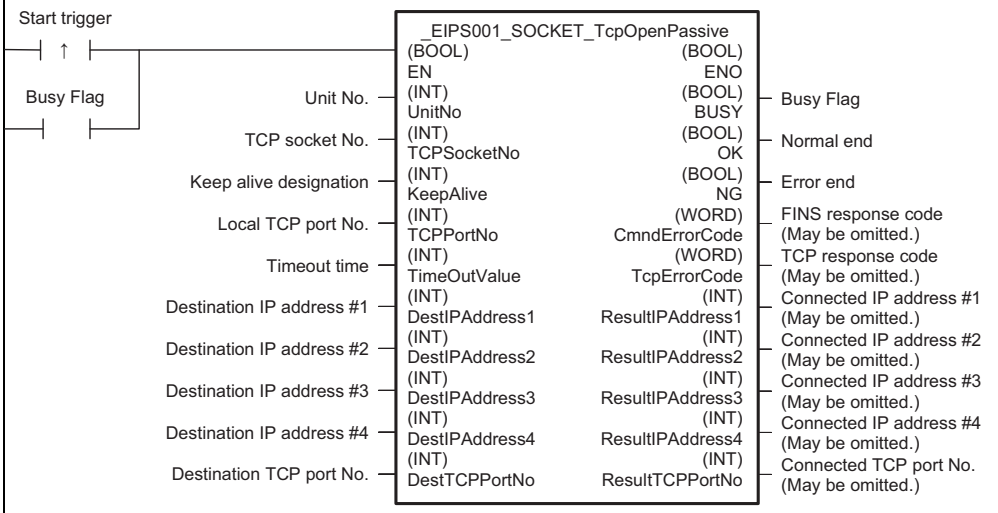
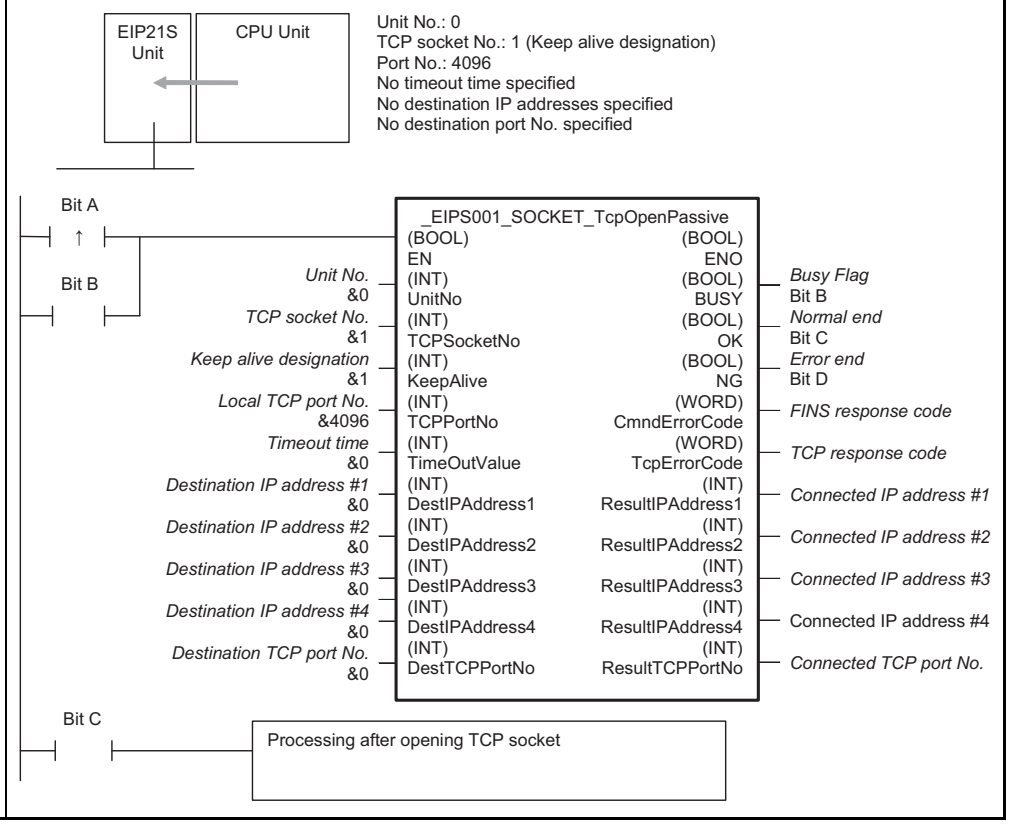
Function	Function Block Name	File Name
Open UDP Socket	_EIPS011_SOCKET_UdpOpen	Lib\FBL\omronlib\programmable controller\EIP21S_EIPS011_SOCKET_UdpOpen .cxf
Close UDP Socket	_EIPS013_SOCKET_UdpClose	Lib\FBL\omronlib\programmable controller\EIP21S_EIPS013_SOCKET_UdpClose .cxf
Receive via UDP Socket	_EIPS014_SOCKET_UdpRecv	Lib\FBL\omronlib\programmable controller\EIP21S_EIPS014_SOCKET_UdpRecv .cxf
Send via UDP Socket	_EIPS015_SOCKET_UcpSend	Lib\FBL\omronlib\programmable controller\EIP21S_EIPS015_SOCKET_UdpSend .cxf

Function Block for TCP Socket

- Common matters

Item	Details	
Applicable models	EtherNet/IP Unit	CS1W-EIP21S, CJ1W-EIP21S and CJ3M-CPU3□
	CPU Unit	CS1*-CPU**H Unit version 3.0 or later CS1D-CPU**HA/SA Unit version 4.0 or later CJ2*-CPU** Unit version 1.0 or later CJ3*-CPU** Unit version 1.0 or later
	CX-Programmer	Version 9.78 or later
Coding Language	Ladder Program	

Item	Details
Usage Conditions	■ CPU Unit Settings PLC Setup: Shared Settings for Communications Instructions in FBs • Communications Instruction Response Timeout Time (default: 2 s) • Number of retries (default: 0) ■ Commonly used sources • Communications port (logical port) ■ Allocated CIO Area • For the layout type of the allocated CIO area, use a layout type in “User settings.” Configure the setting in the Bus Unit settings of the EtherNet/IP Unit. Using CX Programmer, select User defined for Layout Type on the Status Area Tab Page. In the case of the Default setting, the function block will not work. ■ Other Parameters • The crossing of network levels is not supported. • This function block implements the socket service by CMND instruction (FINS command).
Function	Function blocks are executed for the EtherNet/IP Unit specified in Unit Number and the specified TCP socket. If communication completed abnormally, a response code to indicate the error details is output to FINS Response Code. If closing of the TCP socket completed abnormally, a response code to indicate the error details is output to TCP Response Code.
Types of Function Block Definition	Multi-cycle execution type This function block performs processing over multiple cycles after starting. The same instance cannot be used simultaneously in multiple places because the state is maintained internally.
Precautions for Correct Use	• This function block performs processing over several cycles. Whether processing is being executed can be checked from the BUSY output variable. • Upon completion of processing, OK or NG turns ON for one cycle only. Refer to these flags to detect completion of the function block processing. ■ **Timechart** 
Input Conditions of EN	As shown in the figure above, the logical OR of BUSY, which is the rising edge of the start trigger and the output of the function block, is connected to the EN.
Restrictions Input Variables	• Be sure to use a rising edge differential (↑) for the input to EN. • If the value of the input variable is outside of the range, the ENO turns OFF, and the contents of the function block are not executed.
Output Variables	• Be sure to insert the BUSY output variable in the OR circuit of the input conditions to the input variable EN so that processing is executed until completion because this processing needs to be executed over multiple cycles (refer to “Symbol”). • Do not turn ON/OFF the BUSY output variable outside of the function block. • If the layout type of the allocated CIO area is set as the Default type, ENO is turned OFF, and the function block is not executed.

Item	Details
EIPS001	The TCP OPEN REQUEST (PASSIVE) command _EIPS001_SOCKET_TcpOpenPassive
Overview	A TCP socket open request (PASSIVE) is made to the specified Built-in EtherNet/IP Unit.
Symbol	
Function	A TCP socket is opened (PASSIVE) for the EtherNet/IP Unit specified in Unit Number. The socket enters the state of waiting for a connection from another node. When a TCP connection is established, the IP address and TCP port number of the remote node are stored in the specified results storage area. If communication completed abnormally, a response code to indicate the error details is output to FINS Response Code. If opening of the TCP socket completed abnormally, a response code to indicate the error details is output to TCP Response Code.
Application Example	If contact A is turned ON, an open request for the TCP socket is issued. When the open request completes, contact C turns ON 

• Variable tables

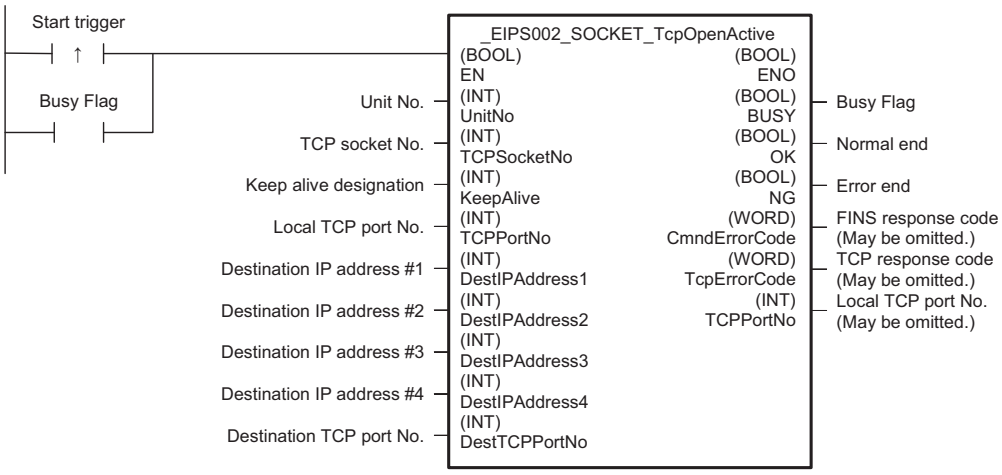
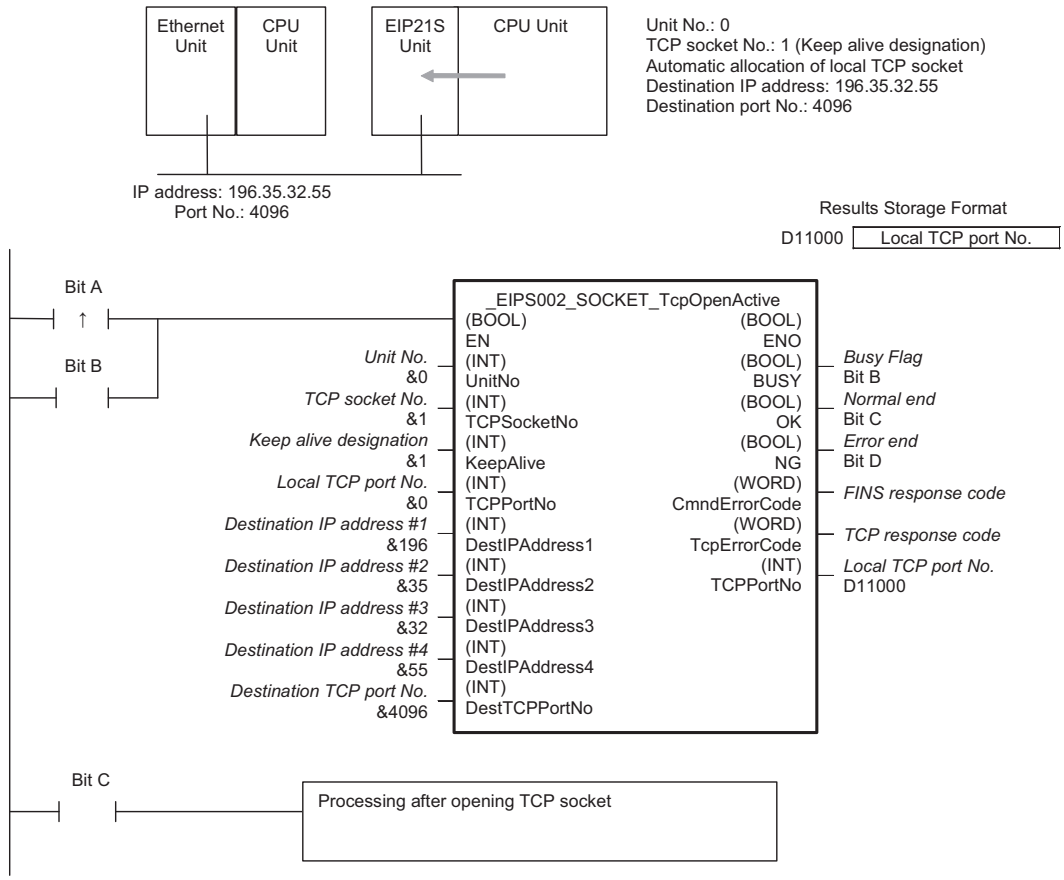
[INPUT]

Name (Japanese Language)	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to &15 #0 to #F	EIP21S Unit Number
TCP Socket No.	TCPSocketNo	INT	&1	&1 to 8	
Keep-alive specification	KeepAlive	INT	&0	&0 to &1	1: Keep-alive specification 0: Keep-alive disabled
Local TCP port number	TCPPortNo	INT	&0		
Timeout value	TimeOutValue	INT	&0	&0 to 32767	&0: Time is not monitored. (set in 100-ms increments)
Remote IP address #1	DestIPAddress1	INT	&0	&0 to &254	
Remote IP address #2	DestIPAddress2	INT	&0	&0 to &254	
Remote IP address #3	DestIPAddress3	INT	&0	&0 to &254	
Remote IP address #4	DestIPAddress4	INT	&0	&0 to &254	
Remote TCP port No.	DestTCPPortNo	INT	&0	&0 min.	&0: This will be a setting without the port number of the remote node specified. There will be a wait for a connection from any port.

[OUTPUT]

Name (Japanese Language)	Symbol name	Data Type	Scope	Details
ENO (This value can be omitted.)	ENO	BOOL		1 (ON): The function block operated normally. 0 (OFF): The function block did not start. / The function block completed abnormally.
Flag	BUSY	BOOL		Turns OFF automatically after processing completes
Normal completion	OK	BOOL		Turns ON for one cycle only when completes normally
Abnormal completion	NG	BOOL		Turns ON for one cycle only when completes abnormally
FINS completion code (This value can be omitted.)	CmndErrorCode	WORD		If an abnormal completion occurred due to a communication command level, a FINS response code is output. Refer to PASSIVE TCP OPEN REQUEST in FINS Command Reference for EtherNet/IP Units or Built-in EtherNet/IP Ports for details about the codes.
TCP completion code (This value can be omitted.)	TCPErrorCode	WORD		If an abnormal completion occurred in the TCP socket operation, the completion code of the socket service is output. Refer to 14-7-6 Response Codes for details about the codes.
Connected remote IP address #1 (This value can be omitted.)	ResultIPAddress1	INT	&0 to &254	

Name (Japanese Language)	Symbol name	Data Type	Scope	Details
Connected remote IP address #2 (This value can be omitted.)	ResultIPAddress2	INT	&0 to &254	
Connected remote IP address #3 (This value can be omitted.)	ResultIPAddress3	INT	&0 to &254	
Connected remote IP address #4 (This value can be omitted.)	ResultIPAddress4	INT	&0 to &254	
Connected remote TCP port number (This value can be omitted.)	ResultTCPPortNo	INT		

EIPS002	The TCP OPEN REQUEST (ACTIVE) command_EIPS002_SOCKET_TcpOpenActive
Overview	A TCP socket open request (ACTIVE) is made to the specified Built-in EtherNet/IP Unit.
Symbol	
Function	A TCP socket is opened (ACTIVE) for the EtherNet/IP Unit specified in Unit Number. The socket connects to another node. When a TCP connection is established, the local TCP port number is stored in the specified results storage area. If communication completed abnormally, a response code to indicate the error details is output to FINS Response Code. If opening of the TCP socket completed abnormally, a response code to indicate the error details is output to TCP Response Code.
Application Example	If contact A is turned ON, an open request for the TCP socket is issued. When the open request completes, contact C turns ON. 

