OMRON

Machine Automation Controller

NX-series

EtherNet/IP™ Unit

User's Manual

NX-EIP201

EtherNet/IP Unit

sysmac
always in control

W627-E1-02

NOTE

Trademarks

Copyrights

Introduction

Thank you for purchasing an NX-series EtherNet/IP Unit.
This manual contains information that is necessary to use the NX-series EtherNet/IP Unit. Please read this manual and make sure you understand the functionality and performance of the NX-series EtherNet/IP Unit before you attempt to use it in a control system.
Keep this manual in a safe place where it will be available for reference during operation.

Intended Audience

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

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

For programming, this manual is intended for personnel who understand the programming language specifications in international standard IEC 61131-3 or Japanese standard JIS B 3503.

Applicable Products

This manual covers the following products.

- NX-series EtherNet/IP Unit
  NX-EIP201

Relevant Manuals

The following table provides the relevant manuals for the NX-series CPU Units. Read all of the manuals that are relevant to your system configuration and application before you use the NX-series CPU Unit.

Most operations are performed from the Sysmac Studio Automation Software. Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for information on the Sysmac Studio.

Purpose of use	**Manual**												
	Basic information												
	NX-series NX502 CPU Unit Hardware User's Manual	**NJ/NX-series CPU Unit Software User's Manual**	**NJ/NX-series Instructions Reference Manual**	**NJ/NX-series CPU Unit Motion Control User's Manual**	**NJ/NX-series Motion Control Instructions Reference Manual**	**NJ/NX-series CPU Unit Built-in EtherCAT Port User's Manual**	**NJ/NX-series CPU Unit Built-in EtherNet/IP Port User's Manual**	**NX-series EtherNet/IP Unit User's Manual**	**NJ/NX-series CPU Unit OPC UA User's Manual**	**NX-series CPU Unit FINS Function User's Manual**	**NJ/NX-series Database Connection CPU Units User's Manual**	**NX-series CPU Unit Automation Playback User's Manual**	**NJ/NX-series Troubleshooting Manual**
Introduction to NX502 CPU Units	●												
Setting devices and hardware	●												
Using motion control				●									
Using EtherCAT						●							
Using EtherNet/IP							●	●					
Software settings		●											
Using motion control				●									
Using EtherCAT						●							
Using EtherNet/IP							●	●					
Using OPC UA									●				
Using FINS										●			
Using the database connection service											●		
Using automation playback												●	

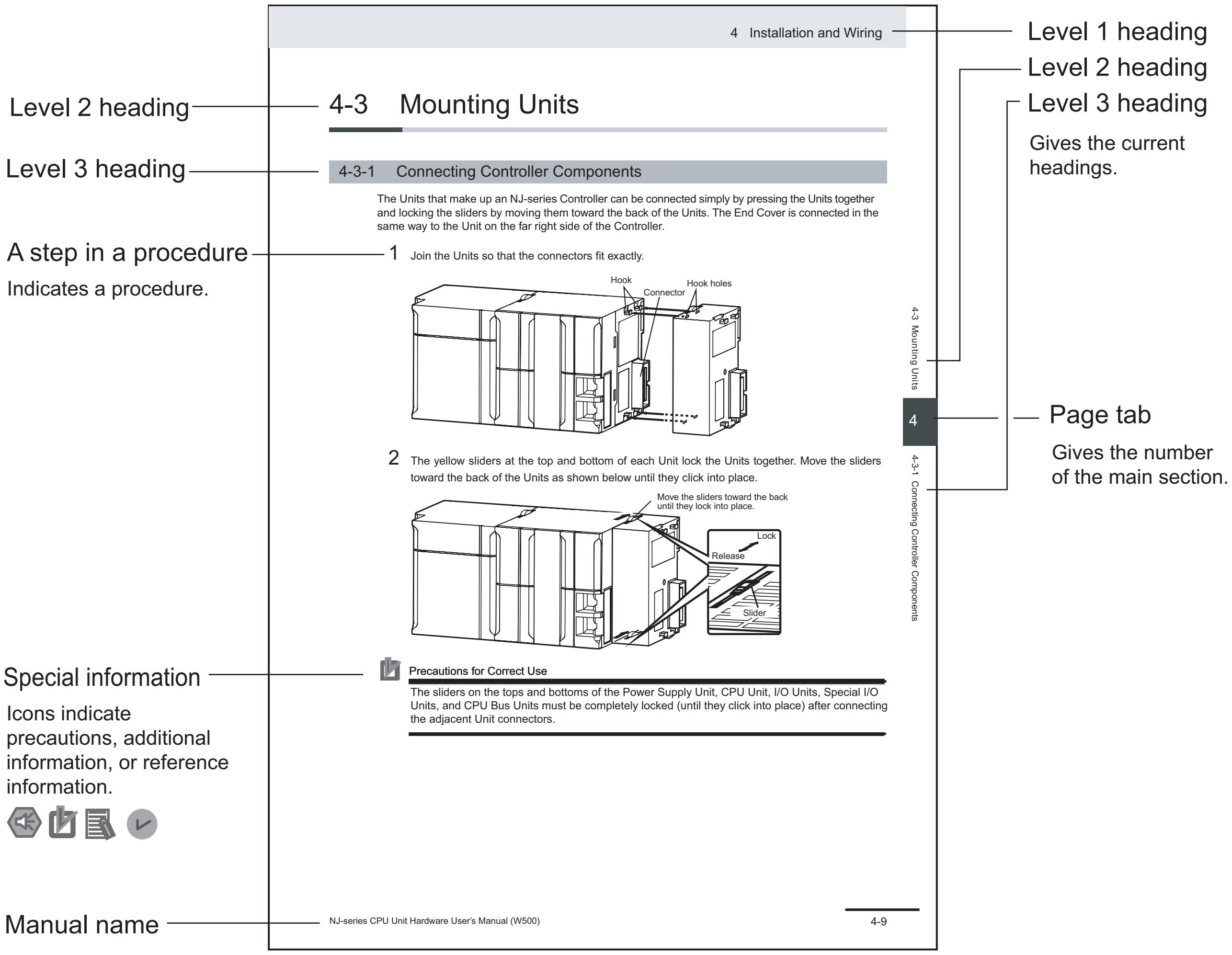
Purpose of use	Manual												
	Basic information												
	NX-series NX502 CPU Unit Hardware User's Manual	NJ/NX-series CPU Unit Software User's Manual	NJ/NX-series Instructions Reference Manual	NJ/NX-series CPU Unit Motion Control User's Manual	NJ/NX-series Motion Control Instructions Reference Manual	NJ/NX-series CPU Unit Built-in EtherCAT Port User´s Manual	NJ/NX-series CPU Unit Built-in EtherNet/IP Port User's Manual	NX-series EtherNet/IP Unit User's Manual	NJ/NX-series CPU Unit OPC UA User's Manual	NX-series CPU Unit FINS Function User's Manual	NJ/NX-series Database Connection CPU Units User's Manual	NX-series CPU Unit Automation Playback User's Manual	NJ/NX-series Troubleshooting Manual
Writing the user program		●	●										
Using motion control				●	●								
Using EtherCAT						●							
Using EtherNet/IP							●	●					
Using OPC UA									●				
Using FINS										●			
Using the database connection service											●		
Using automation playback												●	
Programming error processing													●
Testing operation and debugging		●											
Using motion control				●									
Using EtherCAT						●							
Using EtherNet/IP							●	●					
Using OPC UA									●				
Using FINS										●			
Using the database connection service											●		
Using automation playback												●	
Learning about error management and corrections[*1]									△	△	△	△	●
Maintenance	●												
Using motion control				●									
Using EtherCAT						●							
Using EtherNet/IP							●	●					

*1. Refer to the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* for the error management concepts and the error items. However, refer to the manuals that are indicated with triangles (△) for details on errors corresponding to the products with the manuals that are indicated with triangles (△).

Manual Structure

Page Structure

The following page structure is used in this manual.



4 Installation and Wiring

4-3 Mounting Units

4-3-1 Connecting Controller Components

The Units that make up an NJ-series Controller can be connected simply by pressing the Units together and locking the sliders by moving them toward the back of the Units. The End Cover is connected in the same way to the Unit on the far right side of the Controller.

1 Join the Units so that the connectors fit exactly.

2 The yellow sliders at the top and bottom of each Unit lock the Units together. Move the sliders toward the back of the Units as shown below until they click into place.

Move the sliders toward the back until they lock into place.
Lock
Release
Slider

Precautions for Correct Use

The sliders on the tops and bottoms of the Power Supply Unit, CPU Unit, I/O Units, Special I/O Units, and CPU Bus Units must be completely locked (until they click into place) after connecting the adjacent Unit connectors.

4-3 Mounting Units
4
4-3-1 Connecting Controller Components
NJ-series CPU Unit Hardware User's Manual (W500)
4-9

Level 1 heading

Level 2 heading

Level 3 heading

Gives the current headings.

Page tab

Gives the number of the main section.

Level 2 heading

Level 3 heading

A step in a procedure

Indicates a procedure.

Special information

Icons indicate precautions, additional information, or reference information.

Manual name

This illustration is provided only as a sample. It may not literally appear in this manual.

Special Information

Special information in this manual is classified as follows:

Precautions for Safe Use

Precautions on what to do and what not to do to ensure safe usage of the product.

Precautions for Correct Use

Precautions on what to do and what not to do to ensure proper operation and performance.

Additional Information

Additional information to read as required.
This information is provided to increase understanding or make operation easier.

Version Information

Information on differences in specifications and functionality for Controller with different unit versions and for different versions of the Sysmac Studio is given.

Precaution on Terminology

In this manual, "download" refers to transferring data from the Sysmac Studio to the physical Controller and "upload" refers to transferring data from the physical Controller to the Sysmac Studio.
For the Sysmac Studio, "synchronization" is used to both "upload" and "download" data. Here, "synchronize" means to automatically compare the data for the Sysmac Studio on the computer with the data in the physical Controller and transfer the data in the direction that is specified by the user.

Sections in this Manual

CONTENTS

Section 1 Features and System Configuration

Section 2 Specifications and Application Procedures

Section 3 Part Names and Functions

Section 4 Mounting

Section 5 Installing Ethernet Networks

Section 6 Device Variables Related to the NX-series EtherNet/IP Unit

Section 7 Sysmac Studio Settings for the EtherNet/IP Port

Section 8 TCP/IP Functions

Section 9 Tag Data Link Functions

Section 10 CIP Message Communications

Section 11 SNMP Agent

Section 12 Communications Performance and Communications Load

Section 13 Instructions Specific to NX-series EtherNet/IP Units

Section 14 Troubleshooting

Section 15 Maintenance and Inspection

Appendices

Index

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 OR IN LARGE QUANTITIES 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.

Statement of security responsibilities for assumed use cases and against threats

OMRON SHALL NOT BE RESPONSIBLE AND/OR LIABLE FOR ANY LOSS, DAMAGE, OR EXPENSES DIRECTLY OR INDIRECTLY RESULTING FROM THE INFECTION OF OMRON PRODUCTS, ANY SOFTWARE INSTALLED THEREON OR ANY COMPUTER EQUIPMENT, COMPUTER PROGRAMS, NETWORKS, DATABASES OR OTHER PROPRIETARY MATERIAL CONNECTED THERETO BY DISTRIBUTED DENIAL OF SERVICE ATTACK, COMPUTER VIRUSES, OTHER TECHNOLOGICALLY HARMFUL MATERIAL AND/OR UNAUTHORIZED ACCESS.

It shall be the users sole responsibility to determine and use adequate measures and checkpoints to satisfy the users particular requirements for (i) antivirus protection, (ii) data input and output, (iii) maintaining a means for reconstruction of lost data, (iv) preventing Omron Products and/or software installed thereon from being infected with computer viruses and (v) protecting Omron Products from unauthorized access.

Safety Precautions

Definition of Precautionary Information

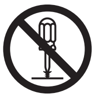
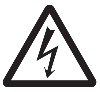
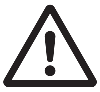
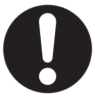
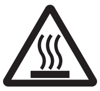
The following notation is used in this manual to provide precautions required to ensure safe usage of the NX-series X Bus Unit.

The safety precautions that are provided are extremely important for safety. Always read and heed the information provided in all safety precautions.

The following notation is used.

⚠ 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.