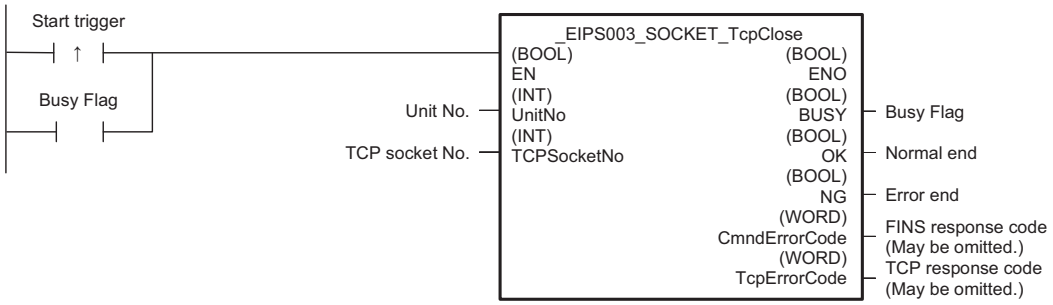
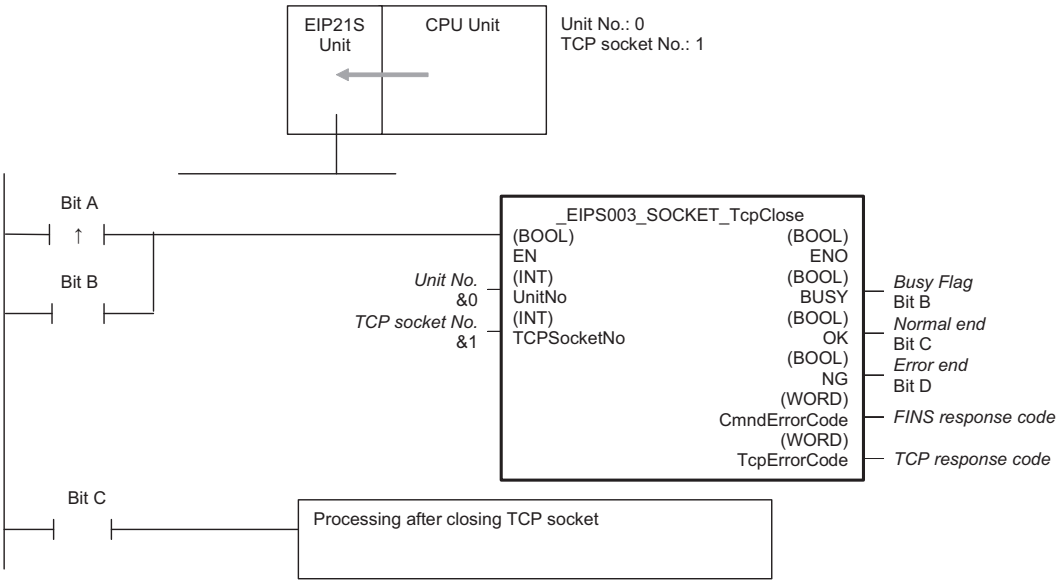
• Variable tables

[INPUT]

Name (Japanese Language)	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to &15 #0 to #F	EIP21S Unit Number
TCP Socket No.	TCPSocketNo	INT	&1	&1 to 8	
Keep-alive specification	KeepAlive	INT	&0	&0 to &1	&1: Keep-alive specification &0: Keep-alive disabled
Local TCP port number	TCPPortNo	INT	&0		If 0 is specified, an available port number is allocated automatically.
Remote IP address #1	DestIPAddress1	INT	&0	&0 to &254	
Remote IP address #2	DestIPAddress2	INT	&0	&0 to &254	
Remote IP address #3	DestIPAddress3	INT	&0	&0 to &254	
Remote IP address #4	DestIPAddress4	INT	&0	&0 to &254	
Remote TCP port No.	DestTCPPortNo	INT	&0	&1 to	

[OUTPUT]

Name (Japanese Language)	Symbol name	Data Type	Scope	Details
ENO (This value can be omitted.)	ENO	BOOL		1 (ON): The function block operated normally. 0 (OFF): The function block did not start. / The function block completed abnormally.
Flag	BUSY	BOOL		Turns OFF automatically after processing completes
Normal completion	OK	BOOL		Turns ON for one cycle only when completes normally
Abnormal completion	NG	BOOL		Turns ON for one cycle only when completes abnormally
FINS communication code (This value can be omitted.)	CmndErrorCode	WORD		If an abnormal completion occurred due to a communication command level, a FINS response code is output. Refer to ACTIVE TCP OPEN REQUEST in FINS Command Reference for EtherNet/IP Units or Built-in EtherNet/IP Ports for details about the codes.
TCP completion code (This value can be omitted.)	TcpErrorCode	WORD		If an abnormal completion occurred in the TCP socket operation, the completion code of the socket service is output. Refer to 14-7-6 Response Codes for details about the codes.
Local TCP port number (This value can be omitted.)	TCPPortNo	INT	&1 to	

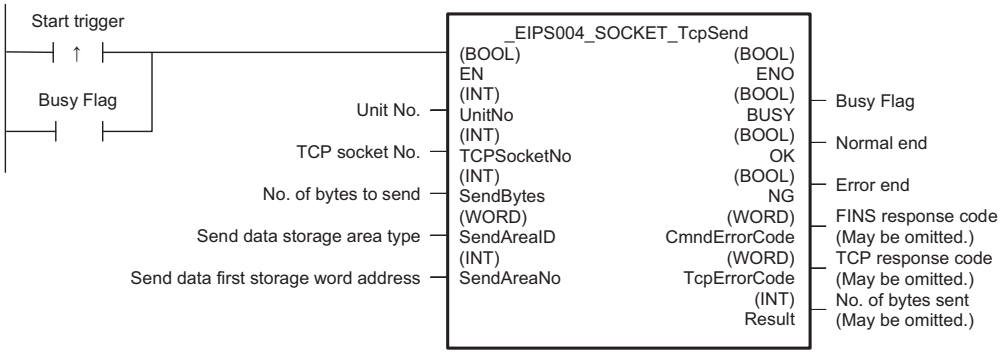
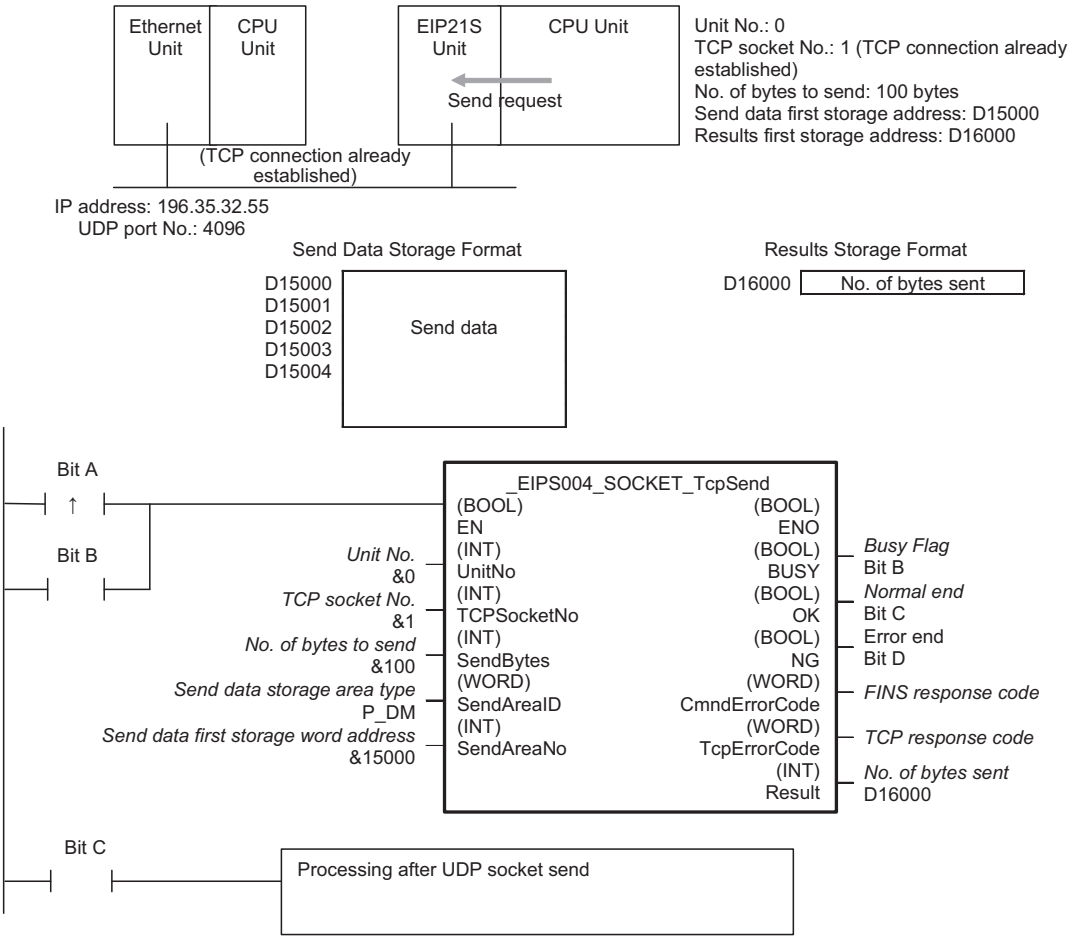
EIPS003	The TCP CLOSE REQUEST command_EIPS003_SOCKET_TcpClose
Overview	TCP socket close processing is performed for the specified Built-in EtherNet/IP Unit.
Symbol	
Function	The specified TCP socket is closed for the EtherNet/IP Unit specified in Unit Number. If communication completed abnormally, a response code to indicate the error details is output to FINS Response Code. If closing of the TCP socket completed abnormally, a response code to indicate the error details is output to TCP Response Code.
Application Example	If contact A is turned ON, a close request for the TCP socket is issued. When the close processing completes, contact C turns ON. 

[INPUT]

Name (Japanese Language)	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to &15 #0 to #F	EIP21S Unit Number
TCP Socket No.	TCPSocketNo	INT	&1	&1 to 8	

[OUTPUT]

Name (Japanese Language)	Symbol name	Data Type	Scope	Details
ENO (This value can be omitted.)	ENO	BOOL		1 (ON): The function block operated normally. 0 (OFF): The function block did not start. / The function block completed abnormally.
Flag	BUSY	BOOL		Turns OFF automatically after processing completes
Normal completion	OK	BOOL		Turns ON for one cycle only when completes normally
Abnormal completion	NG	BOOL		Turns ON for one cycle only when completes abnormally
FINS communication code (This value can be omitted.)	CmndErrorCode	WORD		If an abnormal completion occurred due to a communication command level, a FINS response code is output. Refer to ACTIVE TCP OPEN REQUEST in FINS Command Reference for EtherNet/IP Units or Built-in EtherNet/IP Ports for details about the codes.
TCP completion code (This value can be omitted.)	TcpErrorCode	WORD		If an abnormal completion occurred in the TCP socket operation, the completion code of the socket service is output. Refer to 14-7-6 Response Codes for details about the codes.

EIPS004	The TCP SEND REQUEST command _EIPS004_SOCKET_TcpSend
Overview	A TCP socket send request is made to the specified Built-in EtherNet/IP Unit.
Symbol	
Function	The send request command of the TCP socket is issued using the specified TCP socket for the EtherNet/IP Unit specified in Unit Number. When receive processing is performed normally, the number of sent bytes is stored in the specified results storage area. If the request command itself completed abnormally, a response code to indicate the error details is output to FINS Response Code. If the request command itself completes normally but TCP socket sending completed abnormally, a response code to indicate the error details is output to TCP Response Code.
Application Example	If contact A is turned ON, a close request for the TCP socket is issued. When the close processing completes, contact C turns ON. 

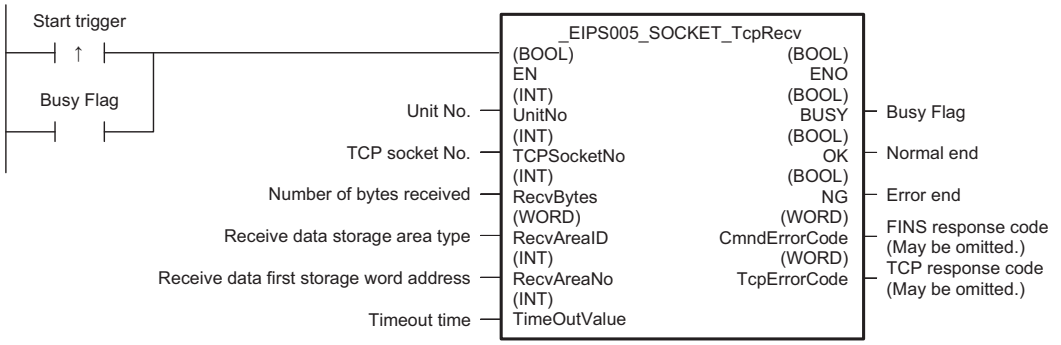
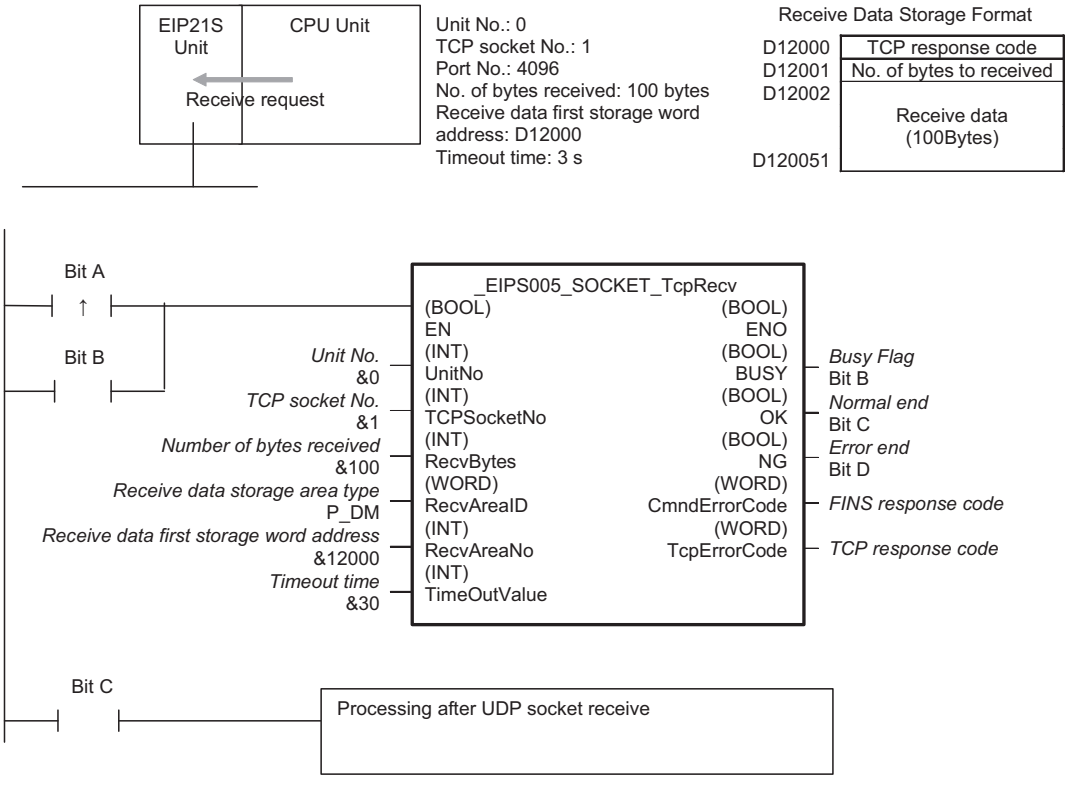
• Variable tables

[INPUT]

Name (Japanese Language)	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to &15 #0 to #F	EIP21S Unit Number
TCP Socket No.	TCPSocketNo	INT	&1	&1 to 8	
Number of bytes sent	SendBytes	INT	&1	&1 to &1980	
Word type of sent data storage	SendAreaID	WORD	#0082	See left column.	P_CIO?(#00B0): CIO P_WR?(#00B1): WR P_HR?(#00B2): HR P_DM?(#0082): DM P_EM0?(#0050) to P_EMC?(#005C): EM bank0 to C
Starting word number of sent data storage	SendAreaNo	INT	&0		

[OUTPUT]

Name (Japanese Language)	Symbol name	Data Type	Scope	Details
ENO (This value can be omitted.)	ENO	BOOL		1 (ON): The function block operated normally. 0 (OFF): The function block did not start. / The function block completed abnormally.
Flag	BUSY	BOOL		Turns OFF automatically after processing completes
Normal completion	OK	BOOL		Turns ON for one cycle only when completes normally
Abnormal completion	NG	BOOL		Turns ON for one cycle only when completes abnormally
FINS completion code (This value can be omitted.)	CmndErrorCode	WORD		If an abnormal completion occurred due to a communication command level, a FINS response code is output. Refer to TCP CLOSE REQUEST in FINS Command Reference for EtherNet/IP Units or Built-in EtherNet/IP Ports for details about the codes.
TCP completion code (This value can be omitted.)	TcpErrorCode	WORD		If an abnormal completion occurred in the TCP socket operation, the completion code of the socket service is output. Refer to 14-7-6 Response Codes for details about the codes.
Number of bytes sent result (This value can be omitted.)	Result	INT		Number of bytes actually sent

EIPS005	The TCP RECEIVED REQUEST command _EIPS005_SOCKET_TcpRecv
Overview	A TCP socket receive request is made to the specified Built-in EtherNet/IP Unit.
Symbol	
Function	The receive request command of the TCP socket is issued using the specified TCP socket for the EtherNet/IP Unit specified in Unit Number. When receive processing is performed normally, the TCP response code (#0000), number of received bytes, and received data are stored in the specified results storage area. If the request command itself completed abnormally, a response code to indicate the error details is output to FINS Response Code. If the request command itself completes normally but TCP socket receiving completed abnormally, a response code to indicate the error details is output to the beginning of the results storage area and TCP Response Code.
Application Example	If contact A is turned ON, a receive request for the TCP socket is issued. When the receive request completes, contact C turns ON. 

• Variable tables

[INPUT]

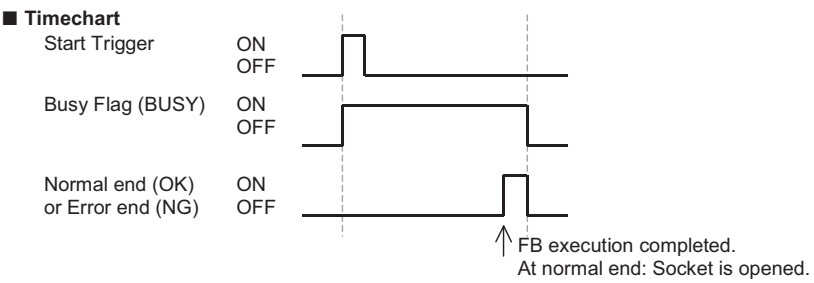
Name (Japanese Language)	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to &15 #0 to #F	EIP21S Unit Number
TCP Socket No.	TCPSocketNo	INT	&1	&1 to 8	
Number of bytes sent	RecvBytes	INT	&1	&1 to &1980	When an odd number of bytes is specified, zero is stored in the lower side of the final word.
Word type of sent data storage	SendAreaID	WORD	#0082	See left column.	P_CIO?(#00B0): CIO P_WR?(#00B1): WR P_HR?(#00B2): HR P_DM?(#0082): DM P_EM0?(#0050) to P_EMC?(#005C): EM bank0 to C
Starting word number of sent data storage	RecvAreaNo	INT	&0		
Timeout value	TimeOutValue	INT	&0		&0: Time is not monitored. set in 100-ms increments

[OUTPUT]

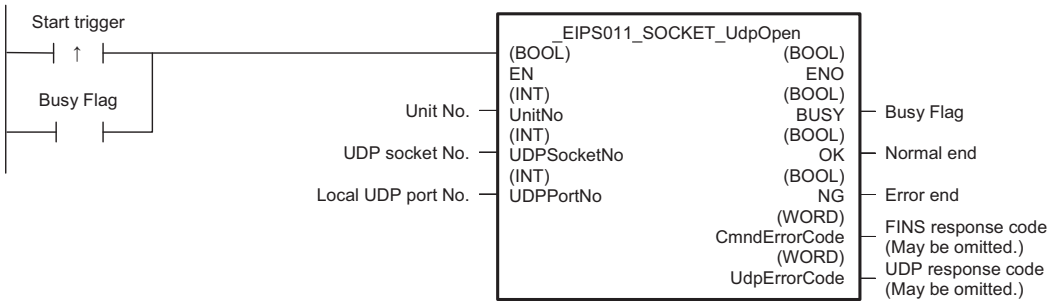
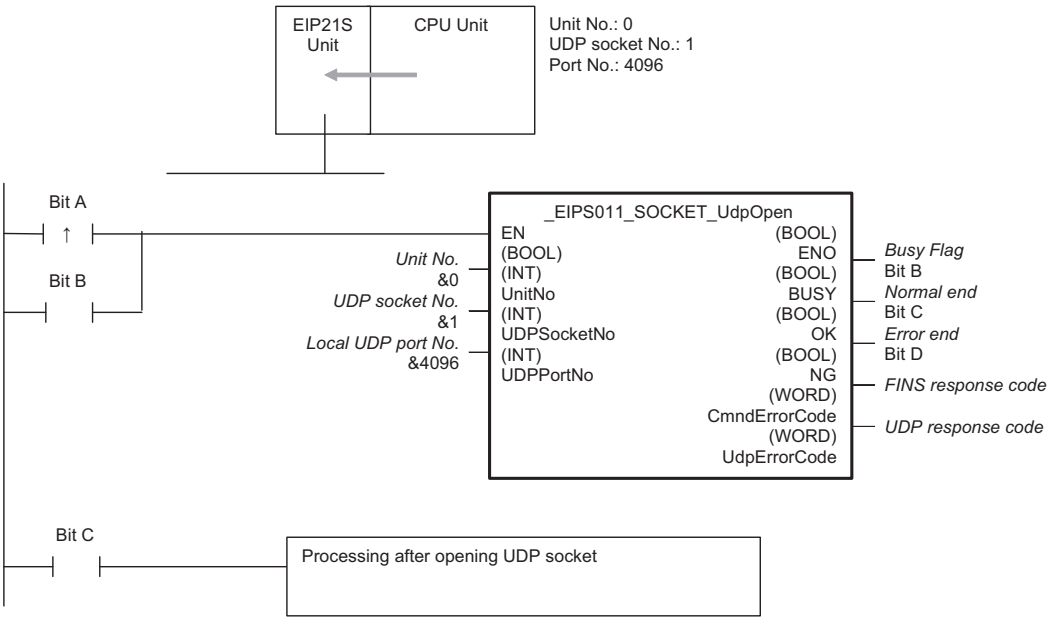
Name (Japanese Language)	Symbol name	Data Type	Scope	Details
ENO (This value can be omitted.)	ENO	BOOL		1 (ON): The function block operated normally. 0 (OFF): The function block did not start. / The function block completed abnormally.
Flag	BUSY	BOOL		Turns OFF automatically after processing completes
Normal completion	OK	BOOL		Turns ON for one cycle only when completes normally
Abnormal completion	NG	BOOL		Turns ON for one cycle only when completes abnormally
FINS completion code (This value can be omitted.)	CmndErrorCode	WORD		If an abnormal completion occurred due to a communication command level, a FINS response code is output. Refer to TCP CLOSE REQUEST in FINS Command Reference for EtherNet/IP Units or Built-in EtherNet/IP Ports for details about the codes.
TCP completion code (This value can be omitted.)	TcpErrorCode	WORD		If an abnormal completion occurred in the TCP socket operation, the completion code of the socket service is output. Refer to 14-7-6 Response Codes for details about the codes.