Symbols

	The circle and slash symbol indicates operations that you must not do. The specific operation is shown in the circle and explained in text. This example indicates prohibiting disassembly.
	The triangle symbol indicates precautions (including warnings). The specific operation is shown in the triangle and explained in text. This example indicates a precaution for electric shock.
	The triangle symbol indicates precautions (including warnings). The specific operation is shown in the triangle and explained in text. This example indicates a general precaution.
	The filled circle symbol indicates operations that you must do. The specific operation is shown in the circle and explained in text. This example shows a general precaution for something that you must do.
	The triangle symbol indicates precautions (including warnings). The specific operation is shown in the triangle and explained in text. This example indicates a precaution for high temperatures.

Warnings

⚠ WARNING

During Power Supply

Do not attempt to take any Unit apart.
In particular, high-voltage parts are present in the Power Supply Unit while power is supplied or immediately after power is turned OFF. Touching any of these parts may result in electric shock. There are sharp parts inside the Unit that may cause injury.

Fail-safe Measures

The NX-series EtherNet/IP Unit will not start operation if an error is detected by the self-diagnosis at startup. External safety measures must be provided to ensure safe operation of the system in such case.

If there is interference in remote I/O communications, output status will depend on the products that are used.
Confirm the operation that will occur when there is interference in communications, and implement safety measures.
Correctly set all of the settings in the remote I/O and Units.

Unintended outputs may occur when an error occurs in variable memory. As a countermeasure for such problems, external safety measures must be provided to ensure safe operation of the system.

Provide measures in the communications system and user program to ensure safety in the overall system even if errors or malfunctions occur in data link communications.

You must take fail-safe measures to ensure safety in the event of incorrect, missing, or abnormal signals caused by broken signal lines, momentary power interruptions, or other causes.
Not doing so may result in serious accidents due to incorrect operation.

Security Measures

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.

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.

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

Data recovery

Backup data and keep the data up-to-date periodically to prepare for data loss.

When using an intranet environment through a global address, connecting to a SCADA or an unauthorized terminal such as an 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.

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.

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.

Precautions for Safe Use

Transporting and Disassembly

- Do not attempt to disassemble, repair, or modify any Units. Doing so may result in malfunction or fire.
- Do not drop any Unit or subject it to abnormal vibration or shock. Doing so may result in Unit malfunction or burning.
- When transporting any Unit, use the special packing box for it. Also, do not subject the Unit to excessive vibration or shock during transportation.

Mounting

- Always turn OFF the power supply before mounting the Units. If the power supply is not OFF, the Unit may result in malfunction or may be damaged.
- Do not exceed the maximum number of mountable X Bus Units in the specifications. Doing so may result in Unit malfunction or burning.

Wiring

- Do not pull on the cables or bend the cables beyond their natural limit.
  Do not place heavy objects on top of the cables or other wiring lines.
  Doing so may break the cables.
- Mount connectors only after checking the mounting location carefully.
- Be sure that the communications cables are locked.

Operation

- After you change any Unit settings, carefully check the safety of the controlled system before you restart the Unit.

Turning OFF the Power Supply

- Always turn OFF the power supply to the Controller before you attempt any of the following.
  a) Mounting or removing the NX Units, X Bus Units or CPU Units
  b) Assembling the Units
  c) Setting DIP switches or rotary switches
  d) Connecting cables or wiring the system
  e) Connecting or disconnecting the terminal blocks or connectors
  The power supply circuit in the CPU Unit may continue to supply power to the Controller for a few seconds after the power supply turns OFF. The POWER indicator is lit during this time. Confirm that the POWER indicator is not lit before you perform any of the above actions.
- Never turn OFF the power supply to the Controller when the BUSY indicator of the NX-series EtherNet/IP Unit is flashing. While the BUSY indicator is flashing, the settings in the NX-series

EtherNet/IP Unit are being backed up in the built-in non-volatile memory. This data will not be backed up correctly if the power supply is turned OFF. Also, a minor fault level Controller error will occur the next time you start operation, and the NX-series EtherNet/IP Unit will stop the operation.

- Do not disconnect the cable or turn OFF the power supply to the Controller while transferring the settings of the NX-series EtherNet/IP Unit from the Support Software.

General Communications

- In the data link communications, create a user program that uses receive data only when there is no current error in the data link originator device with reference to the *EIP_Comm1Status.TargetNodeErr[255]* (CIP Communications1 Target Node Error Information) or *EIP_Comm2Status.TargetNodeErr[255]*(CIP Communications2 Target Node Error Information).
  If there is an error in the source device, the data for the data link may contain incorrect values.
- Before you start the communications of data that is required to operate the equipment, confirm that the data reached the proper destination after you set the IP Address.
- Unexpected operation may result if inappropriate data link tables are set. Even if appropriate data link tables have been set, confirm that the controlled system will not be adversely affected before you transfer the data link tables. The data links start automatically after the data link tables are transferred.

EtherNet/IP Communications

- Make sure that the communications distance, number of nodes connected, and method of connection for EtherNet/IP are within specifications. Do not connect EtherNet/IP communications to EtherCAT or other networks. An overload may cause the network to fail or malfunction.
- All related EtherNet/IP nodes are reset when you transfer settings for the NX-series EtherNet/IP Unit (including IP addresses and tag data links settings). The settings can only be enabled after the reset. Confirm that the system will not be adversely affected by resetting nodes before you transfer the settings.
- Confirm that the system will not be adversely affected before you start the tag data link communications.
- Confirm that the system will not be adversely affected before you stop the tag data link communications.
- Confirm that the system will not be adversely affected by resetting nodes before you transfer the tag data link settings and routing tables.
- To ensure tag set concurrency, match the settings of the *task that updates a tag set on the X Bus* with the refreshing task for variables.
- If EtherNet/IP tag data links (cyclic communications) are used with a repeating hub, the communications load on the network will increase. This will increase collisions and may prevent stable communications. Do not use repeating hubs on networks where tag data links are used. Use an Ethernet switch instead.

Restoring Data

- You cannot back up, restore, or compare data for disabled Units. After you restore data, sufficiently confirm that operation is correct before you start actual operation.

Unit Replacement

- Make sure to transfer the tag data link settings and routing tables before restarting operation after you replaced the NX-series EtherNet/IP Unit.

Precautions for Correct Use

Storage and Installation

- Follow the instructions in this manual to correctly perform installation.
- Do not operate or store the Controller in the following locations. Doing so may result in burning, in operation stopping, or in malfunction.
  a) Locations subject to direct sunlight
  b) Locations subject to temperatures or humidity outside the range specified in the specifications
  c) Locations subject to condensation as the result of severe changes in temperature
  d) Locations subject to corrosive or flammable gases
  e) Locations subject to dust (especially iron dust) or salts
  f) Locations subject to exposure to water, oil, or chemicals
  g) Locations subject to shock or vibration
- Take appropriate and sufficient countermeasures when installing the Controller in the following locations.
  a) Locations subject to strong, high-frequency noise
  b) Locations subject to static electricity or other forms of noise
  c) Locations subject to strong electromagnetic fields
  d) Locations subject to possible exposure to radioactivity
  e) Locations close to power lines
- Before touching a Unit, be sure to first touch a grounded metallic object in order to discharge any static build-up.
- Install the Controller away from sources of heat and ensure proper ventilation. Not doing so may result in malfunction, in operation stopping, or in burning.

Mounting

- When you install the Unit, be careful not to touch or bump the pins in the X Bus connector.
- When you handle the Unit, be careful not to apply stress to the pins in the X Bus connector. If the Unit is installed and the power supply is turned ON when the pins in the X Bus connector are deformed, contact failure may cause malfunctions.
- Attach a cover to the left end of the X Bus Unit to prevent entry of foreign objects. Signal short-circuit or contact failure may cause malfunctions.
- If you use DIN Track Insulation Spacers to install a CPU Rack, the height will be increased by approximately 10 mm. Make sure that the CPU Rack and connecting cables do not come into contact with other devices.

Wiring

- Do not allow wire clippings, shavings, or other foreign material to enter any Unit. Otherwise, Unit burning, failure, or malfunction may occur. Cover the Units or take other suitable countermeasures, especially during wiring work.

Security Measures

- If you forget your user name or password, go online with administrator privileges and check your user authentication settings.
  If you forget the user name or password for administrator privileges, start the CPU Unit in Safe Mode and connect the Sysmac Studio online to perform the Clear All Memory operation following **If you cannot log in** in the Authentication in Safe Mode Dialog Box.
  Refer to the *NX-series NX502 CPU Unit Hardware User's Manual (Cat. No. W629)* for how to start the CPU Unit in Safe Mode.
- If you cannot go online with the Sysmac Studio because of forgetting the registered IP Address for Packet Filter settings, connect from the built-in EtherNet/IP port of the CPU Unit. Refer to *Troubleshooting When You Cannot Go Online from the Sysmac Studio* in the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* for details.

Disposal

- When disposing of or transferring our products, information such as user data stored in the device may be seen by third parties, resulting in information leakage. It is recommended that you erase the data on your responsibility before disposing of or transferring the device. Omron shall not be liable for any loss, damage, or other expenses incurred directly or indirectly in the event of any information leakage due to disposal or transfer.
  For details on *complete data erasure function* for completely erasing user data, refer to the *NJ/NX-series CPU Unit Software User's Manual (Cat. No. W501)*.

Regulations and Standards

Refer to the following manuals for regulations and standards.

- *NX-series NX502 CPU Unit Hardware User’s Manual (Cat. No. W629)*

Unit Versions

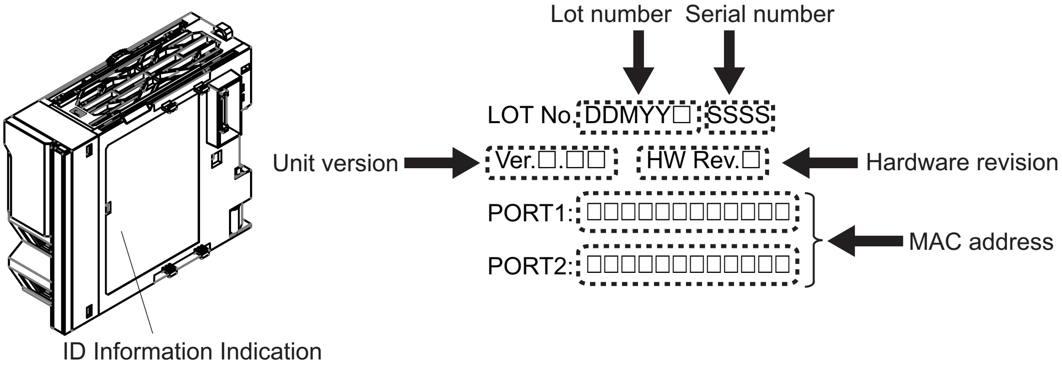
This section describes the notations of unit version and how to check them.

Unit Versions

The unit version is the modification number of the Unit. Even when two Units have the same model number, they will have some functional differences if they have different unit versions.

Checking Unit Versions on ID Information Indications

The unit version is given on the ID information indications on the side of the product.
The ID information on an NX-series EtherNet/IP Unit is shown in the following figure.



The meanings of the ID information are shown in the following table.

Name	Function
Unit version	Shows the unit version of the Unit.
Lot number and serial number	Shows the lot number and the serial number of the Unit. DDMYY: Lot number, □: For use by OMRON, SSSS: Serial number M is 1 to 9 for January to September, X for October, Y for November, and Z for December.
Hardware revision	Shows the hardware revision of the Unit.
MAC addresses	Shows the MAC addresses of the port 1 and port 2 on the Unit.

Checking with the Support Software

Refer to the user's manual of the connected CPU Unit for how to check the unit version of the X Bus Unit.

Related Manuals

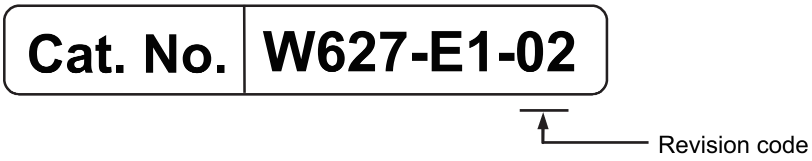
The following manuals are related. Use these manuals for reference.