Function Block for UDP Socket

• Common matters

Item	Details	
Applicable models	EtherNet/IP Unit	CS1W-EIP21S, CJ1W-EIP21S and CJ3M-CPU3□
	CPU Unit	CS1*-CPU**H Unit version 3.0 or later CS1D-CPU**HA/SA Unit version 4.0 or later CJ2*-CPU** Unit version 1.0 or later CJ3*-CPU** Unit version 1.0 or later
	CX-Programmer	Version 9.78 or later
Coding Language	Ladder Program	
Usage Conditions	■ CPU Unit Settings PLC Setup: Shared Settings for Communications Instructions in FBs • Communications Instruction Response Timeout Time (default: 2 s) • Number of retries (default: 0) ■ Commonly used sources • Communications port (logical port) ■ Allocated CIO Area • For the layout type of the allocated CIO area, use a layout type in “User settings.” • Configure the setting in the Bus Unit settings of the EtherNet/IP Unit. Using CX Programmer, select User defined for Layout Type on the Status Area Tab Page. • In the case of the Default setting, the function block will not work. ■ Other Parameters • The crossing of network levels is not supported. • This function block implements the socket service by CMND instruction (FINS command).	
Function	Function blocks are executed for the EtherNet/IP Unit specified in Unit Number and the specified UDP socket. If communication completed abnormally, a response code to indicate the error details is output to FINS Response Code. If opening of the UDP socket completed abnormally, a response code to indicate the error details is output to UDP Response Code.	
Types of Function Block Definition	Multi-cycle execution type This function block performs processing over multiple cycles after starting. The same instance cannot be used simultaneously in multiple places because the state is maintained internally.	
Precautions for Correct Use	• This function block performs processing over several cycles. Whether processing is being executed can be checked from the BUSY output variable. • Upon completion of processing, OK or NG turns ON for one cycle only. Refer to these flags to detect completion of the function block processing. ■ **Timechart**  	
Input Conditions of EN	As shown in the figure above, the logical OR of BUSY, which is the rising edge of the start trigger and the output of the function block, is connected to the EN.	

Item	Details
Restrictions Input Variables	• Be sure to use a rising edge differential (↑) for the input to EN. • If the value of the input variable is outside of the range, the ENO turns OFF, and the contents of the function block are not executed.
Output Variables	• Be sure to insert the BUSY output variable in the OR circuit of the input conditions to the input variable EN so that processing is executed until completion because this processing needs to be executed over multiple cycles (refer to “Symbol”). • Do not turn ON/OFF the BUSY output variable outside of the function block. • If the layout type of the allocated CIO area is set as the Default type, ENO is turned OFF, and the function block is not executed.

EIPS011	The UDP OPEN REQUEST command _EIPS011_SOCKET_UdpOpen
Overview	A UDP socket open request is made to the specified Built-in EtherNet/IP Unit.
Symbol	
Function	The specified UDP socket is opened for the EtherNet/IP Unit specified in Unit Number. If communication completed abnormally, a response code to indicate the error details is output to FINS Response Code. If opening of the UDP socket completed abnormally, a response code to indicate the error details is output to UDP Response Code.
Application Example	If contact A is turned ON, an open request for the UDP socket is issued. When the open request completes, contact C turns ON. 

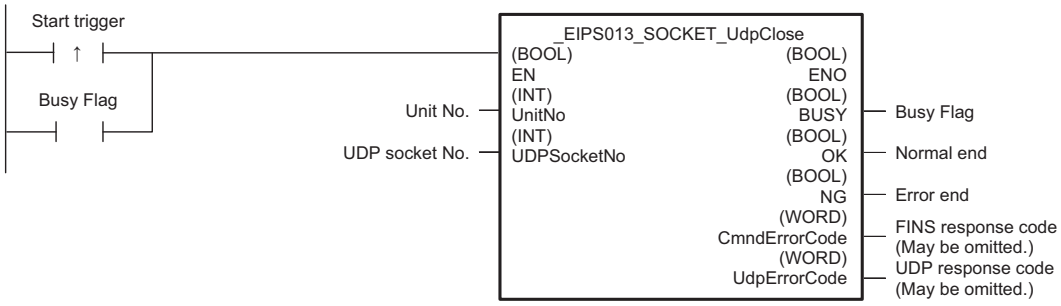
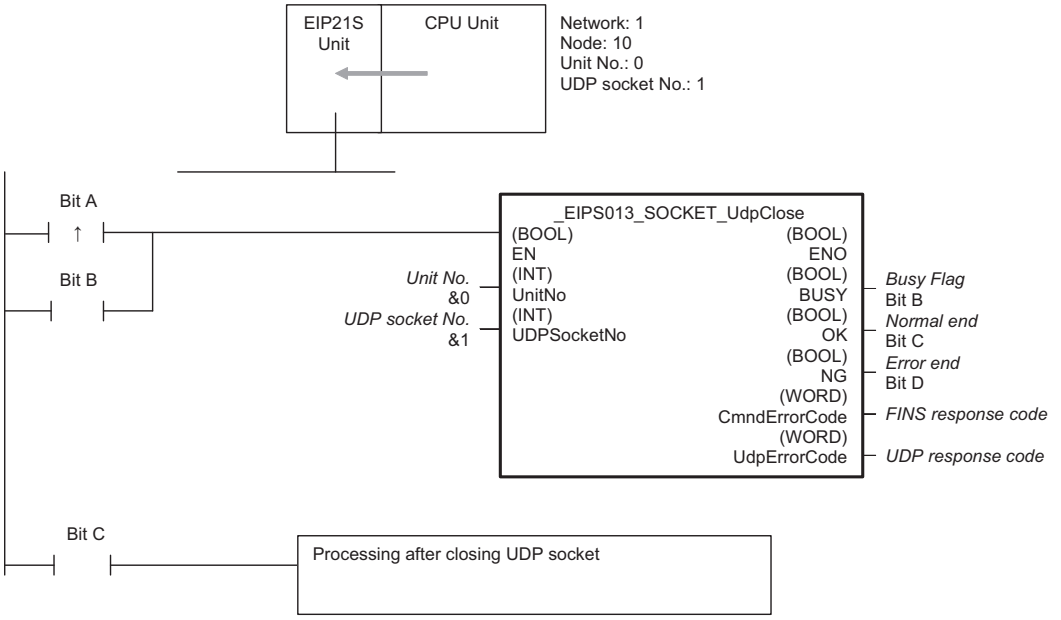
• Variable tables

[INPUT]

Name (Japanese Language)	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to &15 #0 to #F	EIP21S Unit Number
UDP Socket No.	UDPSocketNo	INT	&1	&1 to 8	
Local UDP port number	UDPPortNo	INT	&0		

[OUTPUT]

Name (Japanese Language)	Symbol name	Data Type	Scope	Details
ENO (This value can be omitted.)	ENO	BOOL		1 (ON): The function block operated normally. 0 (OFF): The function block did not start. / The function block completed abnormally.
Flag	BUSY	BOOL		Turns OFF automatically after processing completes
Normal completion	OK	BOOL		Turns ON for one cycle only when completes normally
Abnormal completion	NG	BOOL		Turns ON for one cycle only when completes abnormally
FINS completion code (This value can be omitted.)	CmndErrorCode	WORD		If an abnormal completion occurred due to a communication command level, a FINS response code is output. Refer to TCP CLOSE REQUEST in FINS Command Reference for EtherNet/IP Units or Built-in EtherNet/IP Ports for details about the codes.
UDP completion code (This value can be omitted.)	UdpErrorCode	WORD		If an abnormal completion occurred in the TCP socket operation, the completion code of the socket service is output. Refer to 14-7-6 Response Codes for details about the codes.

EIPS013	The UDP CLOSE REQUEST command _EIPS013_SOCKET_UdpClose
Overview	UDP socket close processing is performed for the specified Built-in EtherNet/IP Unit.
Symbol	
Function	The UDP socket is closed for the EtherNet/IP Unit specified in Unit Number. If communication completed abnormally, a response code to indicate the error details is output to FINS Response Code. If closing of the UDP socket completed abnormally, a response code to indicate the error details is output to UDP Response Code.
Application Example	If contact A is turned ON, a close request for the UDP socket is issued. When the close processing completes, contact C turns ON. 

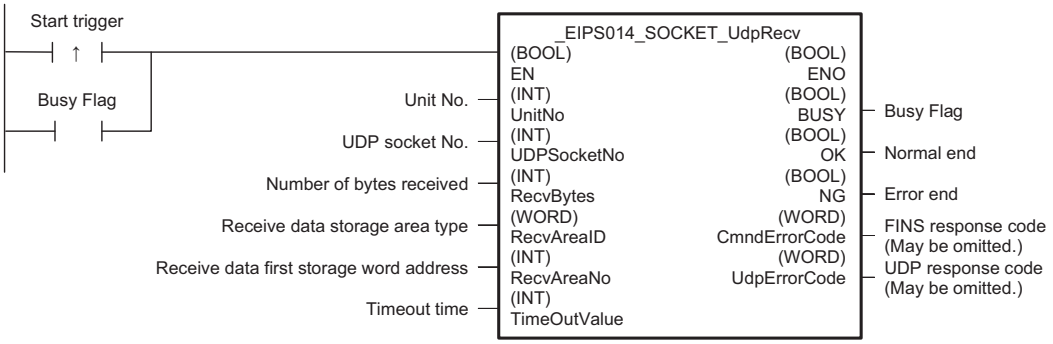
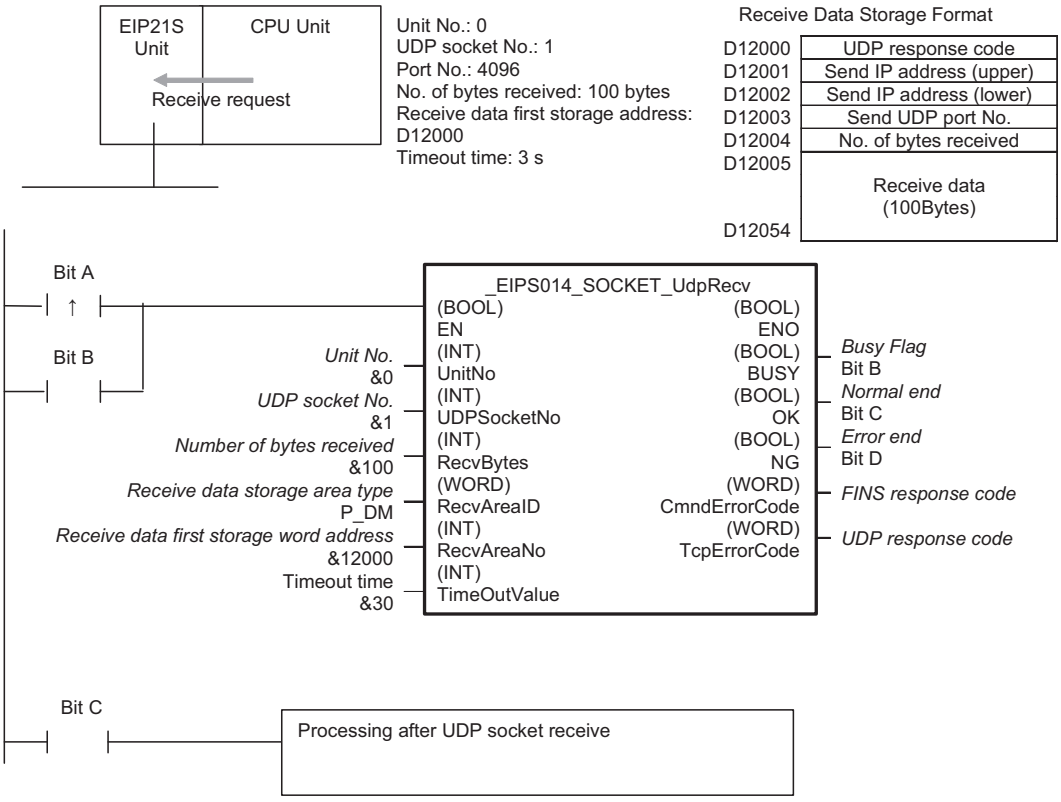
- Variable tables

[INPUT]

Name (Japanese Language)	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to &15 #0 to #F	EIP21S Unit Number
UDP Socket No.	UDPSocketNo	INT	&1	&1 to 8	

[OUTPUT]

Name (Japanese Language)	Symbol name	Data Type	Scope	Details
ENO (This value can be omitted.)	ENO	BOOL		1 (ON): The function block operated normally. 0 (OFF): The function block did not start. / The function block completed abnormally.
Flag	BUSY	BOOL		Turns OFF automatically after processing completes
Normal completion	OK	BOOL		Turns ON for one cycle only when completes normally
Abnormal completion	NG	BOOL		Turns ON for one cycle only when completes abnormally
FINS completion code (This value can be omitted.)	CmndErrorCode	WORD		If an abnormal completion occurred due to a communication command level, a FINS response code is output. Refer to TCP CLOSE REQUEST in FINS Command Reference for EtherNet/IP Units or Built-in EtherNet/IP Ports for details about the codes.
UDP completion code (This value can be omitted.)	UdpErrorCode	WORD		If an abnormal completion occurred in the TCP socket operation, the completion code of the socket service is output. Refer to 14-7-6 Response Codes for details about the codes.

EIPS014	The UDP RECEIVED REQUEST command _EIPS014_SOCKET_UdpRecv
Overview	A UDP socket receive request is made to the specified Built-in EtherNet/IP Unit.
Symbol	
Function	The receive request command of the UDP socket is issued using the specified UDP socket number for the EtherNet/IP Unit specified in Unit Number. When receive processing is performed normally, the UDP response code (#0000), the send source IP address, send source UDP port number, number of received bytes, and received data are stored in the specified results storage area. If the request command itself completed abnormally, a response code to indicate the error details is output to FINS Response Code. If the request command itself completes normally but UDP socket receiving completed abnormally, a response code to indicate the error details is output to the beginning of the specified results storage area and UDP Response Code.
Application Example	If contact A is turned ON, a receive request for the UDP socket is issued. When the receive request completes, contact C turns ON. 

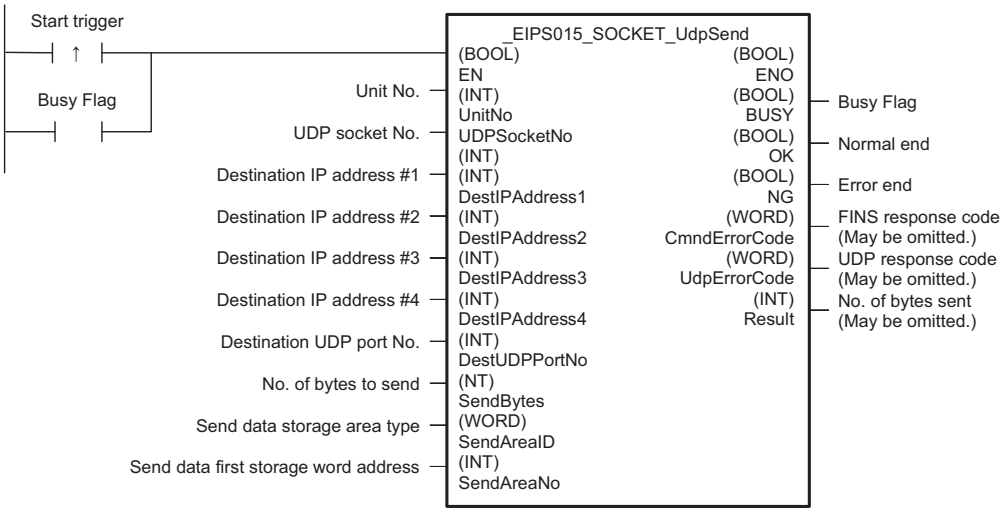
• Variable tables

[INPUT]

Name (Japanese Language)	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to &15 #0 to #F	EIP21S Unit Number
UDP Socket No.	UDPSocketNo	INT	&1	&1 to &8	
Number of bytes of received data	RecvBytes	INT	&1	&1 to &1974	When an odd number of bytes is specified, zero is stored in the lower side of the final word.
Word type of received data storage	RecvAreaID	WORD	#0082	See left column.	P_CIO?(#00B0): CIO P_WR?(#00B1): WR P_HR?(#00B2): HR P_DM?(#0082): DM P_EM0?(#0050) to P_EMC?(#005C): EM bank0 to C
Starting word number of received data storage	RecvAreaNo	INT	&0		
Timeout value	TimeOutValue	INT	&0		&0: Time is not monitored. set in 100-ms increments

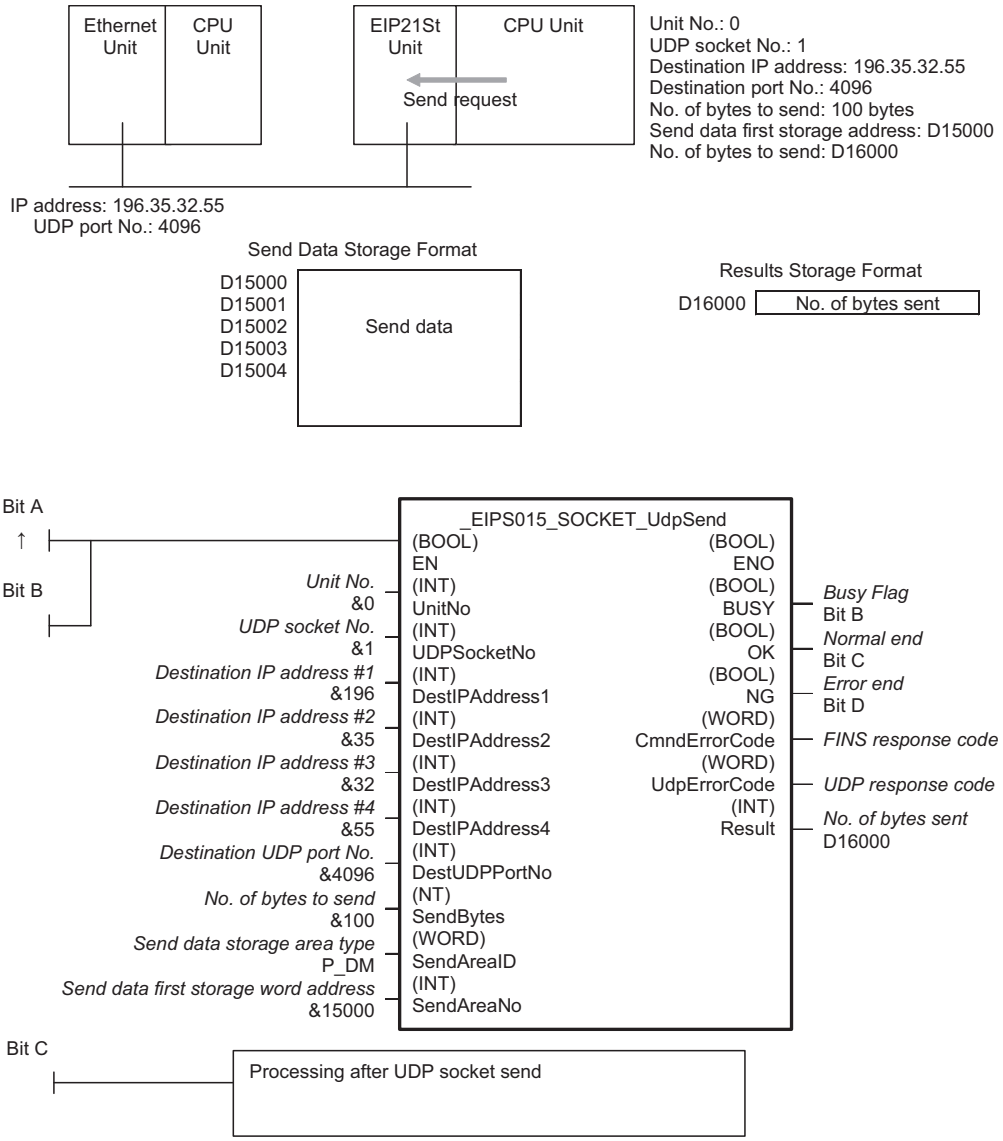
[OUTPUT]

Name (Japanese Language)	Symbol name	Data Type	Scope	Details
ENO (This value can be omitted.)	ENO	BOOL		1 (ON): The function block operated normally. 0 (OFF): The function block did not start. / The function block completed abnormally.
Flag	BUSY	BOOL		Turns OFF automatically after processing completes
Normal completion	OK	BOOL		Turns ON for one cycle only when completes normally
Abnormal completion	NG	BOOL		Turns ON for one cycle only when completes abnormally
FINS completion code (This value can be omitted.)	CmndErrorCode	WORD		If an abnormal completion occurred due to a communication command level, a FINS response code is output. Refer to UDP RECEIVE REQUEST in FINS Command Reference for EtherNet/IP Units or Built-in EtherNet/IP Ports for details about the codes.
UDP completion code (This value can be omitted.)	UdpErrorCode	WORD		If an abnormal completion occurred in the UDP socket operation, the completion code of the socket service is output. Refer to 14-7-6 Response Codes for details about the codes.

EIPS015	The UDP SEND REQUEST command _EIPS015_SOCKET_UdpSend
Overview	A UDP socket send request is made to the specified Built-in EtherNet/IP Unit.
Symbol	
Function	The send request command of the UDP socket is issued to the specified IP address and send destination UDP port number for the EtherNet/IP Unit specified in Unit Number. When send processing is performed normally, the number of sent bytes is stored. If the request command itself completed abnormally, a response code to indicate the error details is output to FINS Response Code. If the request command itself completes normally but UDP socket sending completed abnormally, a response code to indicate the error details is output to UDP Response Code.

Application Example

If contact A is turned ON, a send request for the UDP socket is issued.
When the send request completes, contact C turns ON.



• Variable tables

[INPUT]

Name (Japanese Language)	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to &15 #0 to #F	EIP21S Unit Number
UDP Socket No.	UDPSocketNo	INT	&1	&1 to &8	
Destination IP address #1	DestIPAddress1	INT	&0	&0 to &254	
Destination IP address #2	DestIPAddress2	INT	&0	&0 to &254	
Destination IP address #3	DestIPAddress3	INT	&0	&0 to &254	
Destination IP address #4	DestIPAddress4	INT	&0	&0 to &254	
Destination UDP port number	DestUDPProtNo	INT	&0		
Number of bytes sent	SendBytes	INT	&1	&1 to &1974	
Word type of sent data storage	SendAreaID	INT	#0082	See left	P_CIO?(#00B0): CIO P_WR?(#00B1): WR P_HR?(#00B2): HR P_DM?(#0082): DM P_EM0?(#0050) to P_EMC?(#005C): EM bank0 to C
Starting word number of sent data storage	SendAreaNo	WORD	&0		

[OUTPUT]

Name (Japanese Language)	Symbol name	Data Type	Scope	Details
ENO (This value can be omitted.)	ENO	BOOL		1 (ON): The function block operated normally. 0 (OFF): The function block did not start. / The function block completed abnormally.
Flag	BUSY	BOOL		Turns OFF automatically after processing completes
Normal completion	OK	BOOL		Turns ON for one cycle only when completes normally
Abnormal completion	NG	BOOL		Turns ON for one cycle only when completes abnormally
FINS completion code (This value can be omitted.)	CmndErrorCode	WORD		If an abnormal completion occurred due to a communication command level, a FINS response code is output. Refer to FINS Command Reference for EtherNet/IP Units or Built-in EtherNet/IP Ports for details about the codes.
UDP completion code (This value can be omitted.)	UdpErrorCode	WORD		If an abnormal completion occurred in the UDP socket operation, the completion code of the socket service is output. Refer to 14-7-6 Response Codes for details about the codes.
Number of bytes sent result (This value can be omitted.)	Result	INT		Number of bytes actually sent

Appendix M
Function Block for Modbus Client

Function blocks for the Modbus client are available for TCP and for UDP. The function blocks corresponding to each Modbus function are as follows:

- Function Block for Modbus TCP Client

Function	Function Block Name	Function Code	Modbus Function
Read Coils	_EIPS020_ModbusTcp_Fun01	0x01	Read Coils
Read Holding Registers	_EIPS021_ModbusTcp_Fun03	0x03	Read Holding Registers
Write Single Coil	_EIPS022_ModbusTcp_Fun05	0x05	Write Single Coil
Write Single Register	_EIPS023_ModbusTcp_Fun06	0x06	Write Single Register
Write Multiple Coils	_EIPS024_ModbusTcp_Fun0F	0x0F	Write Multiple Coils
Write Multiple Registers	_EIPS025_ModbusTcp_Fun10	0x10	Write Multiple Registers
The TCP OPEN REQUEST (ACTIVE) command	_EIPS002_SOCKET_TcpOpenActive	-	-
The TCP CLOSE REQUEST command	_EIPS003_SOCKET_TcpClose	-	-

- Function Block for Modbus UDP Client

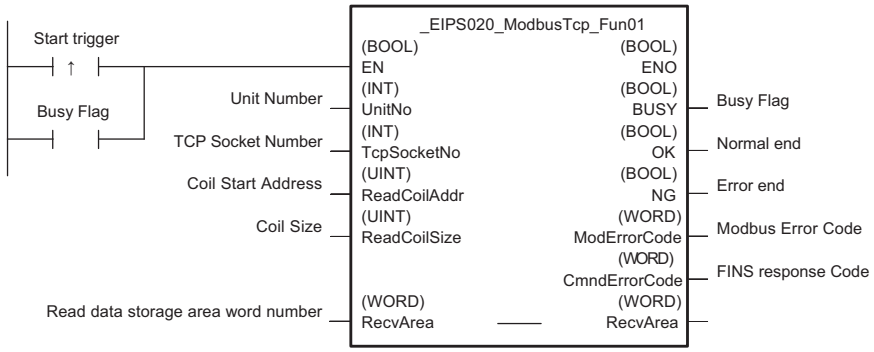
Function	Function Block Name	Function Code	Modbus Function
Read Coils	_EIPS030_ModbusUdp_Fun01	0x01	Read Coils
Read Holding Registers	_EIPS031_ModbusUdp_Fun03	0x03	Read Holding Registers
Write Single Coil	_EIPS032_ModbusUdp_Fun05	0x05	Write Single Coil
Write Single Register	_EIPS033_ModbusUdp_Fun06	0x06	Write Single Register
Write Multiple Coils	_EIPS034_ModbusUdp_Fun0F	0x0F	Write Multiple Coils
Write Multiple Registers	_EIPS035_ModbusUdp_Fun10	0x10	Write Multiple Registers
The UDP OPEN REQUEST command	_EIPS011_SOCKET_UdpOpen	-	-
The UDP CLOSE REQUEST command	_EIPS013_SOCKET_UdoClost	-	-

Function Block for Modbus TCP Client

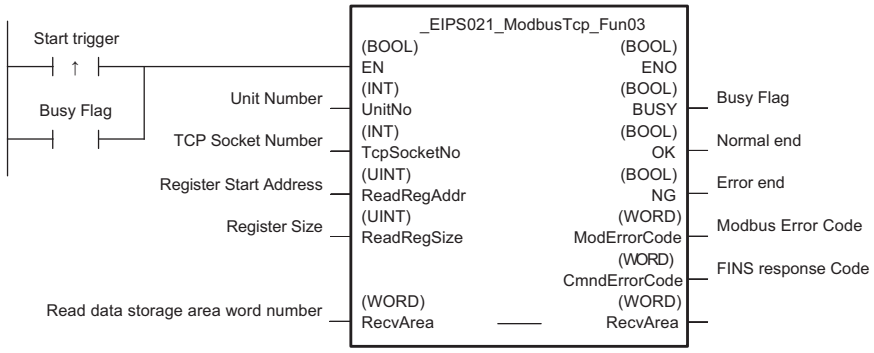
EIPS 020 to 025	Modbus TCP Client _EIPS**_ModbusTcp_Fun**
Overview	A Modbus TCP command is issued using a socket service function for the specified Built-in EtherNet/IP Unit.

Symbol

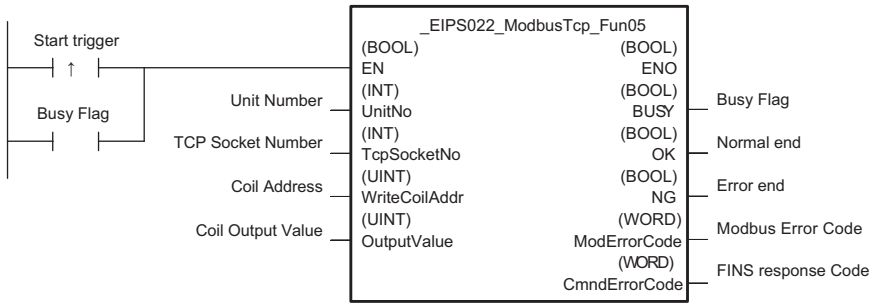
■ Function01: Read Coils



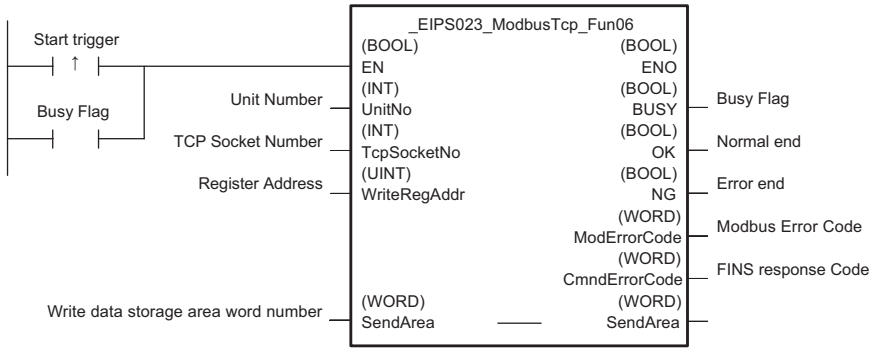
■ Function03: Read Holding Registers

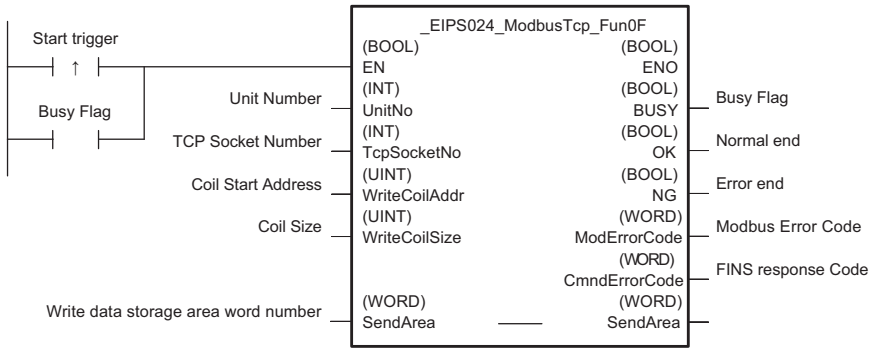


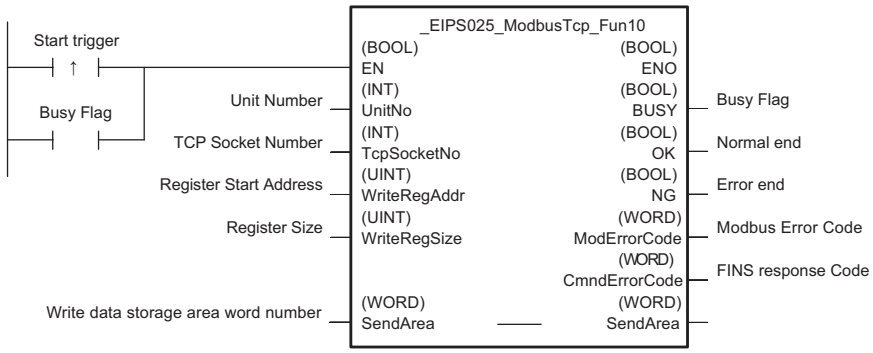
■ Function05: Write Single Coil

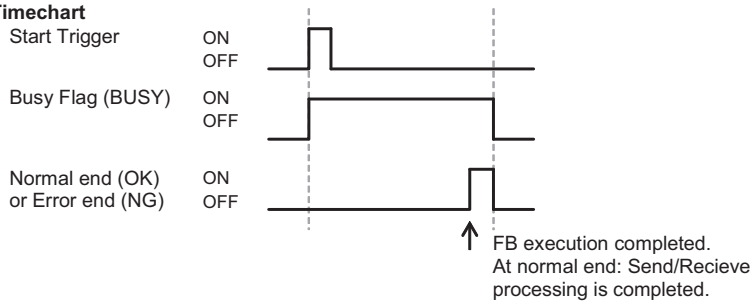


■ Function06: Write Single Register

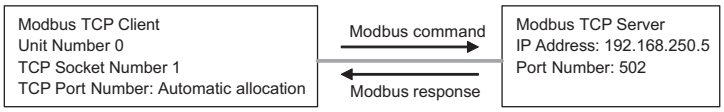


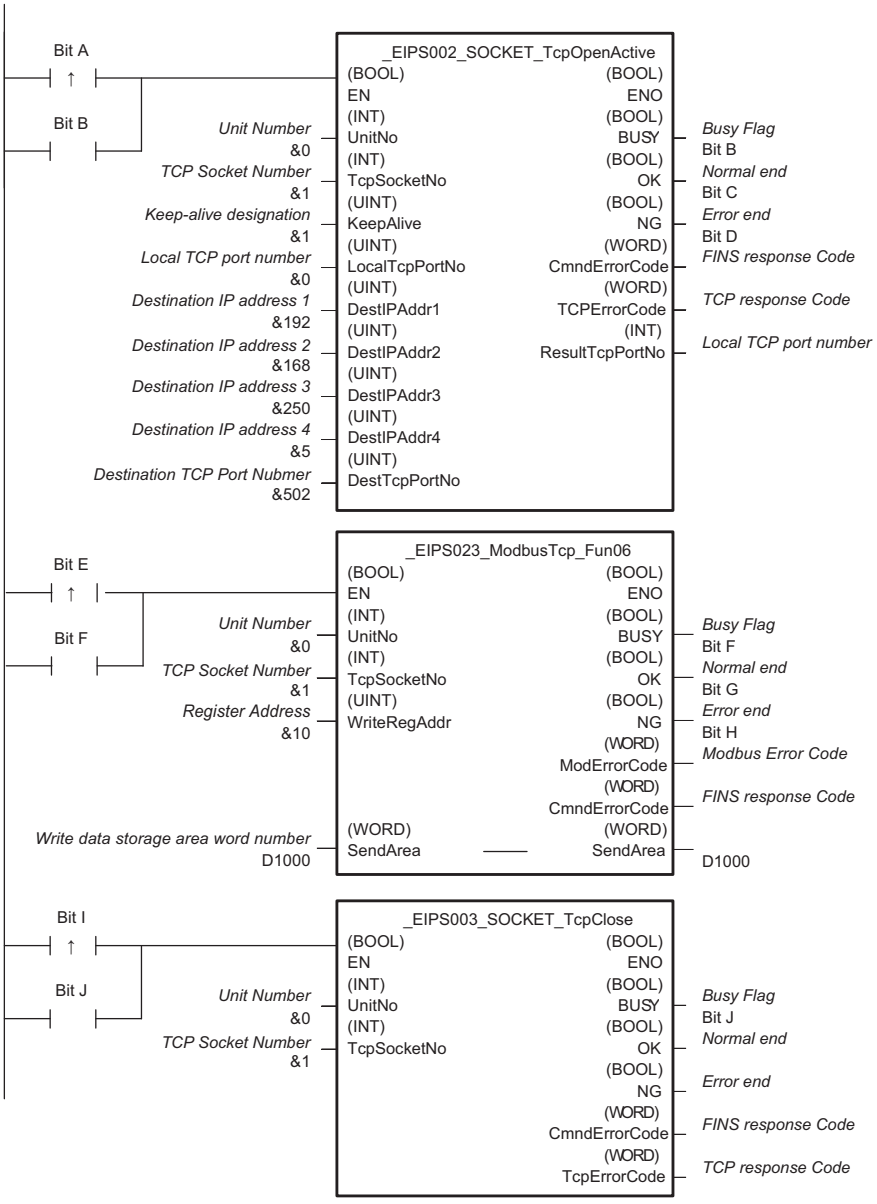
<table>
<tr><td>Symbol</td><td colspan="2">■ Function0F: Write Multiple Coils
 