Manual name	Cat.No.	Model numbers	Application	Description
NX-series EtherNet/IP™ Unit User's Manual	W627	NX-EIP201	Learning how to use the NX-series EtherNet/IP Unit.	Information on the NX-series EtherNet/IP Unit is provided. Information is provided on the basic setup, tag data links, and other features.
NX-series NX502 CPU Unit Hardware User's Manual	W629	NX502-□□□□	Learning the basic specifications of the NX502 CPU Units, including introductory information, designing, installation, and maintenance. Mainly hardware information is provided.	An introduction to the entire NX502 system is provided along with the following information on the CPU Unit. • Features and system configuration • Introduction • Part names and functions • General specifications • Installation and wiring • Maintenance and inspection
NJ/NX-series CPU Unit Software User's Manual	W501	NX701-□□□□ NX502-□□□□ NX102-□□□□ NX1P2-□□□□ NJ501-□□□□ NJ301-□□□□ NJ101-□□□□	Learning how to program and set up an NJ/NX-series CPU Unit. Mainly software information is provided.	The following information is provided on a Controller built with an NJ/NX-series CPU Unit. • CPU Unit operation • CPU Unit features • Initial settings • Programming based on IEC 61131-3 language specifications
NJ/NX-series Instructions Reference Manual	W502	NX701-□□□□ NX502-□□□□ NX102-□□□□ NX1P2-□□□□ NJ501-□□□□ NJ301-□□□□ NJ101-□□□□	Learning detailed specifications on the basic instructions of an NJ/NX-series CPU Unit.	The instructions in the instruction set (IEC 61131-3 specifications) are described.
NJ/NX-series CPU Unit Motion Control User's Manual	W507	NX701-□□□□ NX502-□□□□ NX102-□□□□ NX1P2-□□□□ NJ501-□□□□ NJ301-□□□□ NJ101-□□□□	Learning about motion control settings and programming concepts.	The settings and operation of the CPU Unit and programming concepts for motion control are described.
NJ/NX-series Motion Control Instructions Reference Manual	W508	NX701-□□□□ NX502-□□□□ NX102-□□□□ NX1P2-□□□□ NJ501-□□□□ NJ301-□□□□ NJ101-□□□□	Learning about the specifications of the motion control instructions.	The motion control instructions are described.
NJ/NX-series CPU Unit Built-in EtherCAT® Port User's Manual	W505	NX701-□□□□ NX502-□□□□ NX102-□□□□ NX1P2-□□□□ NJ501-□□□□ NJ301-□□□□ NJ101-□□□□	Using the built-in EtherCAT port on an NJ/NX-series CPU Unit.	Information on the built-in EtherCAT port is provided. This manual provides an introduction and provides information on the configuration, features, and setup.

Manual name	Cat.No.	Model numbers	Application	Description
NJ/NX-series CPU Unit Built-in EtherNet/IP™ Port User's Manual	W506	NX701-□□□□ NX502-□□□□ NX102-□□□□ NX1P2-□□□□ NJ501-□□□□ NJ301-□□□□ NJ101-□□□□	Using the built-in EtherNet/IP port on an NJ/NX-series CPU Unit.	Information on the built-in EtherNet/IP port is provided. Information is provided on the basic setup, tag data links, and other features.
NJ/NX-series CPU Unit OPC UA User's Manual	W588	NX701-□□□□ NX502-□□□□ NX102-□□□□ NJ501-1□00	Using the OPC UA.	Describes the OPC UA.
NX-series CPU Unit FINS Function User's Manual	W596	NX701-□□20 NX502-□□□□ NX102-□□□□	Using the FINS function of an NX-series CPU Unit.	Describes the FINS function of an NX-series CPU Unit.
NJ/NX-series Troubleshooting Manual	W503	NX701-□□□□ NX502-□□□□ NX102-□□□□ NX1P2-□□□□ NJ501-□□□□ NJ301-□□□□ NJ101-□□□□	Learning about the errors that may be detected in an NJ/NX-series Controller.	Concepts on managing errors that may be detected in an NJ/NX-series Controller and information on individual errors are described.
Sysmac Studio Version 1 Operation Manual	W504	SYSMAC -SE2□□□	Learning about the operating procedures and functions of the Sysmac Studio.	Describes the operating procedures of the Sysmac Studio.
NXR-series IO-Link Master Unit for EtherNet/IP™ User's Manual	W619	NXR-ILM08C-EIT	Learning how to use an NXR-series IO-Link Master Unit for EtherNet/IP.	The hardware, setup methods, and functions of the NXR-series IO-Link Master Unit for EtherNet/IP are described.

Revision History

A manual revision code appears as a suffix to the catalog number on the front and back covers of the manual.



Revision code	Date	Revised content
01	April 2023	Original production
02	June 2023	Corrected mistakes.

1

Features and System Configuration

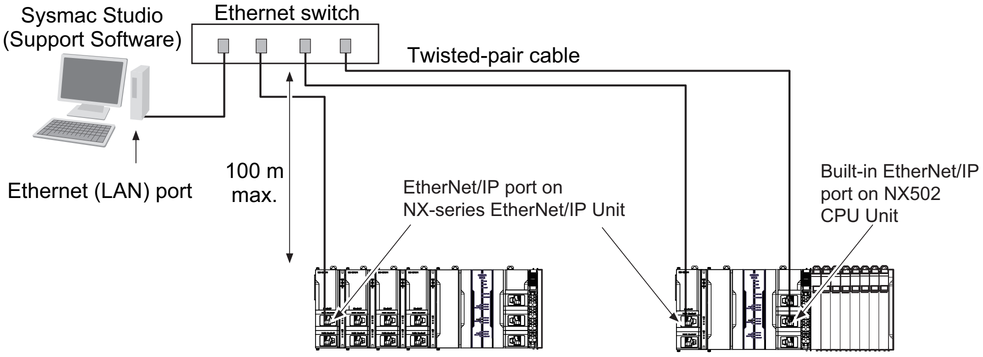
This section describes the features, system configuration, introduction to communications services, and Support Software of the NX-series EtherNet/IP Unit.

1-1 Features

The NX-series EtherNet/IP Unit has the EtherNet/IP function when mounted on the X Bus.
The EtherNet/IP and NX-series EtherNet/IP Unit have the following features.

1-1-1 EtherNet/IP Features

EtherNet/IP is an industrial multi-vendor network that uses Ethernet.
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. Because EtherNet/IP uses standard Ethernet technology, various general-purpose Ethernet devices can be used in the network.



EtherNet/IP System Configuration Example

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

The EtherNet/IP protocol supports implicit communications, which allows cyclic communications (called tag data links in this manual) with EtherNet/IP devices.

● Tag Data Link (Cyclic Communications) Cycle Time

Tag data links (cyclic communications) 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 concurrency of the connection's data is maintained.
Because the refresh cycle can be set for each connection, each application can communicate at its ideal refresh cycle. For example, interprocess interlocks can be transferred at high speed, while the production commands and the status monitor information are transferred at low speed.

1-1-2 Features of NX-series EtherNet/IP Units

The features of the NX-series EtherNet/IP Units are described below.

● X Bus Connection which Enable High-speed and Large Capacity Data Transfer

The NX502 CPU Unit has a built-in X Bus, which is an internal bus capable of transferring data at higher speed and larger capacity than the NX bus. The NX-series EtherNet/IP Unit is one of the X Bus Units that are connected to the X Bus.
The X Bus connector is located on the left side of the NX502 CPU Unit. You can connect the NX-series EtherNet/IP Unit on the left side of the NX502 CPU Unit.

● Up to Ten EtherNet/IP Networks can be Built

The NX-series EtherNet/IP Unit is equipped with two EtherNet/IP ports for EtherNet/IP communications as standard. Also, you can mount up to four Units to an NX502 CPU Unit. Therefore, including the two ports of the built-in EtherNet/IP ports on the NX502 CPU Unit, you can build up to ten EtherNet/IP networks.
The maximum of ten network segmentation enables large capacity data communications of production information, quality information, and equipment information to improve yield rates in production lines.
Furthermore, flexible and safe line configurations on large-scale assembly lines are possible.

Precautions for Correct Use

The NX-series EtherNet/IP Unit uses IO refresh time to exchange data between the CPU Unit and the X Bus Unit. Calculate the approximate task execution time to check the effect on the task execution time.

● Tag Data Links

Cyclic communications between Controllers or between a Controller and other devices are possible on an EtherNet/IP network.
High-speed data exchange can be performed through tag data links.

Precautions for Correct Use

The I/O refresh time varies depending on the number of connections for tag data link communications. Check the effect of the number of connections for tag data link communications on the task execution time.

● CIP Message Communications

You can send CIP commands to devices on the EtherNet/IP network when required by executing CIP communications instructions in a program.
As a result, it is possible to send and receive data with the devices on the EtherNet/IP network.

Additional Information

CIP (Common Industrial Protocol)

CIP is a shared industrial protocol for the OSI application layer. The CIP is used in networks such as EtherNet/IP, CompoNet, and DeviceNet.

Data can be routed easily between networks that are based on the CIP. You can therefore easily configure a transparent network 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. Because the producer can send the same data with the same characteristics in a multicast format, the time required for the transfer is fixed and not dependent on the number of consumer nodes. (Either multicast or unicast can be selected.)

● BOOTP Client

If the built-in EtherNet/IP port is set in the BOOTP settings, the BOOTP client operates when the Controller power is turned ON, and the IP address is obtained from the BOOTP server.

It is possible to set all of the IP addresses of multiple EtherNet/IP ports at the same time.

● DNS Client for Specifying Host Names

You can directly specify IP addresses, but you can also use the host names instead of the IP addresses for SNMP managers (DNS client or hosts settings).

This will help identify the IP address automatically even after the IP addresses of relevant servers are changed due to system revisions.

*1. A separate DNS server is necessary when you use host names with the DNS client.

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

● Network Management with an SNMP Manager

The SNMP agent passes internal status information from the EtherNet/IP port to network management software that uses an SNMP manager.

*1. A separate SNMP manager is necessary for network management.

● Complete Troubleshooting Functions

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

- Self-diagnosis at startup
- Event log that records the time of occurrence and other error details

● IP Routing Function

The NX-series EtherNet/IP Unit is equipped with two EtherNet/IP ports for EtherNet/IP communications as standard, and this allows to separate the information network from the control network. In addition, the EtherNet/IP ports support the IP routing function to send IP packets to devices on other IP network segments.

*1. In order to use the function, you must appropriately set the IP router table and default gateway settings for each device on the network according to your network configuration. For details on the settings, refer to *7-1* ***TCP/IP Settings*** *Display* on page 7-2.

● CIP Safety on EtherNet/IP Compatible

Combined with the NX-SL5□□□ Safety Control Unit, you can build a system which uses CIP Safety on EtherNet/IP communications in networks between Controllers and field networks. Safety communications by CIP Safety is enabled with devices that support CIP Safety on EtherNet/IP and other Safety CPU Units.

Precautions for Correct Use

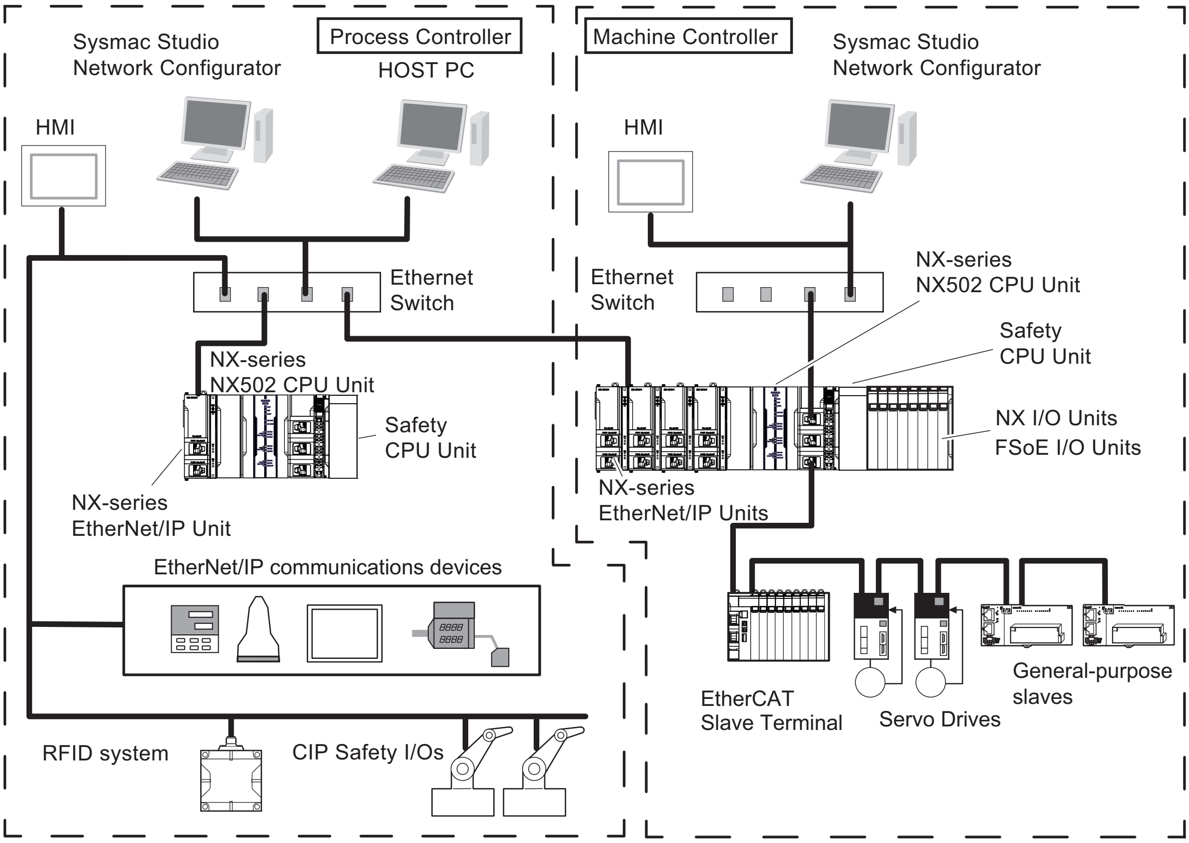
- An NX-series EtherNet/IP Unit is required to perform CIP Safety communications. The built-in EtherNet/IP port on an NX502 CPU Unit does not support the CIP Safety communications.
- CIP Safety communications and tag data links cannot be used together in one NX-series EtherNet/IP Unit.
- The I/O refresh time varies depending on the number of connections for CIP Safety communications. Check the effect of the number of connections for CIP Safety communications on the task execution time.

● LLDP

The LLDP (Link Layer Discovery Protocol) enables to exchange information with other network devices that are connected to a physically communicable range.

1-2 System Configuration

The following figure shows a configuration example for a system that uses the NX-series EtherNet/IP Unit.



The following table shows the description, NX502 CPU Unit connection method, and quantity for each configuration element in the figure above.

Configuration element	Description	NX502 CPU Unit connection method	Qty
NX502 CPU Unit	A CPU Unit to which the NX-series EtherNet/IP Unit is connected. This Unit performs machine control and process control of the system.	---	One Unit for machine control, and one Unit for overall process control
NX-series EtherNet/IP Unit	One of X Bus Units which performs EtherNet/IP communications.	X Bus	Up to four Units per an NX502 CPU Unit
NX I/O Unit	An interface Unit to connect an NX-series CPU Unit to control devices such as sensors and actuators. This Unit can also be connected to an NX-series Communications Coupler Unit.	NX bus of CPU Unit and Slave Terminal	Zero to multiple Units (depends on application)
Safety CPU Unit	A CPU Unit which controls the safety circuit of manufacturing equipment. This Unit controls both of the safety control within equipment by FSoE and the line safety control by CIP Safety.	NX bus of CPU Unit	One Unit per an NX502 CPU Unit

Configuration element	Description	NX502 CPU Unit connection method	Qty
FSoE I/O Unit	This Unit inputs safety input signals and outputs safety output signals in combination with a Safety CPU Unit.	NX bus of CPU Unit and Slave Terminal	Zero to multiple Units (depends on application)
Servo Drive	A control device for an electric motor assembled in a control equipment. It is controlled by the Motion Control Function Module within the CPU Unit.	Built-in EtherCAT port	Zero to multiple Units (depends on application)
EtherCAT general-purpose slave	A general-purpose slave connected to the EtherCAT.	Built-in EtherCAT port	Zero to multiple Units (depends on application)
Ethernet switch	An Ethernet switch connects devices on the network by packet switching and transfers the received data to the target device.	EtherNet/IP port on CPU Unit and NX-series EtherNet/IP Unit	Zero to multiple Units (depends on application)
HMI	An HMI performs operation input to the manufacturing equipment and displays status of the manufacturing equipment.	EtherNet/IP port on CPU Unit and NX-series EtherNet/IP Unit	Zero to multiple Units (depends on application)
Sysmac Studio Network Configurator	Support Software for NX502 CPU Unit.	EtherNet/IP port on CPU Unit and NX-series EtherNet/IP Unit	One to multiple Units (depends on application)
HOST PC	This computer performs EtherNet/IP communications.	EtherNet/IP port on CPU Unit and NX-series EtherNet/IP Unit	One to multiple Units (depends on application)
RFID system	This system uses electromagnetic fields and radio waves to exchange product identification information. Communications is performed with a Modbus/TCP client.	EtherNet/IP port on CPU Unit and NX-series EtherNet/IP Unit	Zero to multiple Units (depends on application)
CIP Safety I/O	A connection interface for sensors and actuators of safety I/O devices. CIP Safety on EtherNet/IP compatible.	EtherNet/IP port on NX-series EtherNet/IP Unit	Zero to multiple Units (depends on application)

1-3 Introduction to Communications Services

This section provides an introduction to the communications services of the NX-series EtherNet/IP Unit.

1-3-1 CIP (Common Industrial Protocol) Communications Services

The services using CIP include tag data link and CIP message communications.

Tag Data Links (Cyclic Communications)

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

Normally, a connection is started with the target device for each tag set that was created with the Network Configurator to start communications for tag data links for an EtherNet/IP port. One connection is used per tag set.

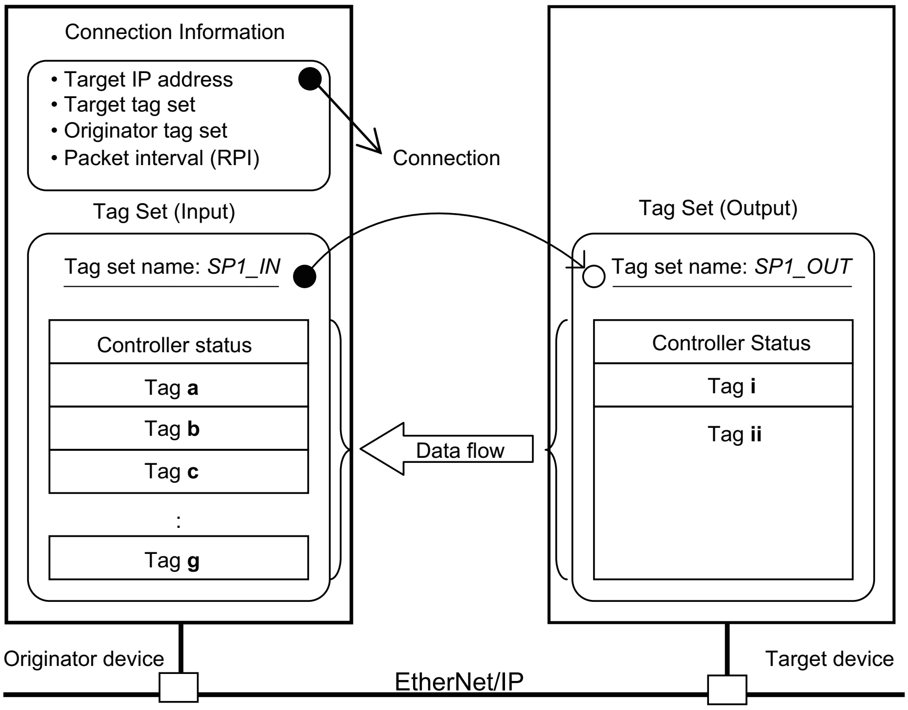
The maximum number of connections that can be registered is 256, or a total of 512 with two ports.

Additional Information

The NX502 CPU Unit can be used with the NX-EIP201 (EherNet/IP Unit) for tag data link communications.

However, check the effect on task execution time because it increases I/O refreshing time.

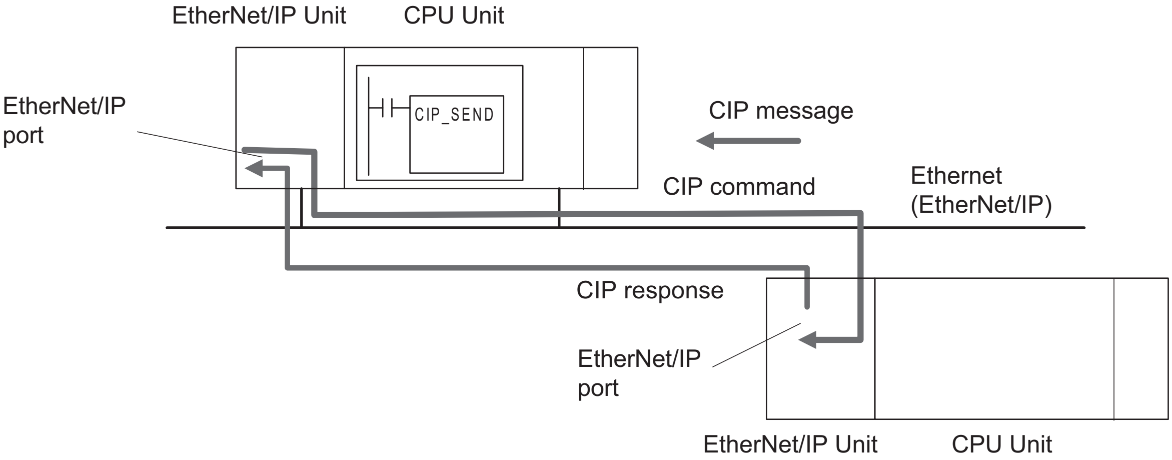
Refer to *2-1 Specifications* on page 2-2 for the EtherNet/IP port tag and tag set specifications.



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

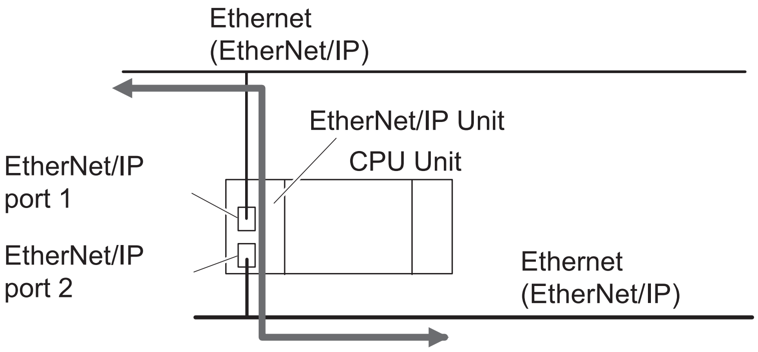
CIP Message Communications

User-specified CIP commands can be sent to devices on the EtherNet/IP network.
CIP commands can be sent and their responses received by executing the CIP communications instructions from the user program in the CPU Unit.



By specifying a route path, you can send CIP messages (CIP commands and responses) to a device on another CIP-based network segment (CIP routing function for message communications). However, since the starting point of route path is the CPU Unit, it is necessary to set the route path from the CPU Unit through the NX-series EtherNet/IP Unit.
The maximum number of levels of CIP routing via the ports is eight for any combination of CS, CJ, NJ, and NX-series CPU Units. Note that the number of levels of IP routing using an L3 Ethernet switch is not counted in the number of levels of CIP routing via the ports.

- Because there are two EtherNet/IP ports, CIP routing is possible by the NX-series EtherNet/IP Unit alone.



Additional Information

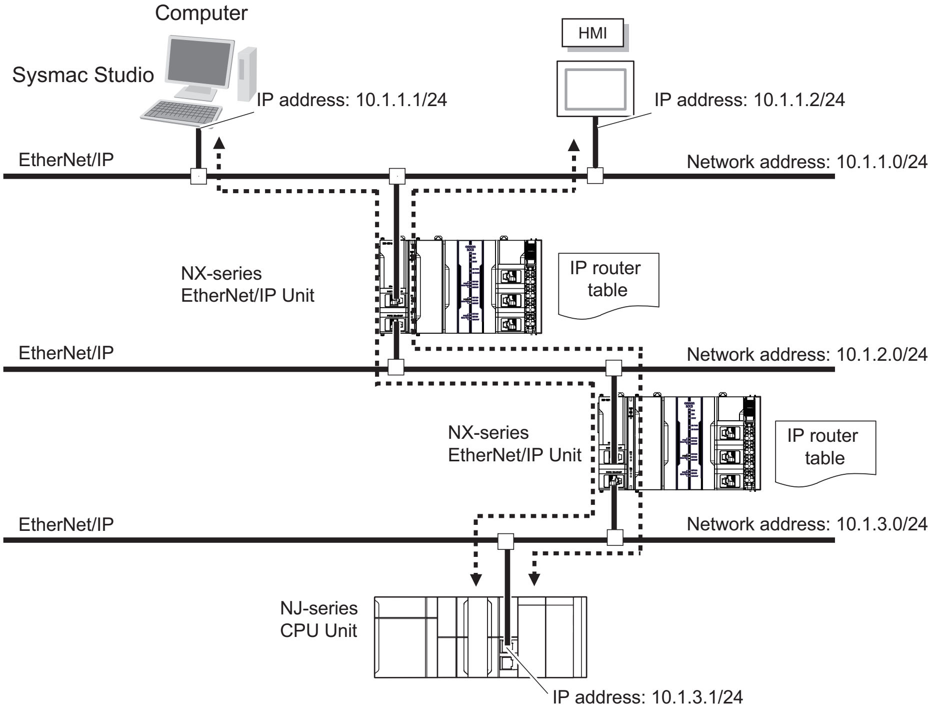
In CIP routing, a node (Unit) that routes information subtracts the equivalent of one hop from the timeout, deletes its own address from the route information, and relays the information to the next node (Unit).
When a timeout is specified, the timeout for the actual request service processing is set in the last hop.
In the case of relay hops, the timeout for the relay route must be added to the timeout for the request.
OMRON products that support CIP subtract 5 seconds per hop.