■ Function10: Write Multiple Registers
 
</td></tr>
<tr><td>File Name</td><td colspan="2">_EIPS020_ModbusTcp_Fun01.cxf: Function 01 (Read Coils)
_EIPS021_ModbusTcp_Fun03.cxf: Function 03 (Read Holding Registers)
_EIPS022_ModbusTcp_Fun05.cxf: Function 05 (Write Single Coil)
_EIPS023_ModbusTcp_Fun06.cxf: Function 06 (Write Single Register)
_EIPS024_ModbusTcp_Fun0F.cxf: Function 0F (Write Multiple Coils)
_EIPS025_ModbusTcp_Fun10.cxf: Function 10 (Write Multiple Registers)</td></tr>
<tr><td rowspan="3">Application Example</td><td>EtherNet/IP Unit</td><td>CJ1W-EIP21S Unit Version 1.0 or later
CJ3M-CPU3□ Unit Version 1.1 or later</td></tr>
<tr><td>CPU Unit</td><td>CJ2H-CPU6□(-EIP), CJ2M-CPU□□, CJ3M-CPU□□ (Cannot be used in CS1 CPU Unit)</td></tr>
<tr><td>CX-Programmer</td><td>Version 9.78 or later</td></tr>
<tr><td>Coding Language</td><td colspan="2">Ladder Program</td></tr>
<tr><td>Usage Conditions</td><td colspan="2">■ CPU Unit Settings
PLC Setup: Shared Settings for Communications Instructions in FBs
• Communications Instruction Response Timeout Time (default: 2 s)
• Number of retries (default: 0)
■ Commonly used sources
• Communications ports (internal logical ports)
■ Other Parameters
• The crossing of network levels is not supported.
• This function block implements the socket service by CMND2 instruction (FINS command).
TCP RECEIVE REQUEST: FINS Commands 2712
TCP SEND REQUEST: FINS Commands 2713</td></tr>
</table>

<table>
<tr><td>Function</td><td>■ Operation of function block
• On the rising edge of the start trigger, a Modbus command is issued using the TCP socket specified in TcpSocketNo for the EtherNet/IP Unit specified in UnitNo.
• In the case of the write command, the data is written to the address specified in Register/Coil (Start) Address.
• In the case of the read command, the data is read from the address specified in Register/Coil (Start) Address.
• Specify the words of sent data and received data directly in I/O memory with an I/O variable.
• If sending is processed normally, the One Cycle ON when Function Block Completes Normally Flag (OK) will turn ON. The error code (ModErrorCode/CmndErrCode) will be #0000.
• If an error code is received from the Modbus server, the One Cycle ON when Function Block Completes Abnormally Flag (NG) will turn ON and the Modbus error code will be stored in Modbus Error Code (ModErrorCode).
• When there is a FINS communication error for the CMND2 instruction, the One Cycle ON when Function Block Completes Abnormally Flag (NG) will turn ON and the FINS completion code will be stored in FINS Completion Code (CmndErrorCode).
• This function block is executed by the TCP socket service function using the CMND2 instruction. Execute the socket open processing before executing the function block. (_EIPS002_SOCKET_TcpOpen Active) For the TCP socket number to use with the function block, use the socket number that was used with the socket open processing
Support Commands
<table>
<tr><th>Function Code</th><th>Command Name</th><th>Function</th></tr>
<tr><td>01 hex</td><td>Read Coils</td><td>Read Coils</td></tr>
<tr><td>03 hex</td><td>Read Holding Registers</td><td>Read Holding Registers</td></tr>
<tr><td>05 hex</td><td>Write Single Coil</td><td>Write Single Coil</td></tr>
<tr><td>06 hex</td><td>Write Single Register</td><td>Write Single Register</td></tr>
<tr><td>0F hex</td><td>Write Multiple Coils</td><td>Write Multiple Coils</td></tr>
<tr><td>10 hex</td><td>Write Multiple Registers</td><td>Write Multiple Registers</td></tr>
</table></td></tr>
<tr><td>Types of Function Block Definition</td><td>Multi-cycle execution type
This function block performs processing over multiple cycles after starting.
The same instance cannot be used simultaneously in multiple places because the state is maintained internally.</td></tr>
<tr><td>Precautions for Correct Use</td><td>• This function block performs processing over several cycles. Whether processing is being executed can be checked from the BUSY output variable.
• Upon completion of processing, OK or NG turns ON for one cycle only. Refer to these flags to detect completion of the function block processing.
■ Timechart
 
</td></tr>
<tr><td>Input Conditions of EN</td><td>As shown in the figure above, the logical OR of BUSY, which is the rising edge of the start trigger and the output of the function block, is connected to the EN.</td></tr>
<tr><td>Restrictions
Input Variables</td><td>• Be sure to use a rising edge differential (↑) for the input to EN.
• If the value of the input variable is outside of the range, the ENO turns OFF, and the contents of the function block are not executed.
• Be sure to insert the BUSY output variable in the OR circuit of the input conditions to the input variable EN so that processing is executed until completion because this processing needs to be executed over multiple cycles.
• Do not turn ON/OFF the BUSY output variable outside of the function block.</td></tr>
</table>

Example of Using	Connect to the Modbus TCP Server with TCP socket number 1 of unit number 0 and the TCP port number automatically allocated. Turn contact A ON to process TCP socket opening. Turn contact E ON after socket opening to send the Modbus command using this function block. To end Modbus TCP communication, turn Bit I ON to close the socket.





• Variable Tables

[INPUT]

Function01: Read Coils

Name	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to &15	EIP21S Unit Number
TCP Socket Number	TCPSocketNo	INT	&1	&1 to 8	
Coil Start Address	ReadCoilAddr	UINT	&0	&0 to &65535	
Coil Size	ReadCoilSize	UINT	&1	&1 to &64	Readable bits: 64 bits maximum
Read data storage area word number	RecvArea	WORD	-	I/O Memory	Since this is an I/O variable, specify it with an I/O memory address. Do not exceed the maximum word number of the I/O memory specified by the starting word number + number of registers.

Function03: Read Holding Registers

Name	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to &15	EIP21S Unit Number
TCP Socket No.	TCPSocketNo	INT	&1	&1 to 8	
Register Start Address	ReadRegAddr	UINT	&0	&0 to &65535	
Register Size	ReadRegSize	UINT	&1	&1 to &20	Readable words: 20 words maximum
Read data storage area starting word number	RecvArea	WORD	-	I/O Memory	Since this is an I/O variable, specify it with an I/O memory address. Do not exceed the maximum word number of the I/O memory specified by the starting word number + number of registers.

Function05: Write Single Coil

Name	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to &15	EIP21S Unit Number
TCP Socket Number	TCPSocketNo	INT	&1	&1 to 8	
Coil Address	WriteCoilAddr	UINT	&0	&0 to &65535	
Coil Output Value	OutputValue	WORD	#0000	See the right	ON:#FF00 OFF:#0000

Function06: Write Single Register

Name	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to &15	EIP21S Unit Number
TCP Socket Number	TCPSocketNo	INT	&1	&1 to 8	
Register Address	WriteRegAddr	UINT	&0	&0 to &65535	
Write data storage area word number	SendArea	WORD	-	I/O Memory	Since this is an I/O variable, specify it with an I/O memory address.

Function0F: Write Multiple Coils

Name	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to &15	EIP21S Unit Number
TCP Socket Number	TCPSocketNo	INT	&1	&1 to 8	
Coil Start Address	WriteCoilAddr	UINT	&0	&0 to &65535	
Coil Size	WriteCoilSize	UINT	&1	&1 to &64	Writable bits: 64 bits maximum
Write data storage area starting word number	SendArea	WORD	-	I/O Memory	Since this is an I/O variable, specify I/O memory. Do not exceed the maximum word number of the I/O memory specified by the starting word number + number of registers.

Function10: Write Multiple Registers

Name	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to &15	EIP21S Unit Number
TCP Socket Number	TCPSocketNo	INT	&1	&1 to 8	
Register Start Address	WriteRegAddr	UINT	&0	&0 to &65535	
Register Size	WriteRegSize	UINT	&1	&1 to &20	Writable words: 20 words maximum
Write data storage area starting word number	SendArea	WORD	-	I/O Memory	Since this is an I/O variable, specify it with an I/O memory address. Do not exceed the maximum word number of the I/O memory specified by the starting word number + number of registers.

[OUTPUT]

Common for all function blocks

Name	Symbol name	Data Type	Scope	Details
ENO	ENO	BOOL		1 (ON): The function block operated normally. 0 (OFF): The function block did not start. / The function block completed abnormally.
Busy Flag	BUSY	BOOL		Turns OFF automatically after processing completes
Normal end	OK	BOOL		Turns ON for one cycle only when completes normally
Error end	NG	BOOL		Turns ON for one cycle only when completes abnormally
Modbus Error Code	ModErrorCode	WORD		When Modbus communication completed abnormally, when an exception response is received, or when the input variable is outside the range, NG turns to ON and a Modbus error code is output. For information on error codes, see below.
FINS response Code	CmndErrorCode	WORD		When a socket service error occurs, NG turns to ON and the FINS response code of the TCP socket is stored.

Modbus Error Code

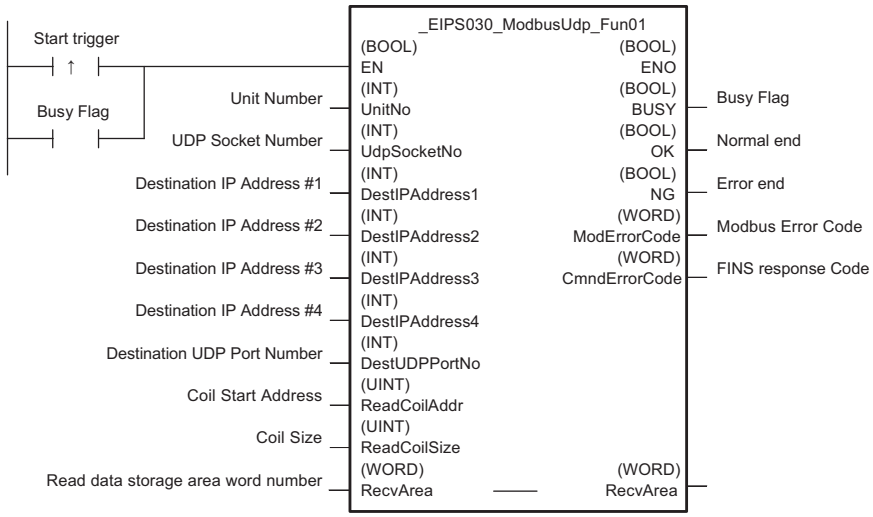
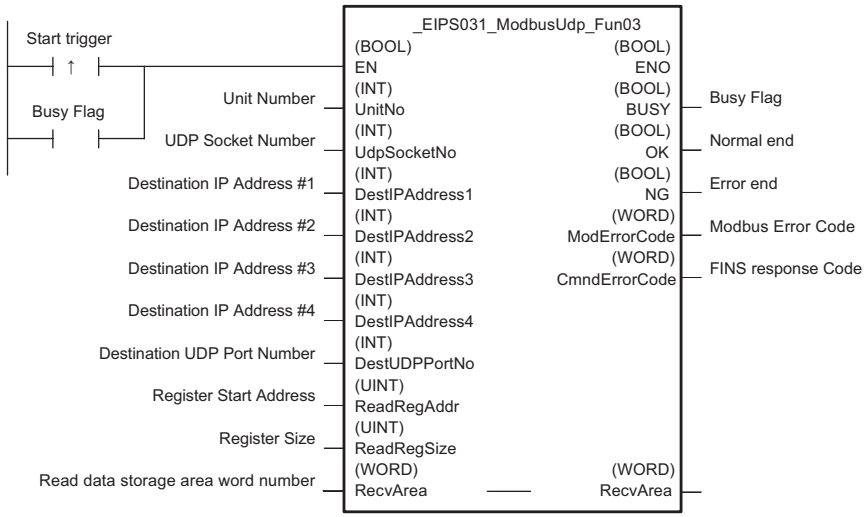
Error Code ModErrorCode	Description	Cause
0000 hex	Normal completion	-
0001 hex	FUNCTION code invalid (exception response code)	An unsupported FUNCTION code is specified.
0002 hex	Data address invalid (exception response code)	There is a mistake with the specified start address. The specified start address and data length exceed the valid range.
0003 hex	Data invalid (exception response code)	Number of data and data length do not match.
0100 hex	No response	No response from Modbus server
FFFF hex	Input variable is outside of range	The value set for the input variable is outside of the range. Sending and receiving of the Modbus command are not executed.

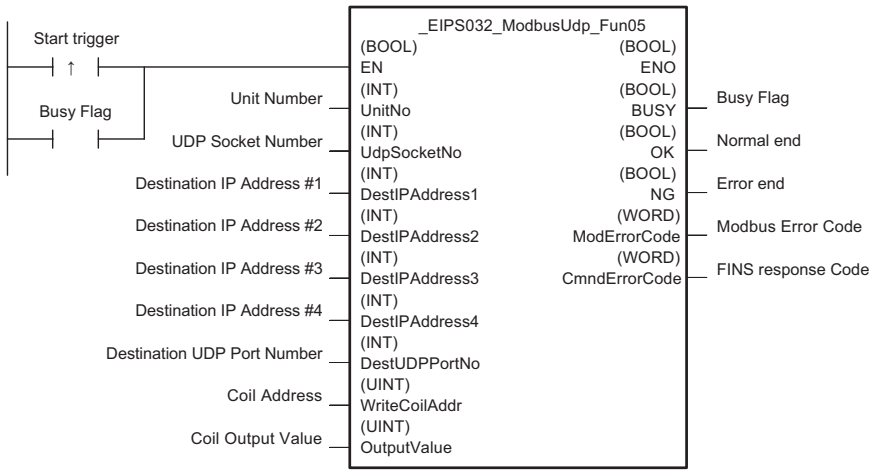
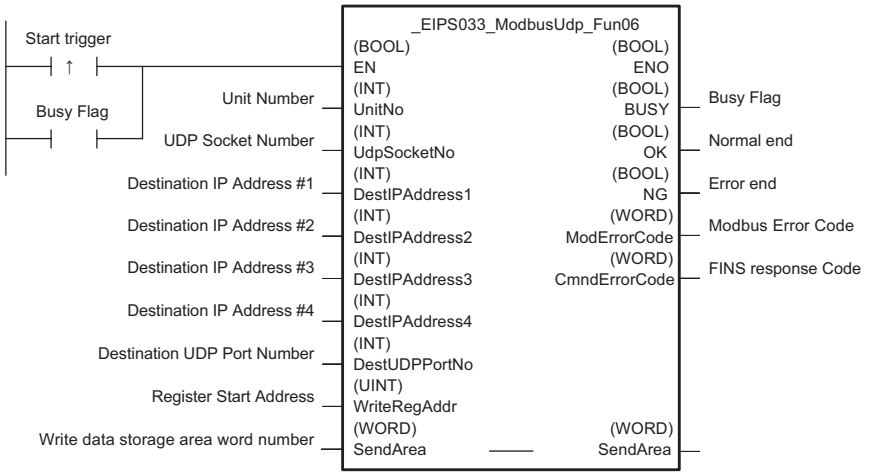
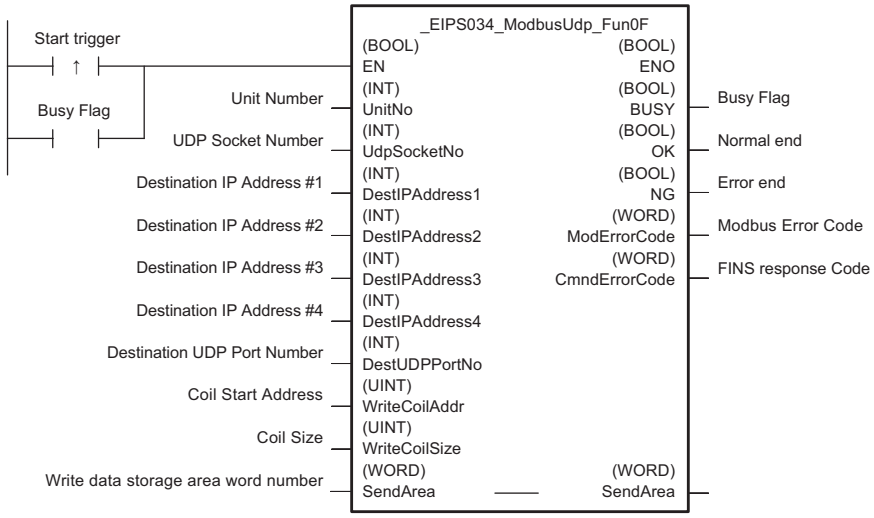
FINS Completion Code

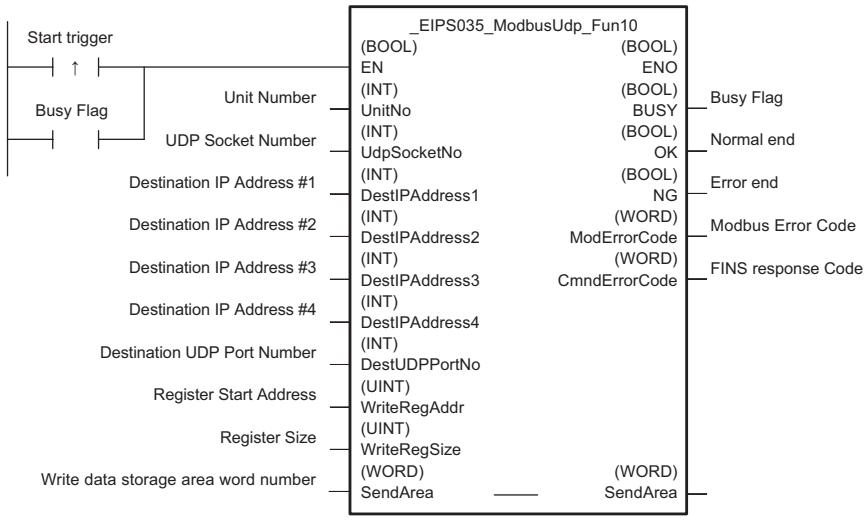
Refer to Appendix 5 FINS Command for EtherNet/IP Units or Built-in EtherNet/IP Ports for details about the FINS completion code.