1-3-2 IP Routing

The IP routing function sends IP packets to other network segments based on the routing information set in the IP router table.
To communicate with devices on other network segments, you must set the IP router table and default gateway settings for the CPU Unit and each device on the network appropriately for your network configuration.

Precautions for Correct Use

You cannot create tag data links between multiple CPU Units using IP routing.



● Port Forward - IP Forward

This function transfers the communications data between the network for the EtherNet/IP port 1 and the network for the EtherNet/IP port 2. Select the *Use* Option for **IP Forward** to transfer the communications data. If you select the *Do not use* Option for **IP Forward**, any other IP packets than those addressed to the NX-series EtherNet/IP Unit are discarded. Refer to *7-1* ***TCP/IP Settings*** *Display* on page 7-2 for details on the settings.

Additional Information

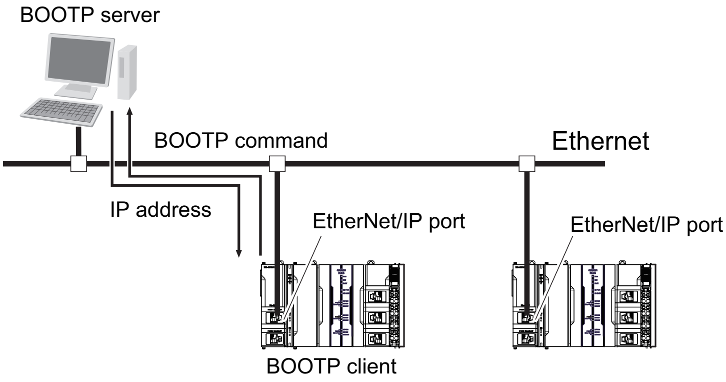
CIP routing is not affected by the **IP Forward** setting.

1-3-3 Packet Filter

IP packets are filtered in the receive processing at the EtherNet/IP ports. Specify packets allowed to be received by IP address or TCP/UDP port number.

1-3-4 BOOTP Client

You set the EtherNet/IP port to the BOOTP setting to use the BOOTP client to obtain settings, such as the EtherNet/IP port IP address, from the BOOTP server.

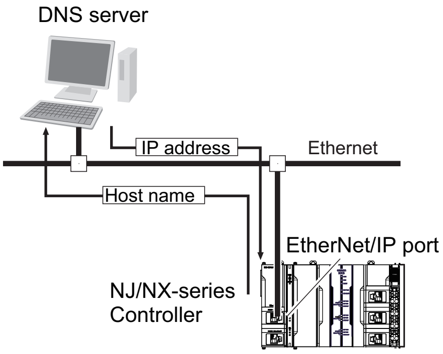


The EtherNet/IP port IP address is obtained from the BOOTP server when the power is turned ON.

1-3-5 Specifying Host Names

You can directly specify IP addresses, but you can also use the host names instead of the IP addresses for SNMP managers (DNS client or hosts settings).

Example: Setting Host Names on the DNS Server



Precautions for Correct Use

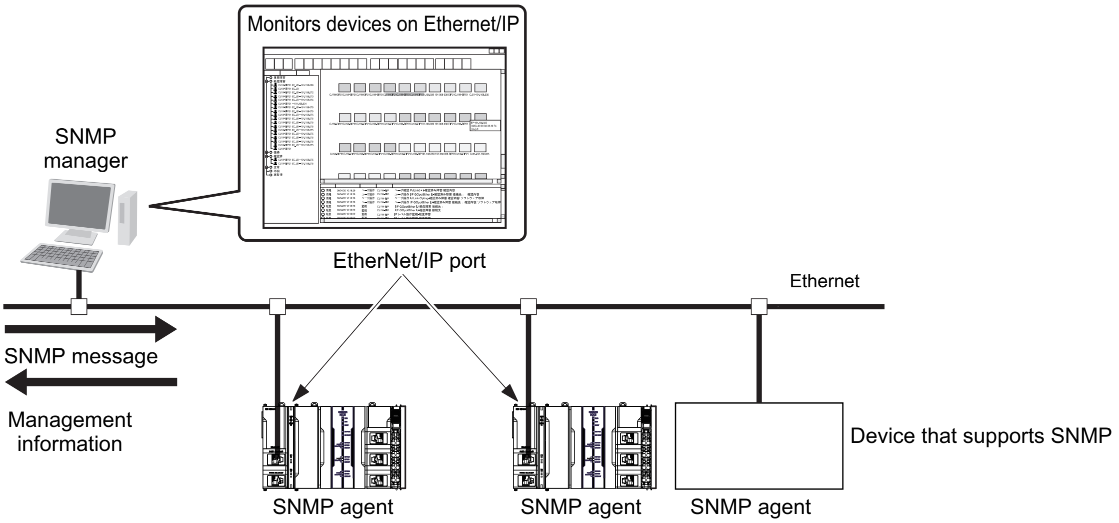
- A DNS server is required to use the server host names for the DNS client.

1-3-6 SNMP Agent

The SNMP agent has the following functions.

SNMP Agent

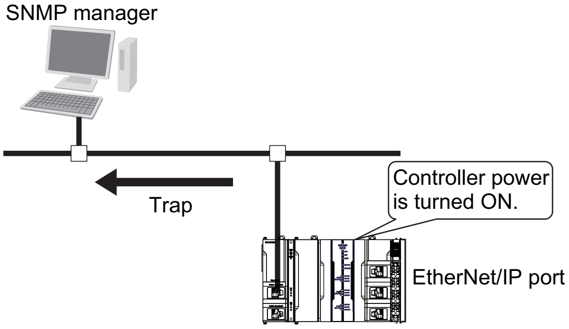
EtherNet/IP port internal status information is provided to network management software that uses an SNMP manager.



SNMP Trap

When specific conditions occur, the EtherNet/IP port that is set as the SNMP agent sends status notification reports to the SNMP manager.
The SNMP manager can learn about changes in status even without periodically monitoring the EtherNet/IP port.
Status notification reports are sent under the following conditions.

- When the Controller is turned ON
- When links are established
- When an SNMP agent fails to be authorized



1-3-7 LLDP

LLDP (Link Layer Discovery Protocol) is a protocol used to exchange information with other network devices that are connected to a physically communicable range. The NX-series EtherNet/IP Unit obtains information of other network devices using the SNMP function. The information to be exchanged includes chassis types and system names of the both. Refer to *Lldp Group* on page 11-19 for details on the information to be exchanged.

1-4 Support Software

The followings are the Support Software for using the NX-series EtherNet/IP Unit.

● Sysmac Studio

This software is used to configure all functions of the NX-series EtherNet/IP Unit.
The NX-series EtherNet/IP Unit is supported by version 1.54 or higher.
Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for details on the Sysmac Studio.

● Network Configurator

This software is used to configure tag data links.
The NX-series EtherNet/IP Unit is supported by version 3.74 or higher.
For the details on the settings, refer to *Section 9 Tag Data Link Functions* on page 9-1.

2

Specifications and Application Procedures

This section describes the specifications and application procedures of the NX-series EtherNet/IP Unit.

2-1 Specifications

This section provides general specifications, performance specifications, and function specifications of the NX-series EtherNet/IP Unit.

2-1-1 General Specifications

The general specifications of the NX-series EtherNet/IP Unit are given below.

Item		Specification
Enclosure		Mounted in a panel
Grounding method		Ground to less than 100 Ω.
Dimensions: Height × Depth × Width		100 × 120 × 39 (mm)
Weight		350 g max.
Power consumption		8.1 W max.
Operating environment	**Ambient operating temperature**	0 to 55°C
	Ambient operating humidity	10% to 95% (with no icing or condensation)
	Atmosphere	Must be free from corrosive gases.
	Ambient storage temperature	-25 to 70°C (with no icing or condensation)
	Altitude	2,000 m max.
	Pollution degree	2 or less: Meets IEC 61010-2-201.
	Noise immunity	2 kV on power supply line (Conforms to IEC 61000-4-4.)
	Overvoltage category	Category II: Meets IEC 61010-2-201.
	EMC immunity level	Zone B
	Vibration resistance	Conforms to IEC 60068-2-6. 5 to 8.4 Hz with 3.5-mm amplitude, 8.4 to 150 Hz, acceleration of 9.8 m/s^2 100 min each in X, Y, and Z directions (10 sweeps of 10 min each = 100 min total) Gravity acceleration is assumed to be G=9.8m/s^2.
	Shock resistance	Conforms to IEC 60068-2-27, 147 m/s^2, 3 times in X, Y, and Z directions. Gravity acceleration is assumed to be G=9.8m/s^2.
	Mounting method	Mount to DIN Track
	Mounting direction	One direction (upright)
Applicable standards		Refer to the OMRON website (http://www.ia.omron.com/) or consult your OMRON representative for the applicable standards.

2-1-2 Performance Specifications

The specifications of the NX-series EtherNet/IP Unit are given below.

Item			NX-EIP201
EtherNet/IP port	**Number of ports**		2
	Physical layer		10BASE-T, 100BASE-TX, or 1000BASE-T
	Frame length		1,514 bytes max.
	Media access method		CSMA/CD
	Modulation		Baseband
	Topology		Star
	Baud rate		1 Gbps (1000BASE-T) max.
	Transmission media		STP (shielded, twisted-pair) cable of Ethernet category 5, 5e or higher
	Maximum transmission distance between Ethernet switch and node		100 m
	Maximum number of cascade connections		There are no restrictions if an Ethernet switch is used.
	LLDP		Supported.
	BOOTP client		Supported.
	DHCP client		Not supported.
	DNS client		Supported.
	SNMP agent, traps		Supported.
	CIP service: Tag data links (cyclic communications)	**Maximum number of connections**	256 per port 512 total
		Packet interval*1*2	Can be set for each connection. 1.0 to 10,000 ms in 1.0-ms increments
		Allowed communications bandwidth per Unit	40,000 pps*3*4 (including heartbeat)
		Maximum number of tag sets	256 per port 512 total
		Tag types	Network variables CIO, Work, Holding, DM, or EM Areas can be used.
		Number of tags per connection (i.e., per tag set)	64 (63 tags if Controller status is included in the tag set.)
		Maximum number of tags	1,024 per port 2,048 total
		Maximum link data size per node (total size for all tags)	369,664 bytes per port (total of 739,328 bytes with two ports)
		Maximum data size per connection	1,444 bytes
		Maximum number of registrable tag sets	256 per port 512 total (1 connection = 1 tag set)
		Maximum tag set size	1,444 bytes (Two bytes are used if Controller status is included in the tag set.)
		Changing tag data link parameters when Controller is in RUN mode	Supported*5

Item				NX-EIP201
		Multicast packet filter[*6]		Supported.
	CIP message service: Explicit messages	**Class 3 (number of connections)**		128 per port 256 total (clients plus server)
		UCMM (non-connection type)	**Maximum number of clients that can communicate at one time**	32 per port 64 total
			Maximum number of servers that can communicate at one time	32 per port 64 total
		CIP routing		Supported CIP routing is supported for the following remote Units: NX-EIP201 NX701-□□□□, NX502-□□□□, NX102-□□□□, NX1P2-□□□□ NJ501-□□□□, NJ301-□□□□, NJ101-□□□□, CS1W-EIP21, CJ1W-EIP21, CJ2H-CPU□□-EIP, CJ2M-CPU3□ Using a combination of any Units above, communication can be extended up to a maximum of 8 levels.
	CIP Safety routing[*7]	**Maximum number of routable CIP Safety connections**		84 total (originator: 80, target: 4)
		Maximum routable safety data length per connection		32 bytes
	SNMP	**Agents**		SNMPv1 or SNMPv2C
		MIB		MIB-II
	EtherNet/IP conformance test			Conforms to CT18.
	Ethernet interface			10BASE-T, 100BASE-TX, or 1000BASE-T Auto negotiation

*1. Data will be refreshed at the set interval, regardless of the number of nodes.