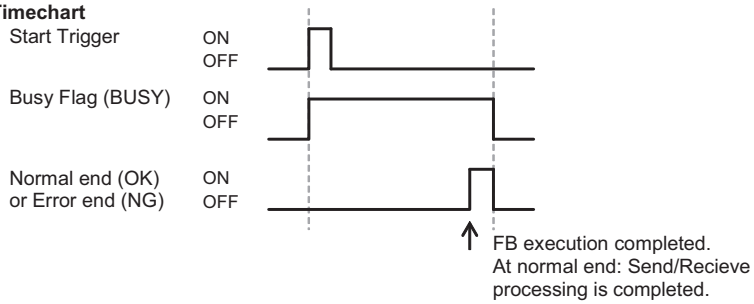
Function Block for Modbus UDP Client

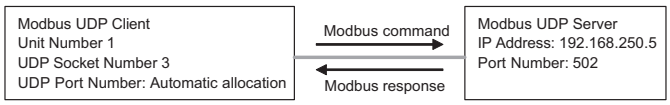
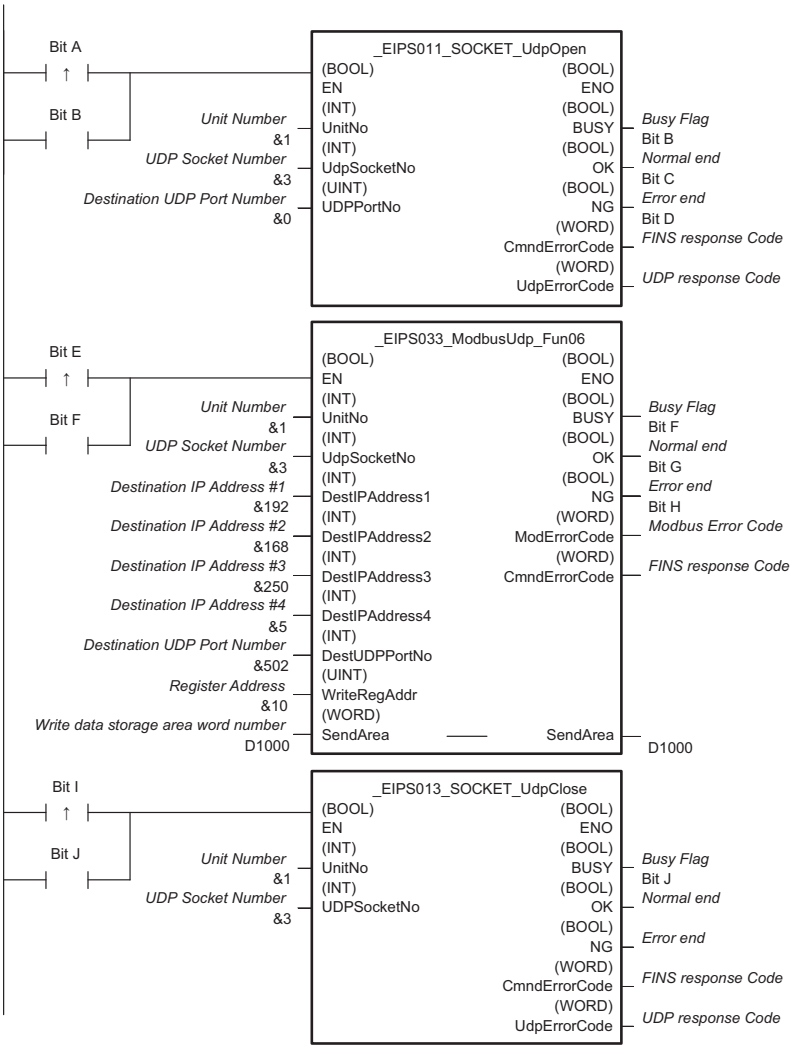
Item	Details
EIPS 030 to 035	Modbus UDP Client _EIPS**_ModbusUdp_Fun**
Overview	A Modbus UDP command is issued using a socket service function for the specified EtherNet/IP Unit.

Item	Details
Symbol	■Function01: Read Coils  ■Function03: Read Holding Registers 

Item	Details
Symbol	■Function05: Write Single Coil  ■Function06: Write Single Register  ■Function0F: Write Multiple Coils 

Item	Details	
Symbol	■Function10: Write Multiple Registers 		
File Name	_EIPS030_ModbusUdp_Fun01.cxf: Function 01 (Read Coils) _EIPS031_ModbusUdp_Fun03.cxf: Function 03 (Read Holding Registers) _EIPS032_ModbusUdp_Fun05.cxf: Function 05 (Write Single Coil) _EIPS033_ModbusUdp_Fun06.cxf: Function 06 (Write Single Register) _EIPS034_ModbusUdp_Fun0F.cxf: Function 0F (Write Multiple Coils) _EIPS035_ModbusUdp_Fun10.cxf: Function 10 (Write Multiple Registers)		
Applicable models	EtherNet/IP Unit	CJ1W-EIP21S Unit Version 1.0 or later (Cannot be used in CS1W-EIP21S) CJ3M-CPU3□ Unit Version 1.1 or later
	CPU Unit	CJ2H-CPU6□(-EIP), CJ2M-CPU□□, CJ3M-CPU□□ (Cannot be used in CS1 CPU Unit)
	CX-Programmer	Version 9.78 or later
Coding Language	Ladder Program	
Usage Conditions	■ CPU Unit Settings PLC Setup: Shared Settings for Communications Instructions in FBs • Communications Instruction Response Timeout Time (default: 2 s) • Number of retries (default: 0) ■ Commonly used sources • Communications ports (internal logical ports) ■ Other Parameters • The crossing of network levels is not supported. • This function block implements the socket service by CMND2 instruction (FINS command). UDP RECEIVE REQUEST: FINS Commands 2702 • UDP SEND REQUEST: FINS Commands 2703	

<table>
<tr><th>Item</th><th>Details</th></tr>
<tr><td>Function</td><td>■ Operation of function block
• On the rising edge of the start trigger, a Modbus command is issued using the UDP socket specified in UdpSocketNo for the EtherNet/IP Unit specified in UnitNo.
• In the case of the write command, the data is written to the address specified in Register/Coil (Start) Address.
• In the case of the read command, the data is read from the address specified in Register/Coil (Start) Address.
• Specify the words of sent data and received data directly in I/O memory with an I/O variable.
• If sending is processed normally, the One Cycle ON when Function Block Completes Normally Flag (OK) will turn ON. The error code (ModErrorCode/CmndErrCode) will be #0000.
• If an error code is received from the Modbus server, the One Cycle ON when Function Block Completes Abnormally Flag (NG) will turn ON and the Modbus error code will be stored in Modbus Error Code (ModErrorCode).
• When there is a FINS communication error for the CMND2 instruction, the One Cycle ON when Function Block Completes Abnormally Flag (NG) will turn ON and the FINS completion code will be stored in FINS Completion Code (CmndErrorCode).
• This function block is executed by the UDP socket service function using the CMND2 instruction. Execute the socket open processing before executing the function block. (_EIPS011_SOCKET_UdpOpen) For the UDP socket number to use with the function block, use the socket number that was used with the socket open processing.
Support Commands
<table>
<tr><th>Function Code</th><th>Command Name</th><th>Function</th></tr>
<tr><td>01 hex</td><td>Read Coils</td><td>Read Coils</td></tr>
<tr><td>03 hex</td><td>Read Holding Registers</td><td>Read Holding Registers</td></tr>
<tr><td>05 hex</td><td>Write Single Coil</td><td>Write Single Coil</td></tr>
<tr><td>06 hex</td><td>Write Single Register</td><td>Write Single Register</td></tr>
<tr><td>0F hex</td><td>Write Multiple Coils</td><td>Write Multiple Coils</td></tr>
<tr><td>10 hex</td><td>Write Multiple Registers</td><td>Write Multiple Registers</td></tr>
</table></td></tr>
<tr><td>Types of Function Block Definition</td><td>Multi-cycle execution type
This function block performs processing over multiple cycles after starting.
The same instance cannot be used simultaneously in multiple places because the state is maintained internally.</td></tr>
<tr><td>Precautions for Correct Use</td><td>• This function block performs processing over several cycles. Whether processing is being executed can be checked from the BUSY output variable.
• Upon completion of processing, OK or NG turns ON for one cycle only. Refer to these flags to detect completion of the function block processing.
■ Timechart
 
</td></tr>
<tr><td>Input Conditions of EN</td><td>As shown in the figure above, the logical OR of BUSY, which is the rising edge of the start trigger and the output of the function block, is connected to the EN.</td></tr>
<tr><td>Restrictions
Input Symbol</td><td>• Be sure to use a rising edge differential (↑) for the input to EN.
• If the value of the input variable is outside of the range, the ENO turns OFF, and the contents of the function block are not executed.
• Be sure to insert the BUSY output variable in the OR circuit of the input conditions to the input variable EN so that processing is executed until completion because this processing needs to be executed over multiple cycles.
• Do not turn ON/OFF the BUSY output variable outside of the function block.</td></tr>
</table>

Item	Details
Example of Using	Connect to the Modbus UDP Server with UDP socket number 3 of unit number 1 and the UDP port number automatically allocated. Turn contact A ON to process UDP socket opening. Turn contact E ON after socket opening to send the Modbus command using this function block. To end Modbus UDP communication, turn Bit I ON to close the socket.  

• Variable Tables

[INPUT]

Function01: Read Coils

Name	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to 15	EIP21S Unit Number
UDP Socket Number	UdpSocketNo	INT	&1	&1 to &8	
Destination IP Address #1	DestIPAddress1	INT	&0	&0 to &254	
Destination IP Address #2	DestIPAddress2	INT	&0	&0 to &254	
Destination IP Address #3	DestIPAddress3	INT	&0	&0 to &254	
Destination IP Address #4	DestIPAddress4	INT	&0	&0 to &254	
Destination UDP Port Number	DestUDPPortNo	INT	&0		
Coil Start Address	ReadCoilAddr	UINT	&0	&0 to &65535	
Coil Size	ReadCoilSize	UINT	&1	&1 to &64	Readable bits: 64 bits maximum
Read data storage area word number	RecvArea	WORD	-	I/O Memory	Since this is an I/O variable, specify it with an I/O memory address. Do not exceed the maximum word number of the I/O memory specified by the starting word number + number of registers.

Function03: Read Holding Registers

Name	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to 15	EIP21S Unit Number
UDP Socket Number	UdpSocketNo	INT	&1	&1 to &8	
Destination IP Address #1	DestIPAddress1	INT	&0	&0 to &254	
Destination IP Address #2	DestIPAddress2	INT	&0	&0 to &254	
Destination IP Address #3	DestIPAddress3	INT	&0	&0 to &254	
Destination IP Address #4	DestIPAddress4	INT	&0	&0 to &254	
Destination UDP Port Number	DestUDPPortNo	INT	&0		
Register Start Address	ReadRegAddr	UINT	&0	&0 to &65535	

Name	Symbol name	Data Type	Default Value	Scope	Details
Register Size	ReadRegSize	UINT	&1	&1 to &20	Readable words: 20 words maximum
Read data storage area starting word number	RecvArea	WORD	-	I/O Memory	Since this is an I/O variable, specify it with an I/O memory address. Do not exceed the maximum word number of the I/O memory specified by the starting word number + number of registers.

Function05: Write Single Coil

Name	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to 15	EIP21S Unit Number
UDP Socket Number	UdpSocketNo	INT	&1	&1 to &8	
Destination IP Address #1	DestIPAddress1	INT	&0	&0 to &254	
Destination IP Address #2	DestIPAddress2	INT	&0	&0 to &254	
Destination IP Address #3	DestIPAddress3	INT	&0	&0 to &254	
Destination IP Address #4	DestIPAddress4	INT	&0	&0 to &254	
Destination UDP Port Number	DestUDPPortNo	INT	&0		
Coil Address	WriteCoilAddr	UINT	&0	&0 to &65535	
Coil Output Value	OutputValue	WORD	#0000	See the right	ON:#FF00 OFF:#0000

Function06: Write Single Register

Name	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to 15	EIP21S Unit Number
UDP Socket Number	UdpSocketNo	INT	&1	&1 to &8	
Destination IP Address #1	DestIPAddress1	INT	&0	&0 to &254	
Destination IP Address #2	DestIPAddress2	INT	&0	&0 to &254	
Destination IP Address #3	DestIPAddress3	INT	&0	&0 to &254	
Destination IP Address #4	DestIPAddress4	INT	&0	&0 to &254	
Destination UDP Port Number	DestUDPPortNo	INT	&0		

Name	Symbol name	Data Type	Default Value	Scope	Details
Register Address	WriteRegAddr	UINT	&0	&0 to &65535	
Write data storage area word number	SendArea	WORD	-	I/O Memory	Since this is an I/O variable, specify it with an I/O memory address.

Function0F: Write Multiple Coils

Name	Symbol name	Data Type	Default Value	Scope	Details
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to 15	EIP21S Unit Number
UDP Socket No.	UdpSocketNo	INT	&1	&1 to &8	
Destination IP Address #1	DestIPAddress1	INT	&0	&0 to &254	
Destination IP Address #2	DestIPAddress2	INT	&0	&0 to &254	
Destination IP Address #3	DestIPAddress3	INT	&0	&0 to &254	
Destination IP Address #4	DestIPAddress4	INT	&0	&0 to &254	
Destination UDP Port Number	DestUDPPortNo	INT	&0		
Coil Start Address	WriteCoilAddr	UINT	&0	&0 to &65535	
Coil Size	WriteCoilSize	UINT	&1	&1 to &64	Writable bits: 64 bits maximum
Write data storage area starting word number	SendArea	WORD	-	I/O Memory	Since this is an I/O variable, specify it with an I/O memory address. Do not exceed the maximum word number of the I/O memory specified by the starting word number + number of registers.

Function10: Write Multiple Registers

Name	Symbol name	Data Type	Default Value	Details	Name
EN	EN	BOOL			1 (ON): Starts the function block. 0 (OFF): Does not start the function block.
Unit Number	UnitNo	INT	&0	&0 to 15	The EIP21S Unit's Unit Number
UDP Socket Number	UdpSocketNo	INT	&1	&1 to &8	
Destination IP Address #1	DestIPAddress1	INT	&0	&0 to &254	
Destination IP Address #2	DestIPAddress2	INT	&0	&0 to &254	
Destination IP Address #3	DestIPAddress3	INT	&0	&0 to &254	
Destination IP Address #4	DestIPAddress4	INT	&0	&0 to &254	
Destination UDP Port Number	DestUDPPortNo	INT	&0		
Register Start Address	WriteRegAddr	UINT	&0	&0 to &65535	

Name	Symbol name	Data Type	Default Value	Details	Name
Register Size	WriteRegSize	UINT	&1	&1 to &20	Writable words: 20 words maximum
Write data storage area starting word number	SendArea	WORD	-	I/O Memory	Since this is an I/O variable, specify it with an I/O memory address. Do not exceed the maximum word number of the I/O memory specified by the starting word number + number of registers.

[OUTPUT]

Common for all function blocks

Name	Symbol name	Data Type	Scope	Details
ENO	ENO	BOOL		1 (ON): The function block operated normally. 0 (OFF): The function block did not start. / The function block completed abnormally.
Busy Flag	BUSY	BOOL		Turns OFF automatically after processing completes
Normal end	OK	BOOL		Turns ON for one cycle only when completes normally
Error end	NG	BOOL		Turns ON for one cycle only when completes abnormally
Modbus Error Code	ModErrorCode	WORD		When Modbus communication completed abnormally, when an exception response is received, or when the input variable is outside the range, NG turns to ON and a Modbus error code is output. For information on error codes, see below.
FINS response Code	CmndErrorCode	WORD		When a socket service error occurs, NG turns to ON and the FINS response code of the UDP socket is stored.

Modbus Error Code

Error Code ModErrorCode	Description	Cause
0000 hex	Normal completion	-
0001 hex	FUNCTION code invalid (exception response code)	An unsupported FUNCTION code is specified.
0002 hex	Data address invalid (exception response code)	There is a mistake with the specified start address. The specified start address and data length exceed the valid range.
0003 hex	Data invalid (exception response code)	Number of data and data length do not match.
0100 hex	No response	No response from Modbus server
FFFF hex	Input variable is outside of range	The value set for the input variable is outside of the range. Sending and receiving of the Modbus command are not executed.

FINS completion code

Refer to *Appendix E FINS Commands Addressed to EtherNet/IP Units or Built-in EtherNet/IP Ports* for details about the FINS completion code.

Modbus Command Response Details

Function 01 Read Coils: Read multiple contacts from coil to I/O memory

Command

Field name	Data Bits	Data or Input variables
FUNCTION codes	1 byte	01 hex
Coil Start Address	2 bytes	ReadCoilAddr 0 to FFFF hex (&0 to &65535)
Coil Size	2 bytes	ReadCoilSize 1 to 40 hex (&1 to &64)

Response

Field name	Data Bits	Data or Input variables
FUNCTION codes	1 byte	01 hex
Number of bytes data	1 byte	1 or 2 hex
Coil data	1 to 8 bytes	Specify the read data storage area starting word number in I/O memory.

Note Response data other than coil data cannot be checked with the function block.

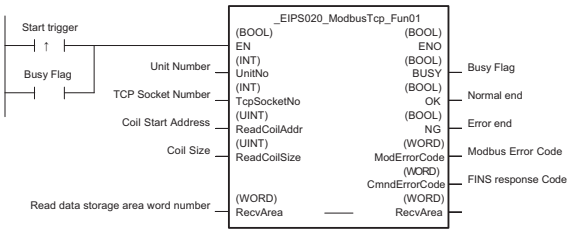
Example: When reading the 20 bits (0010001010001010 02028A hex) from the coil starting address 4 (0004 hex) to W10.

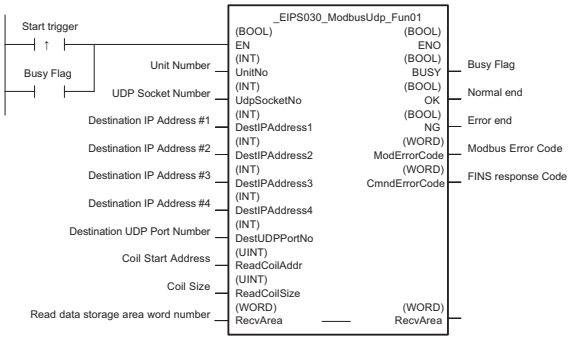
Commands (EIP21S: Modbus client)

Field name	Data
FUNCTION codes	01 hex
Coil Start Address (Upward)	0004 hex (4 or more)
Coil Start Address (Downward)	
Coil Number (Upward)	0014 hex (20 bits)
Coil Number (Downward)	

Response (Modbus server)

Field name	Data
FUNCTION code	01 hex
Number of bytes data	02 hex
Coil Data 4 to 11	8A Hex W10.00 to W10.07
Coil Data 12 to 19	02 hex W10.08 to W10.15
Coil Data 20 to 23	02 hex W11.00 to W10.04





Example: When reading the number of coils as 20 bits from coil starting address 4 (0004 hex) to W10

Modbus server

15(0)	14(0)	13(1)	12(0)	11(1)	10(0)	9(0)	8(0)	7(1)	6(0)	5(1)	4(0)	3	2	1	0
31	30	29	28	27	26	25	24	23(0)	22(0)	21(1)	20(0)	19(0)	18(0)	17(0)	16(0)

Read

EIP21S (Modbus client)

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
W10	(0)	(0)	(0)	(0)	(0)	(0)	(1)	(0)	(1)	(0)	(0)	(0)	(1)	(0)	(1)	(0)
W11													(0)	(0)	(1)	(0)

*: The number in ( ) indicates the coil state.
*: 0 is set for the remaining bits less than 1 byte.

Function 03 Read Holding Registers: Read multiple words from the storage register to I/O memory

Command

Field name	Data Bits	Data or Input variables
FUNCTION codes	1 byte	03 hex
Register Start Address	2 bytes	ReadRegAddr 0 to FFFF hex (&0 to &65535)
Register Size	2 bytes	ReadRegSize 1 to 0014 hex (&1 to &20)

Response

Field name	Data Bits	Data or Input variables
FUNCTION codes	1 byte	03 hex
Number of bytes data	1 byte	2 × N (N: Number of registers)
Register read data	2 × N bytes	Specify the read data storage area starting word number in I/O memory.

Note Response data other than register read data cannot be checked with the function block.

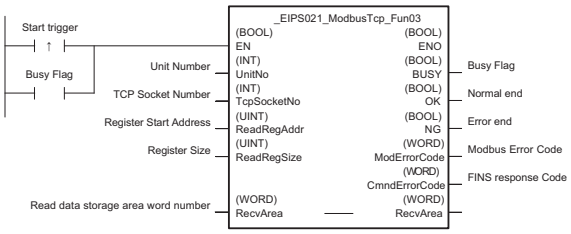
Example: When reading the 3 words (AB12, 5678, and 9713 hex) from the register starting address 100 (0064 hex) of the Modbus server to D1000 to D1002

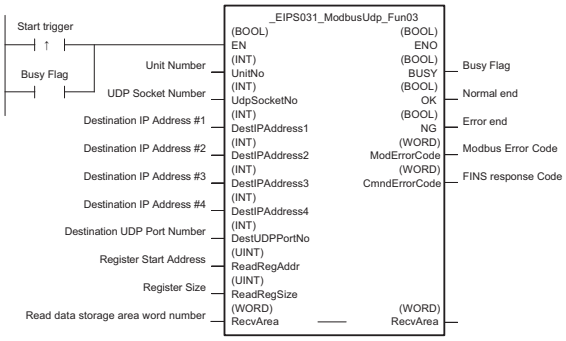
Commands (EIP21S: Modbus client)

Field name	Data
FUNCTION codes	03 hex
Register Start Address (Upward)	0064 hex (100 or more)
Register Start Address (Downward)	
Register Size (Upward)	0003 hex (3 words)
Register Size (Downward)	

Response (Modbus server)

Field name	Data
FUNCTION code	03 hex
Number of bytes data	06 hex
Register Read Data (Upward)	AB12 hex (D1000)
Register Read Data (Downward)	
Register Read Data (Upward)	5678 hex (D1001)
Register Read Data (Downward)	
Register Read Data (Upward)	9713 hex (D1002)
Register Read Data (Downward)	





Modbus server

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
100	A				B				1				2			
101	5				6				7				8			
102	9				7				1				3			

Read

EIP21S (Modbus client)

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
D1000	A				B				1				2			
D1001	5				6				7				8			
D1002	9				7				1				3			

Function 05 Write Single Coil: Write Single Coil from I/O memory storage register

Command

Field name	Data Bits	Data or Input variables
FUNCTION codes	1 byte	05 hex
Coil Address	2 bytes	WriteCoilAddr 0 to FFFF hex (&0 to &65535)
Coil Output Value	2 bytes	OutputValue ON(1): FF00 hex OFF(0): 0000 hex

Response

Field name	Data Bits	Data or Input variables
FUNCTION codes	1 byte	05 hex
Coil Address	2 bytes	WriteCoilAddr 0 to FFFF hex (&0 to &65535)
Coil Write Data	2 bytes	ON(1): FF00 hex OFF(0): 0000 hex

Note Response data other than coil data cannot be checked with the function block.

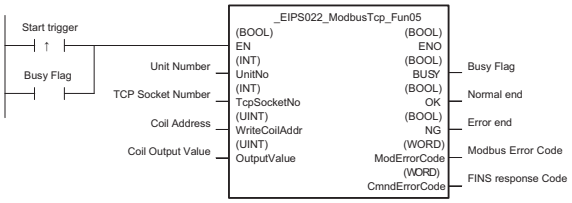
Example: When turning coil address 10 of the Modbus server ON

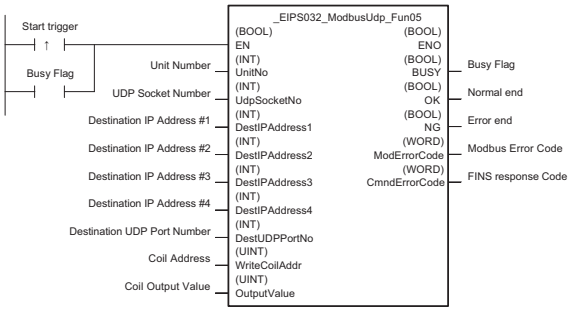
Commands (EIP21S: Modbus client)

Field name	Data
FUNCTION codes	05 hex
Coil address (Upward)	000A hex
Coil address (Downward)	(&10)
Coil Write Data	FF00 hex

Response (Modbus server)

Field name	Data
FUNCTION codes	05 hex
Coil address (Upward)	000A hex
Coil address (Downward)	(&10)
Coil Write Data	FF00 hex



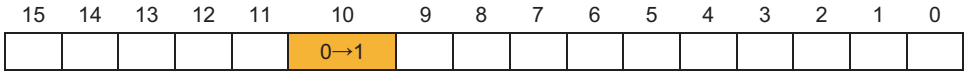


EIP21S (Modbus client)

Coil address: &10, Write items: FF00 hex

Write

Modbus server



Function 06 Write Single Register: Write 1 word from I/O memory to storage register

Command

Field name	Data Bits	Data or Input variables
FUNCTION codes	1 byte	06 hex
Register Address	2 bytes	WriteRegAddr 0 to FFFF hex (&0 to &65535)
Register Write Data	2 bytes	Specify the write data storage area word number in I/O memory.

Response

Field name	Data Bits	Data or Input variables
FUNCTION codes	1 byte	06 hex
Register Address	2 bytes	Same as WriteRegAddr 0 to FFFF hex (&0 to &65535)
Register Write data	2 bytes	0000 to FFFF hex

Note Response data cannot be checked with the function block.

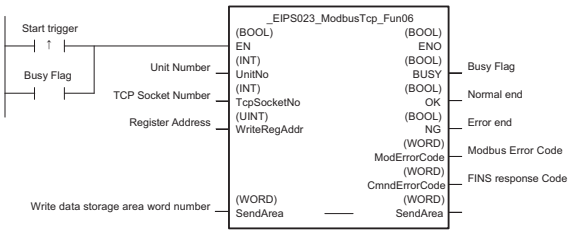
Example: When writing to address 100 of Modbus server 200 from D500 (3AC5 hex).

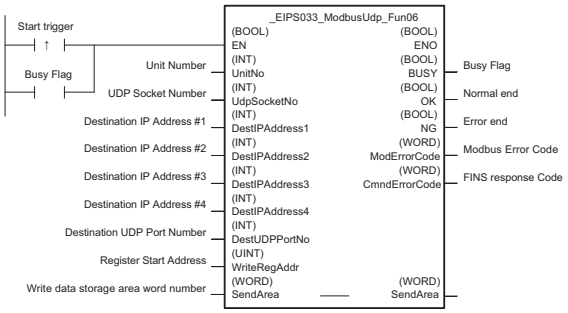
Commands (EIP21S: Modbus client)

Field name	Data
FUNCTION codes	06 hex
Register Address (Upward)	00C8 hex
Register Address (Downward)	(200)
Register Write Data (Upward)	3AC5 hex
Register Write Data (Downward)	(D500)

Response (Modbus server)

Field name	Data
FUNCTION codes	06 hex
Register Address (Upward)	00C8 hex
Register Address (Downward)	(200)
Register Write Data (Upward)	3AC5 hex
Register Write Data (Downward)	





EIP21S (Modbus client)

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
D500	3				A				C				5			
D501																

Write

Modbus server

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
200	3				A				C				5			
201																

Function 0F Write Multiple Coils: Write multiple contacts from I/O memory to coil

Command

Field name	Data Bits	Data or Input variables
FUNCTION code	1 byte	0F hex
Coil Start Address	2 bytes	WriteCoilAddr 0 to FFFF hex (&0 to &65535)
Coil Size	2 bytes	WriteCoilSize 1 to 40 hex (&1 to &64)
Number of bytes	1 byte	WriteCoilSize/8
Coil Write Data	1 to 8 bytes	Specify the write data storage area starting word number in I/O memory.

Response

Field name	Data Bits	Data or Input variables
FUNCTION codes	1 byte	0F hex
Coil Start Address	2 bytes	Same as WriteCoilAddr
Coil Size	2 bytes	Same as WriteCoilSize

Note Response data other than coil data cannot be checked with the function block.

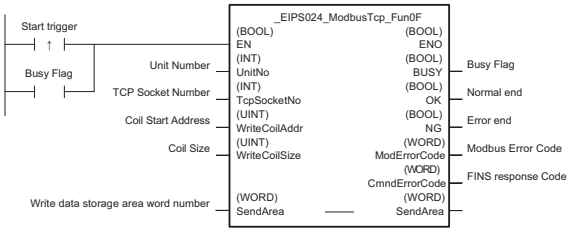
Example: When writing 13 bits of W30.00 to W30.11 (1100101100010 = 1962 hex) to coil starting address 20 (0014 hex) in the Modbus server.

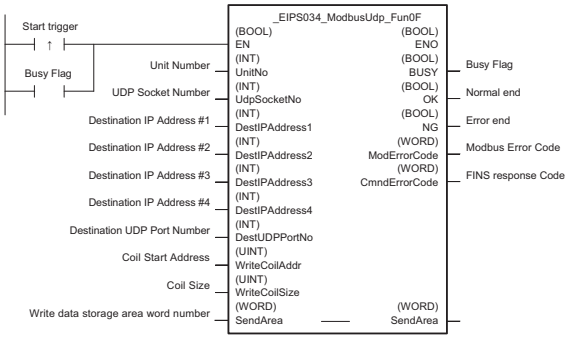
Commands (EIP21S: Modbus client)

Field name	Data
FUNCTION codes	0F hex
Coil Start Address (Upward)	0014 hex
Coil Start Address (Downward)	(20)
Coil Number (Upward)	000C hex
Coil Number (Downward)	(13 bits)
Coil Data 20 to 27	62 hex W200.00 to W200.07
Coil Data 28 to 31	19 hex W200.08 to W200.12

Response (Modbus server)

Field name	Data
FUNCTION codes	0F hex
Coil Start Address (Upward)	0014 hex
Coil Start Address (Downward)	
Coil Number (Upward)	000C hex
Coil Number (Downward)	





EIP21S (Modbus client)

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
W30	- (0)	- (0)	- (0)	(1)	(1)	(0)	(0)	(1)	(0)	(1)	(1)	(0)	(0)	(0)	(1)	(0)

*: The number in ( ) indicates the coil state.
*: Set 0 for the remaining bits less than 1 byte.

Write

Modbus server

31(1)	30(0)	29(0)	28(1)	27(0)	26(1)	25(1)	24(0)	23(0)	22(0)	21(1)	20(0)	19	18	17	16
47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32(1)

*: The number is a coil address, and the number in ( ) indicates the coil state.

Function 10 Write Multiple Registers: Write multiple words from I/O memory to storage register

Command

Field name	Data Bits	Data or Input variables
FUNCTION code	1 byte	10 hex
Register Start Address	2 bytes	WriteRegAddr 0 to FFFF hex (&0 to &65535)
Register Size	2 bytes	WriteRegSize 0 to 0014 hex (&0 to &20)
Number of bytes	1 byte	2 × N (N: Number of registers)
Register Write Data	2 × N bytes	Specify the write data storage area starting word number in I/O memory.

Response

Field name	Data Bits	Data
FUNCTION codes	1 byte	10 hex
Register Start Address	2 bytes	Same as WriteRegAddr
Register Size	2 bytes	Same as WriteRegSize

Note Response data cannot be checked with the function block.

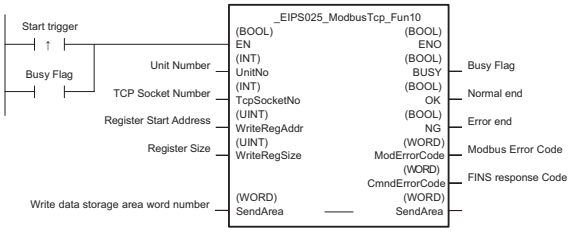
Example: When writing the 2 words (0100 and 3A98 hex) from D2000 to D2001 to the register starting address 10 (000A hex) of Modbus server.

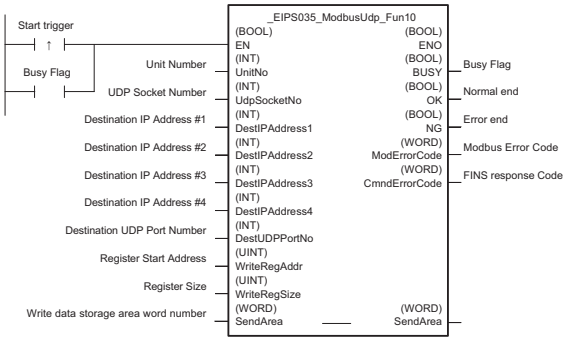
Commands (EIP21S: Modbus client)

Field name	Data
FUNCTION codes	10 hex
Register Start Address (Upward)	000A hex (10 or more)
Register Start Address (Downward)	
Register Size (Upward)	02 hex (2 words)
Register Size (Downward)	
Number of bytes	04 hex
Register Write Data (Upward)	0100 hex (D2000)
Register Write Data (Downward)	
Register Write Data (Upward)	3A98 hex (D2001)
Register Write Data (Downward)	

Response (Modbus server)

Field name	Data
FUNCTION codes	10 hex
Register Start Address (Upward)	000A hex
Register Start Address (Downward)	
Register Size (Upward)	0002 hex (2 words)
Register Size (Downward)	





EIP21S (Modbus client)

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
D2000	0				1				0				0			
D2001	3				A				9				8			

Write

Modbus server

	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
10	0				1				0				0			
11	3				A				9				8			

Index

Numerics

7-segment display, 35

A

adding accounts, 391
Adjust Time field, 372, 374
alternate DNS server, 70
applications
  precautions, xxxii
Auto Adjust Time field, 372, 373
Auto Adjust Time Tab, 373
automatic clock adjustment
  Automatic Clock Adjustment Switch, 374
  errors
    error codes, 374
    error log, 374
    SNTP, 374
  overview, 370
  procedure, 371
  settings, 372
  specifications, 371
Auxiliary Area
  related data, 120

B

Backup Tool, 522
bandwidth usage
  relationship to packet interval (RPI), 307
baud rate, 71, 73, 313
  CJ-series, 18, 20
  CS-series, 16
bits
  addresses, 623
  Automatic Clock Adjustment Switch, 374
  dedicated control bits, 431
  Socket Service Request Switches, 449
    Close Request Switch, 450
    Send Request Switch, 449
    TCP Active Open Request Switch, 449
    TCP Passive Open Request Switch, 449
    UDP Open Request Switch, 449
BROADCAST DATA SEND, 630
broadcast test
  command, 630
  reading results, 630
BROADCAST TEST RESULTS READ, 630
buffers, 607, 663
bye command, 347, 353, 357

C

cables
  connections, 56
  installation, 55
  precautions, 52
cd command, 347, 353, 355
changing authority, 393
changing passwords, 392
changing user names, 392
checking accounts, 392
CIDR, 3, 126
CIO Area
  allocations, 96
CIP, 4, 611
CIP communications services, 7
CIP message communications., 611
cleaning, 378, 516
close command, 347, 353, 357
Close Request Switch, 111, 450
Closing Flag, 113, 440
CMND(490) instruction, 230, 232, 233, 264, 284
  requesting socket services, 433, 465
commands
  FTP commands, 353
communications
  high traffic conditions, 272
  message communications, 228
  message communications errors, 235
communications cables, xxxiii
Communications Port Enabled Flags, 266
Communications Port Error Flags, 266
communications specifications, 24
Communications Status 1, 105
Communications Status 2, 107
Communications Status 3, 108
communications test, 90
component names, 31
connecting to the FTP server, 348
connection
  setting, 174
Connections settings (Edit All Connections), 177

Connections Tab, 174
connectors (modular plug)
  recommended models, 39
Contact Output Units
  precautions, 54
control bits, 99
CONTROLLER DATA READ, 624
CONTROLLER STATUS READ, 626
CPU Bus Units
  precautions, xxxiv
creating a tag set, 159
creating tag sets, 159
creating tags, 161
crimp terminals, xxxiii
current consumption
  CJ-series, 18, 20
  CS-series, 16
CX-Integrator, 58
  creating routing tables, 248
CX-Programmer, 10, 58
  connecting to PLC, 251
cyclic communications
  required settings, 45