*2. The approximate I/O response time of the tag data link is determined by the relationship between the packet interval and the number of connections. Refer to *12-3 Tag Data Link I/O Response Time* on page 12-23 for details.

*3. “pps” means packets per second, i.e., the number of communications packets that can be sent or received in one second.

*4. When the Unit is performing tag data link communications where the allowable communications bandwidth per Unit is close to or greater than 30,000 pps, the following functions may not be used properly. In that case, use the built-in EtherNet/IP port on the CPU Unit or an EtherNet/IP port of a different NX-series EtherNet/IP Unit.

- Connecting the Sysmac Studio online from the EtherNet/IP port of the NX-series EtherNet/IP Unit
- Connecting the Network Configurator online from the EtherNet/IP port of the NX-series EtherNet/IP Unit
- Connecting the NA-series Programmable Terminal online from the EtherNet/IP port of the NX-series EtherNet/IP Unit

- Port forward via the NX-series EtherNet/IP Unit
- CIP message communications
- SNMP function

These functions of the NX-series EtherNet/IP Unit can be used via X Bus from the built-in EtherNet/IP port on the CPU Unit or an EtherNet/IP port of a different NX-series EtherNet/IP Unit.

*5. If the parameters of the EtherNet/IP port are changed, the port is restarted. When other nodes are in communications with the affected node, the communications will temporarily time out and automatically recover after the restart.

*6. As the EtherNet/IP port implements the IGMP client, unnecessary multi-cast packets can be filtered by using an Ethernet switch that supports IGMP Snooping.

*7. CIP Safety communications and tag data links cannot be used together in one NX-series EtherNet/IP Unit.

2-1-3 Function Specifications

The function specifications of the NX-series EtherNet/IP Unit are given below.

Item				NX-EIP201
Communications	**EtherNet/IP port**	**Communications protocol**		TCP/IP or UDP/IP
		CIP communications services	**Tag data links**	Programless cyclic data exchange is performed with the devices on the EtherNet/IP network.
			Message Communications	CIP commands are sent to or received from the devices on the EtherNet/IP network.
		TCP/IP application	**SNMP agent**	EtherNet/IP port internal status information is provided to network management software that uses an SNMP manager.
System management	**Event logs**	**Function**		Events are recorded in the logs.
		Maximum number of events	**System event log**	1,024
			Access event log	512
			User-defined event log	None

2-2 EtherNet/IP Communications Procedures

● Basic Operation

1 Wire the Ethernet network with twisted-pair cable.

Section 5 Installing Ethernet Networks on page 5-1

↓

2 Set the EtherNet/IP port IP address with the Sysmac Studio.

8-1 Determining IP Addresses on page 8-2

1. Use the Sysmac Studio to create a new project.
2. Set the local IP address in one of the following ways:

- Defaults:

Port	Default IP address The subnet mask is 255.255.255.0 for all ports.
Port 1	192.168.250.1
Port 2	192.168.251.1

- Set any IP address.
- Obtain from the BOOTP server.

↓

3 Perform a communications test with a PING command from a computer.

8-3 Testing Communications on page 8-13

↓

4 Use the Sysmac Studio to set the initial settings of the EtherNet/IP Function Module.

Section 7 Sysmac Studio Settings for the EtherNet/IP Port on page 7-1

- Set the TCP/IP settings and Ethernet settings as required.

● Using Tag Data Links

1 Import the variable settings for the tags that were created on the Sysmac Studio to the Network Configurator.

9-2-4 Creating Tags and Tag Sets on page 9-19

↓

2 Use the Network Configurator to create the tag data link table.

Section 9 Tag Data Link Functions on page 9-1

- Create the network configuration.
- Set the tags, tag sets, and connections.

↓

3 Connect the Network Configurator online.

↓

4 Download the tag data link setting.

↓

5 Start the tag data links (the links starts automatically when power is turned ON).

↓

6 Check operation.

Section 3 Part Names and Functions on page 3-1
Section 14 Troubleshooting on page 14-1

- Check the EtherNet/IP port indicators.
- Use the Sysmac Studio to check the communications status with the All Tag Data Link Communications Status device variable.
- Use the monitor function of the Network Configurator to confirm that the tag data links are in normal operation.

● Using the Message Communications Service

- CIP Communications Instructions

1	**Execute CIP communications instructions in the user program.**	*Section 10 CIP Message Communications* on page 10-1

↓

2	**Check operation.**	*Section 3 Part Names and Functions* on page 3-1 *Section 14 Troubleshooting* on page 14-1

- Use the Sysmac Studio to check the communications status with the end codes of the instructions (Done, Err, and ErrID).

● Using the SNMP Agent

1	**Use the Sysmac Studio to set the initial settings of the EtherNet/IP Function Module.**	*Section 11 SNMP Agent* on page 11-1

- Set the SNMP settings.
- Set the SNMP trap settings.

↓

2	**Check operation.**

- Check the event log to see if the SNMP agent started.

● Using the BOOTP

1	**Use the Sysmac Studio to set the initial settings of the EtherNet/IP Function Module.**	*Section 7 Sysmac Studio Settings for the EtherNet/IP Port* on page 7-1

- Set the BOOTP settings.

↓

2	**Check operation.**

- Check the event log to see if the BOOTP started.
- Check the Online device variable.

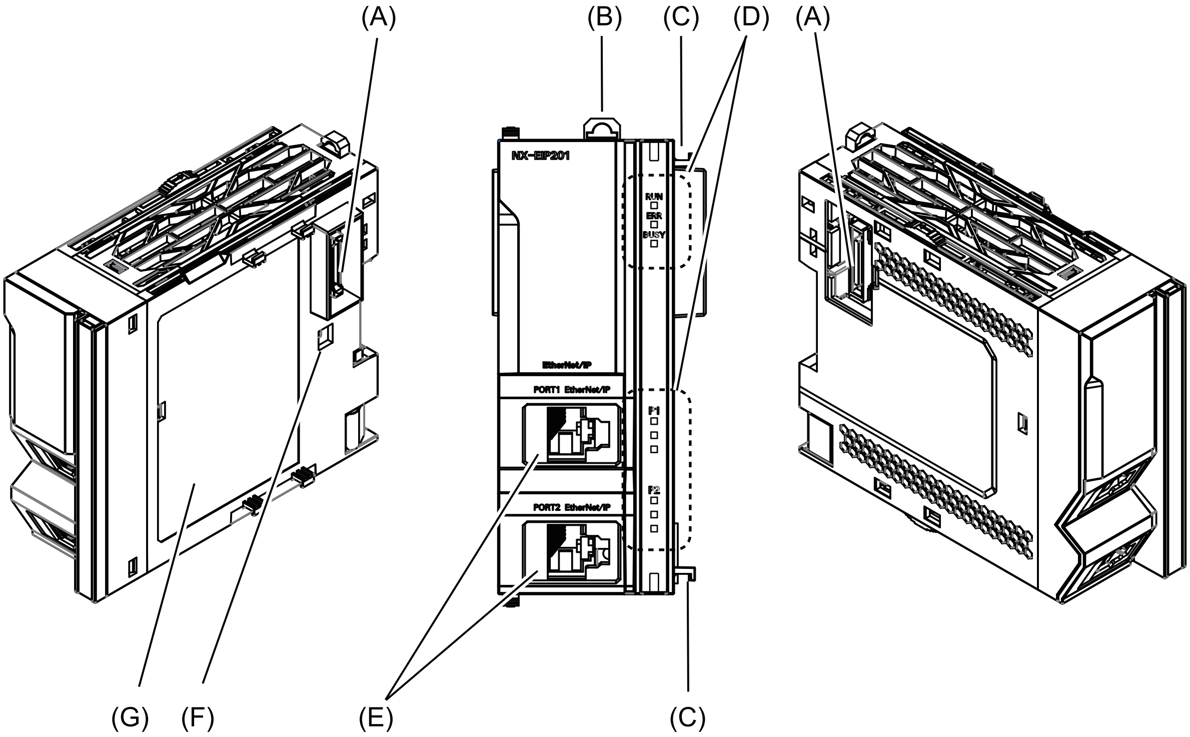
3

Part Names and Functions

This section describes part names and functions of the NX-series EtherNet/IP Unit.

3-1 Part Names

The following table gives the name of each part of the NX-series EtherNet/IP Unit.



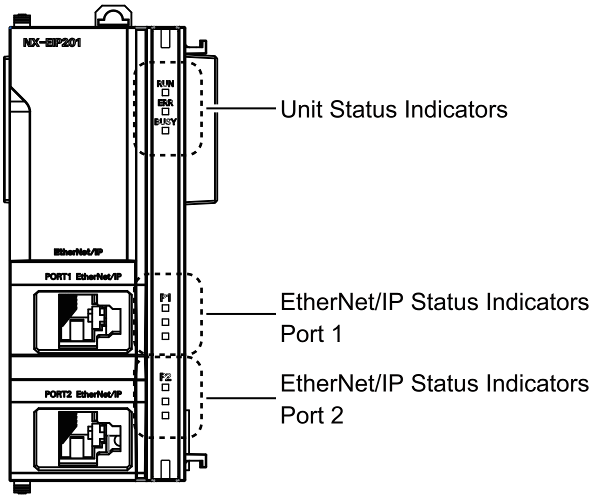
Symbol	Name	Function
A	X Bus connectors	These connectors are used to connect another Unit.
B	DIN Track mounting hook	This hook is used to mount the Unit to a DIN Track.
C	Unit hookup guides	These guides are used to connect two Units.
D	Operation status indicators	The indicators show the current operating status of the Unit.
E	EtherNet/IP ports	The communications ports for EtherNet/IP connection. There are two ports.
F	DIP switch	This switch is for configuring internal settings of the Unit, but not used normally. Always keep all pins from SW1 to SW4 in OFF state.
G	Unit specifications	The specifications of the Unit are given here.

3-2 Part Functions

3-2-1 Operation Status Indicators

The operation status indicators include the Unit status indicators which display the operating status of the NX-series EtherNet/IP Unit and the EtherNet/IP (Port 1/Port 2) status indicators which display the status of EtherNet/IP ports.

The specifications of both instructions are given in the following table.



Unit Status Indicators

Indicator	Color	Indicator status	Status of NX-series EtherNet/IP Unit
RUN	Green	Lit	Power is ON.
		Flashing	A System Initialization Error occurred.
		Not lit	Power is OFF, or a Power Supply Error, a Hardware Initialization Error, an X Bus Unit Hardware Error, or an error for which the user cannot recover operation occurred in the Unit.
ERR	Red	Lit	An error for which the user cannot recover operation occurred in the Unit.
		Flashing	An error for which the user can recover operation occurred in the Unit.
		Not lit	An error not occurred in the Unit.
BUSY	Yellow	Flashing	Built-in non-volatile memory access in progress.
		Not lit	Other than the above.

EtherNet/IP (Port 1/Port 2) Status Indicators

Indicator	Color	Indicator status	Status of EtherNet/IP port
NET RUN	Green	Lit	Normal
		Flashing	Ethernet communications are in progress.
		Not lit	Ethernet communications are not possible.

Indicator	Color	Indicator status	Status of EtherNet/IP port
NET ERR	Red	Lit	An error for which the user cannot recover operation occurred.
		Flashing	An error for which the user can recover operation occurred.
		Not lit	There are no Ethernet communications errors. • The power supply is OFF or the Unit was reset.
LINK/ACT	Yellow	Lit	The link was established.
		Flashing	The link is established, and data communications are in progress.
		Not lit	A link was not established. • The cable is not connected. • The power supply is OFF or the Unit was reset.

3-2-2 DIP Switch

Do not use the DIP switch. Always keep all pins from SW1 to SW4 in OFF state.

4

Mounting

This section describes how to mount the NX-series EtherNet/IP Unit.

4-1 Mounting and Removing NX-series EtherNet/IP Units

Refer to *Mounting and Removing Units* in the *NX-series NX502 CPU Unit Hardware User's Manual (Cat. No. W629)* for how to mount and remove the NX-series EtherNet/IP Unit.

5

Installing Ethernet Networks

5-1 Selecting the Network Devices

5-1-1 Recommended Network Devices

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

● Ethernet Switches

Manufacturer	Model	Description
OMRON	W4S1-05D	Packet priority control (QoS): EtherNet/IP control data priority Ethernet standard: IEEE 802.3 10Base-T, 100Base-TX Auto-negotiation: Supported Broadcast storm control: Supported Number of ports: 5
Cisco Systems, Inc.	Consult the manufacturer. http://www.cisco.com/	
Contec USA, Inc.	Consult the manufacturer. http://www.contec.com/	
Phoenix Contact USA	Consult the manufacturer. https://www.phoenixcontact.com	

● Twisted-pair Cables and Connectors

Applicable EtherNet/IP communications cables and connectors vary depending on the used baud rate.
For 100Base-TX and 10Base-T, use an STP (shielded twisted-pair) cable of category 5 or higher. You can use either straight or cross cable.
For 1000Base-T, use an STP (shielded twisted-pair) cable (double shielding with aluminum tape and braiding) of category 5e or higher. You can use either straight or cross cable.
Cabling materials used for EtherNet/IP communication cables are shown in the table below.
"100Base-TX" in the "Product" column of the table below indicates that either 100Base-TX or 10Base-T can be used.

Product			Manufacturer	Model
For 1000Base-T and 100Base-TX	Size and conductor pairs: AWG24 × 4 pairs *1	Cable	Hitachi Metals, Ltd.	NETSTAR-C5E SAB 0.5 × 4P CP
			Kuramo Electric Co.	KETH-SB
			JMACS Japan Co., Ltd.	IETP-SB
		RJ45 Connectors	Panduit Corporation	MPS588
For 100Base-TX	Size and conductor pairs: AWG22 × 2 pairs*1	Cable	Kuramo Electric Co., Ltd.	KETH-PSB-OMR
			JMACS Japan Co., Ltd.	PNET/B
		RJ45 Assembly Connectors	OMRON	XS6G-T421-1

*1. We recommend that you use cables and connectors in above combinations.

5-1-2 Ethernet Switch Types

● Unmanaged Layer 2 (L2) Ethernet Switches

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

● Managed Layer 2 (L2) Ethernet Switches

These Ethernet switches use the Ethernet MAC address to switch ports. Ethernet switch functions and settings can be changed with special software tools for Ethernet switches running on a network node. You can also collect analytical data. These Ethernet switches provide more-advanced functions than unmanaged layer 2 Ethernet switches.

5-1-3 Ethernet Switch Functions

This section describes the Ethernet switch functions that are important for an EtherNet/IP network. For an EtherNet/IP port, consider whether the Ethernet switch supports the following two functions when you select the Ethernet switch.

- 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 Ethernet switch as IGMP snooping or GMRP.

"Specific nodes" are nodes equipped with an IGMP client, and have made transfer requests to the Ethernet switch. (OMRON EtherNet/IP ports are equipped with an IGMP client.) When the Ethernet switch 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 Ethernet switch to enable this function. There must be enough multicast filters for the network.

● 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 specific 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.

Also, when tag data links and CIP Safety communications are executed on the same network, it is possible to reduce the impact of tag data link traffic by increasing the priority of CIP Safety communications with QoS settings.

Refer to *7-5* ***CIP Settings*** *Display* on page 7-15 for details on the QoS settings.

Settings must be made in the Ethernet switch to enable QoS function and give higher priority to tag data link packets.

These functions are supported by Ethernet switches as described in the table below.

Ethernet switch type	Multicast filtering	L4 QoS	Remarks
Unmanaged L2 Ethernet switch	Not supported	Not supported	---
Managed L2 Ethernet switch	Supported	Supported	Both functions must be set with a special software tool.
OMRON Ethernet switch (W4S1-series Ethernet switches)	Not supported	Supported	L4 QoS is set with a switch. No software tool is necessary. [*1]

[*1] Even QoS settings are made, tag data links and CIP Safety communications are processed with the same priority.

Additional Information

- If you select **Multi-cast Connection** for the connection type in the connection settings on the Network Configurator, multicast packets are used. If the connection type is set to a **Point to Point Connection**, multicast packets are not used.

5-1-4 Precautions for Ethernet Switch Selection

The functions supported by the Ethernet switch may affect tag data link transmission delays and the settings in the Controller configurations and setup.
In addition, if the Ethernet switch supports advanced functions, special settings are required for the functions.
When you select an Ethernet switch, it is necessary to consider what kind of data transmission and how much traffic you use over the the network.
Refer to the following precautions when you select an Ethernet switch.
Refer to *12-2 Adjusting the Communications Load* on page 12-7 to estimate the communications load for tag data links.

Selecting the Ethernet Switch Based on the Type of Network Communications

● Executing Tag Data Links Only

We recommend that you use an L2 Ethernet switch without multicast filtering or an L2 Ethernet switch with multicast filtering.
An L2 Ethernet switch 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, there is no difference in the traffic condition whether multicast filtering is supported or not.

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

When multicast filtering is used, settings must be made accordingly on the Ethernet switch. There must be enough multicast filters for the network.

● Executing Tag Data Links and Message Communications

We recommend an L2 Ethernet switch with multicast filtering and L4 QoS.

If you set 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.

Refer to *7-5* ***CIP Settings*** *Display* on page 7-15 for details on the QoS settings.

When multicast filtering and L4 QoS are used, settings must be made accordingly on the Ethernet switch.

● Executing Tag Data Links and CIP Safety Communications

We recommend an L2 Ethernet switch with multicast filtering and L4 QoS.

If you set CIP Safety packets for higher-priority transmission, it is possible to reduce the impact from problems such as transmission delays due to tag data link communications traffic and packet losses due to buffer overflow.

When L4 QoS is used, settings must be made accordingly in the QoS configuration on the Sysmac Studio and on the Ethernet switch. Refer to *7-5* ***CIP Settings*** *Display* on page 7-15 for details on configuring QoS on the Sysmac Studio.

Selecting the Ethernet Switch Based on the Ethernet Switch's Supported Functions

● L2 Ethernet Switch without Multicast Filtering

We recommend this kind of Ethernet switch 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. (Multicast packets are transferred to all nodes in the network, just like broadcast transmission.)
- The tag data link settings are all one-to-one (unicast) and multicast packets are not used.
- There is little traffic in the tag data links.

No special settings are required for an L2 Ethernet switch without multicast filtering.

● L2 Ethernet Switch with Multicast Filtering

We recommend this kind of Ethernet switch 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.

Specific settings are required for an L2 Ethernet switch with multicast filtering. There must be enough multicast filters for the network.

● L3 Ethernet Switch with Multicast Filtering and L4 QoS Functions

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

If you set tag data links for higher-priority transmission, you can prevent problems such as transmission delays due to message communications traffic and packet losses due to buffer overflow.

When multicast filtering and L4 QoS are used, settings must be made accordingly on the Ethernet switch. There must be enough multicast filters for the network.

Selecting the Ethernet Switch Based on the Network Communication Speed

● Executing Tag Data Links at a Baud Rate Over 100 Mbps

If you use data tag links with the following conditions, use an Ethernet switch with multicast filtering or an Ethernet switch that supports a baud rate of 1,000 Mbps.

- Multicast
- Baud rate over 100 Mbps

If there is an Ethernet device on the same network that communicates at a speed of 100 Mbps or less, the device may affect tag data link communications and cause tag data links to be broken, even if the device is not related to tag data link communications.

Precautions for Correct Use

- Ask the Ethernet switch manufacturer for setting procedures for the Ethernet switch.
- Install the Ethernet switch based on its environmental resistance specifications so that the environmental resistance specifications are fully met. Ask the Ethernet switch manufacturer for information on the environmental resistance of the Ethernet switch.

5-2 Network Installation

5-2-1 Basic Installation Precautions

- Take the greatest care when you install the Ethernet System. Be sure to follow ISO 8802-3 specifications. Be sure you understand them before attempting to install an Ethernet System.
- Unless you are already experienced in installation of 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 installation of network components in metal cases or the use of optical cable in the system.
- When using a shielded cable with the shields on both ends of the cable connected to connector hoods, ground loops induced by improper grounding methods may decrease noise immunity and cause device damage. To prevent ground loops caused by differences in potential between device grounding points, the reference potential between the devices must be stabilized. Design grounding appropriately so that noise current does not flow to ground lines between the devices.
  For grounding methods, refer to the *NX-series NX502 CPU Unit Hardware User's Manual (Cat. No. W629)*.
- To obtain information on installing EtherNet/IP cable, contact ODVA.
  ODVA web site: http://www.odva.org
- When you install an EtherNet/IP network that combines an information network with the control system, and the communications load may be heavy due to tag data links, we recommend that you set up a network where the load does not affect communications. For example, install the tag data links in a segment that is separate from the information network.

5-2-2 Recommended Network Devices

Refer to *5-1 Selecting the Network Devices* on page 5-2 for the devices recommended for use with the EtherNet/IP port.

5-2-3 Precautions When Laying Twisted-pair Cable

Connecting the Shield to Connector Hoods

● Between an EtherNet/IP Port and an Ethernet Switch

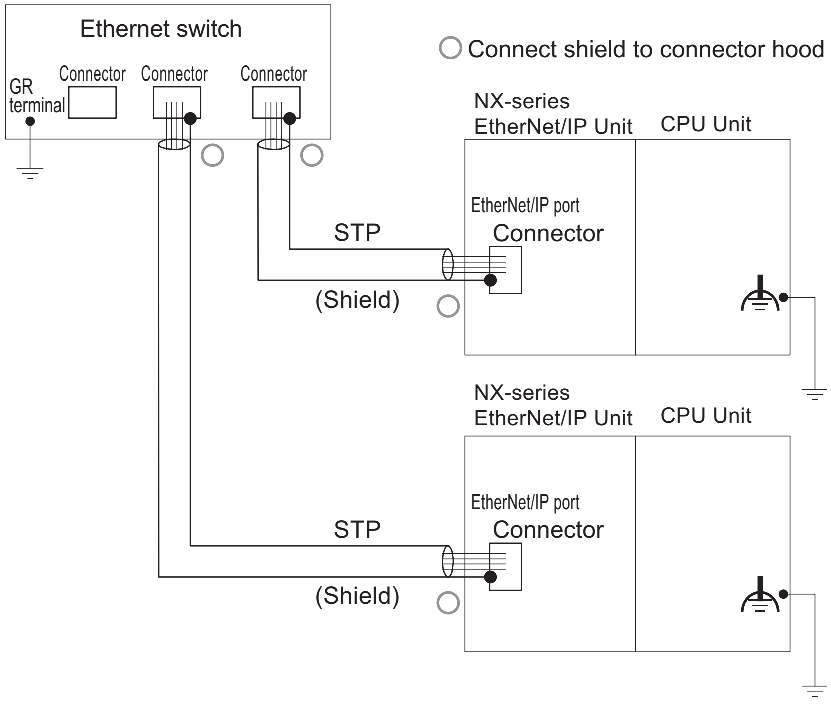
Connect the shield to connector hoods as described below.

Communications standard	Connection
10Base-T	• Connect the shield at both ends or • Connect the shield only at the Ethernet switch side. A clamp core must be attached to the EtherNet/IP port side of the cable.
100Base-TX	
1000Base-T	Connect the shield at both ends

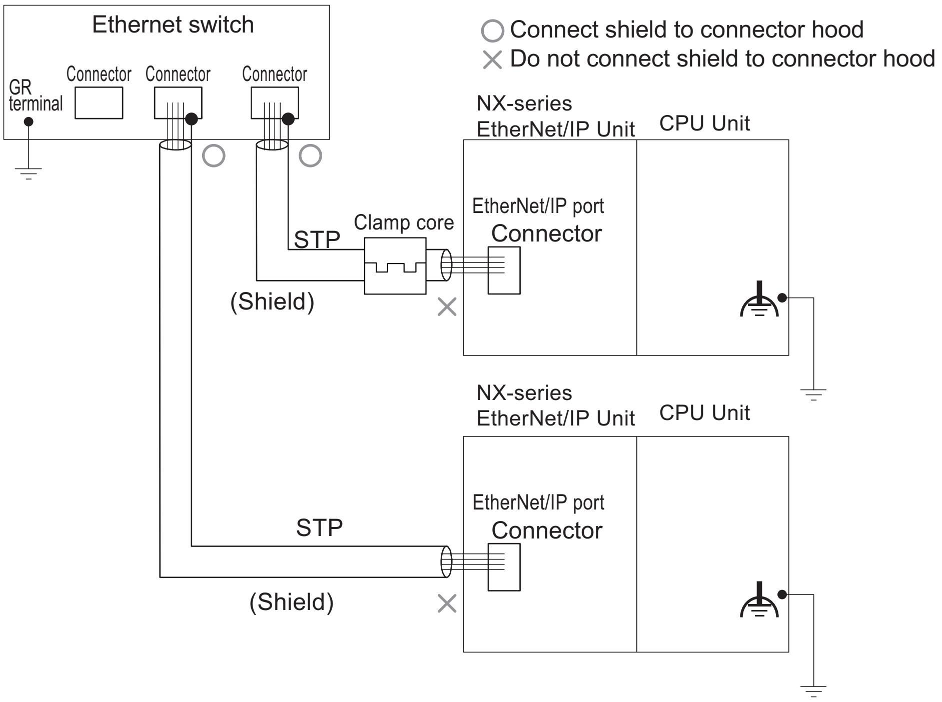
- 10Base-T or 100Base-TX

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.
   A clamp core must be attached to the end of the cable at the EtherNet/IP port side. For a recommended clamp core and attachment methods, refer to *Recommended Clamp Core and Attachment Method* on page 5-10.
   To comply with EMC standards, it is mandatory that a clamp core be attached when connecting the shield to the connector hood only at the Ethernet switch side.