D

d5 error (verification error, target nonexistent) mask, 35, 107, 540
data areas
  FINS communications, 622
Data Received Flag, 113, 440
Datalink Tool, 74, 183
default gateway, 69
delays
  message service delays, 337
delete command, 347, 353, 356
deleting accounts, 391
Device Monitor function, 528
device parameter settings, 94
device parameters
  clearing, 213
  editing, 160, 169, 172, 174
devices
  registering, 157
DHCP client computer, 134
DHCP service
  automatic IP address setting by DHCP service, 134
dimensions
  CJ-series, 18, 20, 28, 29
  CS-series, 17, 28
dir command, 347, 353, 354
distance
  CJ-series transmission distance, 18, 20
  transmission distance, 16
DM Area
  allocations, 114
DNS server, 69
  automatic clock adjustment
    errors, 374
DNS Tab, 372
domain name, 70
downloading tag data link parameters, 204
dynamic changes of remote IP address
  prohibiting, 131

E

EC Directives, xxxv
Edit Parameters, 44, 67
editing and checking the user authentication settings, 390
editing settings for individual connections, 175
EDS file management, 671
EDS files, 671
  creating, 672
  installing, 671
  saving, 672
  searching, 673
EIP21S, 6
EIP21S User Management Tool, 6, 379
electromagnetic fields, xxxii
EM File Memory, 360
  using, 360
EMC Directives, xxxv
EPATH type, 613
error codes
  table of error codes, 374, 555
error flags
  Target Node PLC Error Flags, 101, 119
error log
  clearing, 554
  codes, 555
  overflow, 554
  specifications, 554
ERROR LOG CLEAR, 632

error log function, 554
ERROR LOG READ, 631
error processing, 374, 535
errors
  automatic clock adjustment, 374
  controller status, 626
  error log
    clearing, 632
    reading, 631
  error messages, 358
  flags
    FINS communications, 627
  message communications, 234, 235
  UNIX error messages, 570
Ethernet communications
  addresses
    reading from Unit, 624
  network parameters, 605
  parameters, 605, 607
Ethernet Connectors, 56
Ethernet Units
  reading status, 663
EtherNet/IP Datalink Tool, 74, 183
EtherNet/IP Unit Features, 2
EtherNet/IP Units
  resetting, 623
ETN11-compatible mode, 131
explicit message communications, 228, 232, 233
explicit message communications service, 140
explicit messages
  list of PLC object services, 288
  receiving, 287
  sending, 274
  sending using CMND(490), 282

F

FALS instruction, xxix
FINS communications, 273
  commands
    format, 622
    socket services, 622
  memory areas, 622
  overview, 9
  precautions on high traffic, 272
  socket numbers, 622
  specifications, 239, 260
  testing, 651
  troubleshooting, 563
FINS communications service, 141
FINS message communications, 228, 230
FINS node address
  relationship to IP address, 126, 137
FINS response codes
  troubleshooting with response codes, 572
FINS/TCP, 242
  communications, 244
  connection numbers, 243
  connection status, 110, 244
  features, 242
  frame format, 243
  procedure, 245
  TCP port number, 243
FINS/TCP communications method, 132
FINS/UDP, 240
  frame format, 240
  procedure, 241
  UDP port numbers, 241
FINS/UDP and FINS/TCP
  comparison, 239
FINS/UDP communications methods, 128
FinsGateway, 255
flags
  Error Flags, 627
  FTP Status Flag, 359
  Port Enabled Flag, 468
FTP, 3, 82
FTP server
  application examples, 351
  commands, 353
    bye, 357
    cd, 355
    close, 357
    delete, 356
    dir, 354
    get, 356
    ls, 354
    mdelete, 357
    mget, 356
    mput, 356
    open, 353
    put, 356
    pwd, 355
    quitting, 357
    type, 355
    user, 354
  connecting, 348, 353
  data type, 355
  displaying current directory, 355

file types (FTP server function), 347
protection, 347
protocol, 347
quitting, 357
See also Memory Cards
specifications, 347
status, 359
FTP Status Flag, 359
full duplex, 71

G

gateway
default gateway, 69
general specifications, 16
get command, 347, 353, 356, 365
Get the time information from the SNTP server field, 372, 373
global address, 138
GMRP, 40

H

half duplex, 71
high communications traffic
preventing, 272
host name, 69
Host Name field, 372, 373

I

I/O allocations
CIO Area, 96
DM Area, 114
I/O memory address, 148
I/O response time, 328
I/O tables
creating, 58
overview, 58
ICMP communications
status, 660
IGMP snooping, 26, 40
importing, 169
indicators, 33
using LED indicators for troubleshooting, 535
initial settings, 44
initializing user authentication settings, 393
installation, 43
cable connections, 56
location, xxxii
mounting Unit to PLC, 49
precautions, 52
INTERNODE ECHO TEST, 629
internode test
command, 629
IP address, 124
automatic generation, 127
automatic generation (dynamic), 128
automatic generation (static), 129
automatic IP address setting by DHCP service, 134
combined method, 130
determining IP addresses, 124
global address, 138
IP address table method, 127, 129
private address, 138
prohibiting dynamic changes of remote IP address, 131
relationship to FINS node address, 126, 137
responding to computers with changed IP address, 134
setting local IP address, 63
IP Address Display/Setting Area, 115
IP Address field, 372, 373
IP ADDRESS TABLE READ, 656
IP addresses
allocating, 124
configuration, 124
IP communications
IP addresses
reading from Units, 624
reading tables, 656
remote devices, 447
IP router tables
reading, 658
programming examples, 461, 470, 478
status, 659
IP ROUTER TABLE READ, 658

K

keep-alive, 69

L

ladder programming for tag data links, 220
LED indicators, 33

using for troubleshooting, 535
link setting (baud rate), 71
local network table, 247
Local UDP/TCP Port No., 447
locking devices
precautions, xxxiii
ls command, 347, 353, 354

M

maintenance, 516
maximum tag data link I/O response time, 332
maximum transmission delay, 490
maximum transmission delay of instruction, 337
mdelete command, 347, 353, 357
memory allocation, 94
memory areas
See also data areas
Memory Card, 517
restoring data, 520
Memory Cards, 347, 360
deleting files, 357
displaying directories, 354
See also FTP server
transferring files from host, 356
transferring files to host, 356
MEMORY STATUS READ, 663
message communications, 9
errors, 234
specifications, 233
message communications functions, 228
message communications service
required settings, 45
mget command, 347, 353, 356
mkdir command, 347, 353
mode settings
reading from Unit, 624
mounting procedure, 50
mput command, 347, 353, 356
MRES, 468
MS indicator, 34
multicast communications, 147
multicast filter, 40
multivendor device connections, 6

N

n
beginning word of allocated CIO Area, 96
network
devices required for constructing a network, 5
network configuration file
reading, 215
saving, 214
Network Configurator, 153
connecting to the network, 194
Device Monitor function, 528
requirements, 13
starting, 153
TCP/IP settings, 72
Network Configurator overview, 13
network devices
recommended devices, 39
networks
network memory, 663
network parameters, 605
network symbol, 145, 149, 159
Node Address Setting Switch, 38
node addresses
setting, 47
noise, xxxii
Contact Output Units, 54
nomenclature and functions, 31
Normal Target Node Flags, 110, 118
NS indicator, 34
Number of Bytes Received at TCP Socket, 441
Number of Bytes to Send/Receive, 448

O

online editing, xxxi
open command, 347, 353
Opening Flag, 113, 440
operating environment
precautions, xxxii
operation authority, 397
operation authority list, 398, 401

P

packet interval (RPI)
relationship to bandwidth usage, 307
setting, 306

PCMR(260) instruction, 268
PING, 651
PING command, 90
PLC object services, 288
Port Enabled Flag, 468
Port No. field, 372, 373
port numbers
  TCP port, 447
    remote device, 448
  UDP port, 447
    reading from Unit, 624
    remote device, 448
power supply, xxxii
  precautions, xxxiii
precautions, xxvii
  applications, xxxii
  Contact Output Units, 54
  general, xxviii
  handling, 51
  installation, 52
  operating environment, xxxii
  power supply, xxxiii
  safety, xxix
  Socket Service Request Switches, 489
  socket services, 488
  TCP communications, 437
  UDP communications, 438
  wiring, 56
preferred DNS server, 70
private address, 138
Programming Console, 58
Programming Devices
  connecting, 58
  CX-Net, 58
  CX-Programmer, 58
  Programming Console, 58
PROTOCOL STATUS READ, 659
protocols
  FTP server, 347
  reading status, 659
put command, 347, 353, 356, 365
pwd command, 347, 353, 355

Q

QoS, 40, 42
quit command, 347, 353, 357

R

radioactivity, xxxii
Receive Request Switch, 111, 450
receiving explicit messages, 287
Receiving Flag, 113, 440
recommended network devices, 39
recommended products, 52
RECV(098) instruction, 230, 263
  delays, 340
refresh cycle, 313
Register Device List, 174
Registered Target Node Flags, 109, 117
registering devices, 157, 174
relay tables, 247
Remote IP Address, 447
Remote UDP/TCP Port No., 448
rename command, 347, 353
replacing a Unit, 516
replacing Units
  precautions, xxxiv
response codes
  Results Storage Area, 468
  Socket Service Request Switches, 450
  UNIX error messages, 570
restoring data from the Memory Card, 520
restrictions for installation (CS1W/CJ1W-EIP21S only), 21
Results Storage Area, 468, 622
  response codes, 570
Results Storage Error Flag, 113, 440
Retry Timer field, 372, 374
rmdir command, 347, 353
route path, 613
routing tables, 247
  precautions, xxxiv
  relay network table, 247
  setting examples, 249

S

safety precautions, xxix
Send Request Switch, 111, 449
SEND(090) instruction, 230, 262
  accessible data areas, 261
  delays, 337
Send/Receive Data Address, 448

sending explicit messages, 282
sending FINS messages, 127
Sending Flag, 113, 440
Server Specification Type field, 372, 373
settings for various use scenarios, 410
settings required for security functions, 46
seven-segment Display, 35
seven-segment display
  error status, 535, 539, 540, 542, 544, 547
short-circuits
  precautions, xxxiii
Simple Backup Function, 380, 517
SNMP, 3, 86
SNMP trap, 87
SNTP, 3, 84, 370
SNTP server
  automatic clock adjustment
    errors, 374
  obtaining clock information, 370
Socket Option, 447
socket option, 622
socket service, 10, 11
Socket Service Parameter Area 1 to 8, 116
Socket Service Request Switches 1 to 8, 111
socket services
  applications, 465
  FINS communications, 622
  functions, 431
  parameters, 442
  precautions, 488
  socket option, 622
  Socket Service Parameter Area, 432, 443
  Socket Service Request Switches, 431, 449
    application procedure, 442
    precautions, 489
  Socket Status Area, 444
  TCP communications, 433
    parameters, 446
  timing charts, 455, 468, 469
  troubleshooting, 570
  UDP communications, 433
    parameters, 446
  using CMND(490) instruction, 431, 433, 465
  using Socket Service Request Switches, 432
SOCKET STATUS READ, 609, 664
sockets
  closing
    TCP, 650
    UDP, 638
  numbers, 622
  opening, 436
    TCP, 640, 643
    UDP, 632
  overview, 434
  port numbers, 434
  reading status, 664
  receiving data
    TCP, 646
    UDP, 634
  sending data
    TCP, 648
    UDP, 636
  TCP sockets
    number, 447
    status, 609
    troubleshooting, 567
  testing communications, 651
  UDP socket
    number, 447
  UDP sockets
    troubleshooting, 564
specifications, 16
  CJ-series general specifications, 18, 20
  communications specifications, 24
  CS-series general specifications, 16
  FINS communications, 260
  FTP server, 347
  message communications, 233
  Network Configurator, 13
SRES, 468
startup procedure, 44
static electricity, xxxii
  precautions, xxxiv
status
  reading memory status, 663
  reading protocol status, 659
  reading socket status, 664
status flags for tag data links, 224
Status of UDP/TCP Sockets 1 to 8, 112
subnet mask, 68, 125
  reading from Unit, 624
switch
  Node Address Setting Switch, 38
switches
  Socket Service Request Switches, 449
switching hub
  connection methods, 54
  environment precautions, 53
  functions, 40

precautions when selecting, 40
recommended models, 39
switching hub types, 39
SYSMAC BUS/2, 260
SYSMAC LINK, 260

T

tag, 145, 149
tag data link parameters
downloading, 145, 204
setting, 145
uploading, 208
verifying, 209
Tag Data Link Start Bit, 99
Tag Data Link Stop Bit, 99
tag data links
checking bandwidth usage, 314
data areas, 149
delay time, 310
functions, 148
I/O response time, 328
ladder programming, 220
maximum I/O response time, 332
overview, 144
required settings, 45
specifications, 148
status flags, 224
tag data links (cyclic communications), 2, 7
tag set, 145, 149
tag sets
creating, 159
Target Node PLC Error Flags, 101, 119
Target Node PLC Operating Flags, 100, 119
TCP Active Open Request Switch, 111, 449
TCP CLOSE REQUEST, 650
TCP communications
comparison with UDP, 435
data fragmentation, 437
precautions, 437
programming example, 470
socket services
parameters, 446
sockets, 436
status, 609
troubleshooting, 567
status, 661
TCP Connection Status, 441
TCP OPEN REQUEST (ACTIVE), 643
TCP OPEN REQUEST (PASSIVE), 640
TCP Passive Open Request Switch, 111, 449
TCP RECEIVE REQUEST, 646
TCP SEND REQUEST, 648
TCP Socket No. (1 to 8)
Connection Status, 116
Number of Bytes Received, 116
TCP status transitions, 609
TCP/IP, 66
TCP/UDP Open Flag, 113, 440
terminal blocks, xxxi
Time Out Time, 448
timeout errors, 562
timers, 607
timing
socket communications, 468
socket services, 469
timing of data transmissions, 328
to, 79
transmission delays, 490
troubleshooting, 559
FINS communications, 563
socket services, 570
TCP sockets, 567
UDP sockets, 564
UNIX error messages, 570
twisted-pair cable
recommended models, 39
twisted-pair cables
precautions, 52
type command, 347, 353, 355

U

UDP CLOSE REQUEST, 638
UDP communications
comparison with TCP, 435
data fragmentation, 437
precautions, 438
programming example, 461, 478
socket services
parameters, 446
sockets
troubleshooting, 564
UDP OPEN REQUEST, 632
UDP Open Request Switch, 111, 449
UDP RECEIVE REQUEST, 634
UDP SEND REQUEST, 636

UDP/TCP Socket No., 447
UDP/TCP Socket Status, 439
unicast communications, 147
Unit Number Setting Switch, 37
Unit replacement, 516
unit setup, 6, 79
Unit Status 1, 101
Unit Status 2, 103
UNIX error messages, 570
Unregister Device List, 175
uploading tag data link parameters, 208
user authentication setting, 393
user authentication timeout, 402
user command, 347, 353, 354
user name
  specifying, 354
User Settings Area, 117
using FTP commands, 353

V

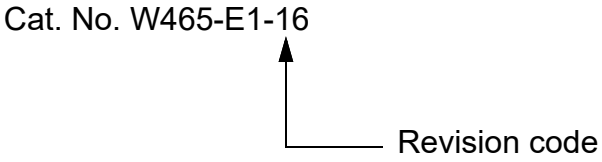
verifying tag data link parameters, 209

W

what to do if you forget administrator account information, 396
wiring
  precautions, 56

Revision History

A manual revision code appears as a suffix to the catalog number on the front cover of the manual.



The following table outlines the changes made to the manual during each revision. Page numbers refer to the previous version.

Revision code	Date	Revised content
01	June 2007	Original production
02	July 2008	Added information for CJ-series CJ2 CPU Units and for new unit version 2.0 functions.
03	December 2008	Added the CJ-series CJ2 CPU Units (CJ2H-CPU□□).
04	December 2009	Added information on methods to create connections and heartbeats. Greatly changed the structure of sections 1 and 2. Added and improved information on communications performance and communications load in section 10. Made changes accompanying a new version of the Network Configurator (V3.10).
05	February 2010	Added the CJ-series CJ2M CPU Units (CJ2M-CPU3□).
06	October 2010	Added information on functions for unit version 2.1 of the CJ-series CJ2M CPU Units (CJ2M-CPU3□).
07	October 2012	Added information on functions for unit version 2.1 of the EtherNet/IP Unit (and built-in EtherNet/IP port).
08	December 2013	**Cover and pages xii, :** Added trademark symbol. **Page v:** Modified "Trademarks and Copyrights" information **Pages xv to xvii:** Replaced "Warranty and Application Considerations" with "Terms and Conditions Agreement." **Page 25:** Added paragraph above figure and added sentence to callout in figure. **Page 26:** Added precaution. **Page 44:** Changed caution and changed dimension in figure. **Pages 79 and 80:** Added note and reference to it. **Page 85:** Changed figure and added information at beginning of section 4-3-2. **Page 127:** Deleted part of note. **Page 354:** Added note in Error column cell for Verification Error.
09	November 2014	The allowable bandwidth was increased to 12,000 pps.
10	November 2021	Corrected mistakes.
11	July 2022	Revisions for adding safety precautions regarding security.
12	August 2022	Corrected mistakes.
13	July 2023	Added information for CS1W/CJ1W-EIP21S EtherNet/IP Units. Added information on security functions in section 13 and socket services in section 14.
14	October 2024	Revisions for the CJ1W-EIP21S to support connection to NJ-series CPU Units.
15	April 2025	Made changes accompanying the connection support of CJ1W-EIP21S to CP1H CPU Units. Added information on the hardware revision. Corrected mistakes.
16	October 2026	Changes were made throughout the manual to include information for new products (CJ3M CPU Unit).

OMRON Corporation **Industrial Automation Company**

Kyoto, JAPAN **Contact : www.ia.omron.com**

Regional Headquarters

OMRON EUROPE B.V.
Wegalaan 67-69, 2132 JD Hoofddorp
The Netherlands
Tel: (31) 2356-81-300 Fax: (31) 2356-81-388

OMRON ELECTRONICS LLC
2895 Greenspoint Parkway, Suite 200
Hoffman Estates, IL 60169 U.S.A.
Tel: (1) 847-843-7900 Fax: (1) 847-843-7787

OMRON ASIA PACIFIC PTE. LTD.
438B Alexandra Road, #08-01/02 Alexandra
Technopark, Singapore 119968
Tel: (65) 6835-3011 Fax: (65) 6835-3011

OMRON (CHINA) CO., LTD.
Room 2211, Bank of China Tower,
200 Yin Cheng Zhong Road,
PuDong New Area, Shanghai, 200120, China
Tel: (86) 21-6023-0333 Fax: (86) 21-5037-2388

Authorized Distributor:

©OMRON Corporation 2007 - 2026 All Rights Reserved.
In the interest of product improvement,
specifications are subject to change without notice.

Cat. No. W465-E1-16 1026