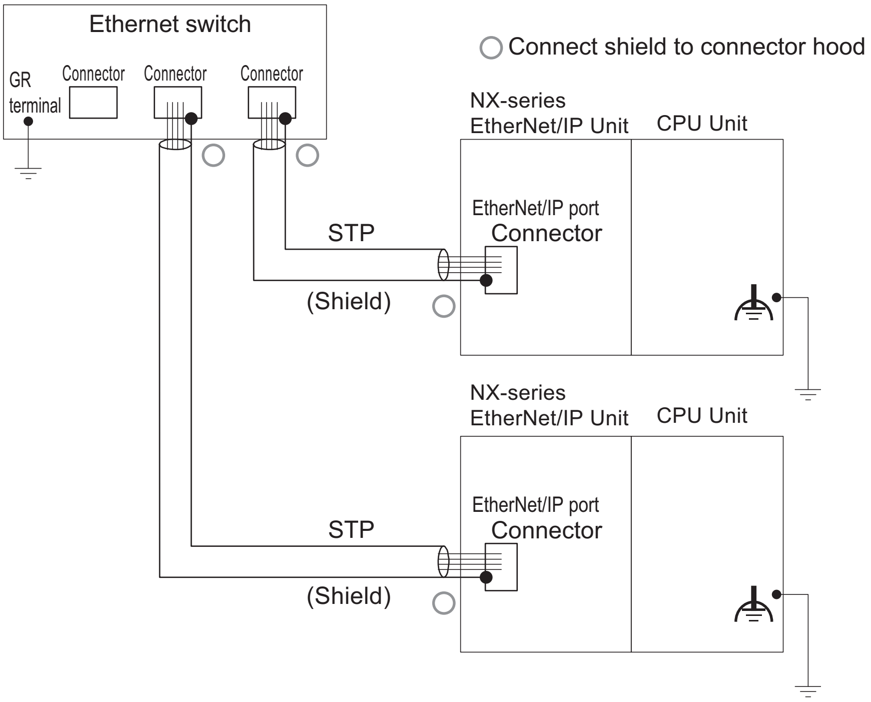
Additional Information

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.
When using a baud rate of 100 Mbps or less, it may be possible to alleviate this problem by connecting the shield only at the Ethernet switch side as described in (2), rather than connecting both ends as described in (1).

- 1000Base-T

  Connect the shields to respective connector hoods at both ends of the cables.

  This connection is required for 1000Base-T to ensure compliance with EMC standards.


Ethernet switch
GR terminal
Connector
Connector
Connector
○ Connect shield to connector hood
NX-series EtherNet/IP Unit
CPU Unit
EtherNet/IP port Connector
STP
(Shield)
NX-series EtherNet/IP Unit
CPU Unit
EtherNet/IP port Connector
STP
(Shield)

● 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.

Other Precautions When Laying the Twisted-pair Cable

- Firmly insert the connector until it locks into place when you connect the cable to the Ethernet switch and the EtherNet/IP port.
- Do not install the twisted-pair cable together with high-voltage lines.
- Do not install the twisted-pair cable near devices that generate noise.
- Do not install the twisted-pair cable in locations subject to high temperatures or high humidity.
- Do not install the twisted-pair cable in locations subject to excessive dirt, dust, oil mist or other contaminants.

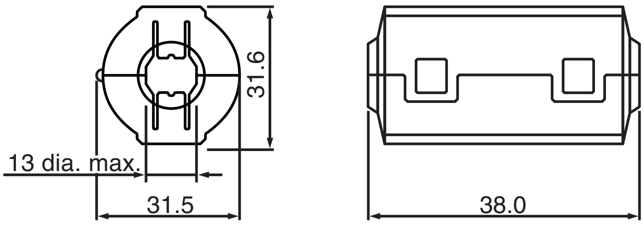
Recommended Clamp Core and Attachment Method

When you connect the cable shield only with the connector hood of the Ethernet switch, you need to attach a clamp core to the EtherNet/IP port.
The recommended clamp core and attachment method are given below.

● Recommended Clamp Core

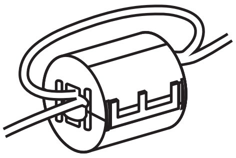
Manufacturer	Product	Model
NEC TOKIN	Clamp core	ESD-SR-250

ESD-SR-250 dimensions



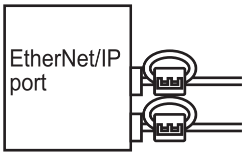
● Recommended Attachment Method

- Attach a clamp core to the communications cable as shown below.



Make two loops with the cable as shown.

- Connect the communications cable as shown below.



Attach close to the cable connection as shown.

5-2-4 Precautions When Installing and Connecting Ethernet Switches

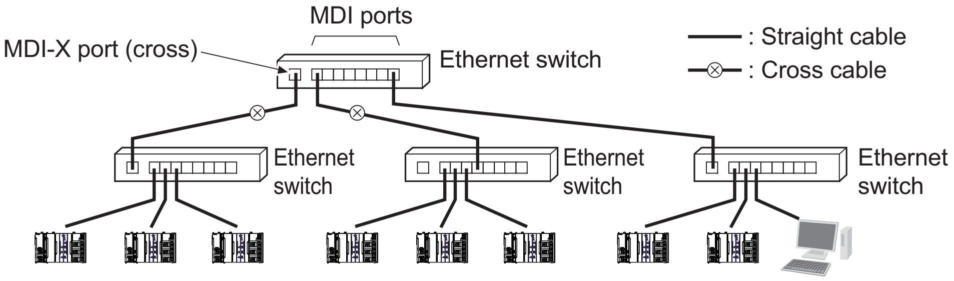
Precautions When Installing Ethernet Switches

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

Ethernet Switch Connection Methods

- Connect Ethernet switches with twisted-pair cables, as follows: Connect an MDI port to an MDI-X port with a straight cable. Connect two MDI ports or 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 cascade connections with straight cables wherever possible.



- Some Ethernet switches can automatically distinguish between MDI and MDI-X. When this kind of Ethernet switch is used, straight cable can be used between Ethernet switches.

Precautions for Correct Use

EtherNet/IP port link settings is fixed as the auto negotiation. The following table shows the connection for communications mode of the Ethernet switch.
(Auto-Nego: Auto negotiation, Full: Full duplex, Half: Half duplex)

Communications mode of the Ethernet switch		Connection
Auto-Nego		Best
10 Mbps (fixed)	Full	---
	Half	OK
100 Mbps (fixed)	Full	---
	Half	OK
1,000 Mbps (fixed)	Full	---

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

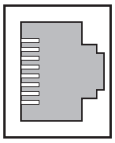
5-3 Connecting to the Network

5-3-1 Ethernet Connectors

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

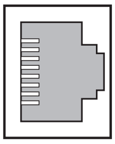
- Electrical specifications: Conforming to IEEE 802.3 standards.
- Connector structure: RJ45 8-pin Modular Connector (conforming to ISO 8877)
- For information on connecting shield wire to connector hoods, refer to *5-1-2 Ethernet Switch Types* on page 5-3.

10Base-T and 100Base-TX



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	---	---

1000Base-T



Connector pin	Signal name	Abbr.	Signal direction
1	Communication data DA+	BI_DA+	Input/output
2	Communication data DA−	BI_DA-	Input/output
3	Communication data DB+	BI_DB+	Input/output
4	Communication data DC+	BI_DC+	Input/output
5	Communication data DC−	BI_DC−	Input/output
6	Communication data DB−	BI_DB−	Input/output
7	Communication data DD+	BI_DD+	Input/output
8	Communication data DD−	BI_DD−	Input/output

5-3-2 Connecting the Cable

Precautions for Correct Use

- Turn OFF the Controller's power supply before connecting or disconnecting Ethernet communications cable.
- Allow extra space for the bending radius of the communications cable.
  For the dimensions when the communications cable is connected to the Unit, refer to *Installation Height* on page A-3. The required space depends on the communications cable and connector that are used. Consult the manufacturer or sales agent.

1 Install the twisted-pair cable.

2 Connect the cable to the Ethernet switch.

3 Connect the twisted-pair cable to the connector on the EtherNet/IP port.
Be sure to press the connectors (both the Ethernet switch side and Ethernet side) until they lock into place.

6

Device Variables Related to the NX-series EtherNet/IP Unit

6-1 What You Can Check with Device Variables

You can use the device variables that are provided for the NX-series EtherNet/IP Unit in the user program to check errors that occur in the NX-series EtherNet/IP Unit and the status of the NX-series EtherNet/IP Unit.

Additional Information

This section describes only the device variables that are used to check the errors and status which are unique to the NX-series EtherNet/IP Unit. Refer to *Specifications for Individual Device Variables* in the *NJ/NX-series CPU Unit Software User's Manual (Cat. No. W501)* for information on the device variables that are used to check the errors and status of the X Bus Unit Common Function Module.

6-1-1 Checking for Errors in the NX-series EtherNet/IP Unit

You can check for a Communications Port Error and a CIP Communications Error that occur in the NX-series EtherNet/IP Unit.

The device variables related to errors have a hierarchical structure combined with the system-defined variables as shown in the following table. The system gives the error status at each level by logically ORing the error status information in the lower level. For example, the value of *ETN_ErrSta* in Level 5 changes to TRUE when the value of any of the following five device variables in the lower level is TRUE.

- *ETN_Port1Status.PortErr*
- *ETN_Port2Status.PortErr*
- *ETN_TcpAppCfgErr*
- *ETN_IPRTblErr*
- *ETN_DNSCfgErr*

From Level 1 to Level 4 are the system-defined variables. Refer to the *NJ/NX-series CPU Unit Software User's Manual (Cat. No. W501)* for details on the specifications of these system-defined variables.

System-defined variables from Level 1 to Level 4

Level 1		Level 2		Level 3		Level 4	
Variable	Name	Variable	Name	Variable	Name	Variable	Name
_ErrSta	Controller Error Status	_PLC_ErrSta	PLC Function Module Error Status	The rest of levels are omitted.			
		_EIP_ErrSta	EtherNet/IP Error	The rest of levels are omitted.			
		_NXB_ErrSta	NX Bus Function Module Error Status	The rest of levels are omitted.			
		_XBU_ErrSta	X Bus Function Module Error Status	_XBU_MstrErr	X Bus Function Module Master Error Status	The rest of levels are omitted.	
				_XBU_UnitErr	X Bus Function Module Unit Error Status	_XBU_UnitErrTbl	X Bus Function Module Unit Error Status Table

Device variables in levels lower than Level 4*_XBU_UnitErrTbl*

Level 5		Level 6		Level 7	
Variable	Name	Variable	Name	Variable	Name
ETN_ErrSta	Communications Port Error	ETN_Port1Status.PortErr	Communications Port1 Error	ETN_Port1Status.MacAdrErr	Port1 MAC Address Error
				ETN_Port1Status.LanHwErr	Port1 Communications Controller Error
				ETN_Port1Status.EtnCfgErr	Port1 Basic Ethernet Setting Error
				ETN_Port1Status.IPAdrCfgErr	Port1 IP Address Setting Error
				ETN_Port1Status.IPAdrDupErr	Port1 IP Address Duplication Error
				ETN_Port1Status.BootpErr	Port1 BOOTP Server Error
		ETN_Port2Status.PortErr	Communications Port2 Error	ETN_Port2Status.MacAdrErr	Port2 MAC Address Error
				ETN_Port2Status.LanHwErr	Port2 Communications Controller Error
				ETN_Port2Status.EtnCfgErr	Port2 Basic Ethernet Setting Error
				ETN_Port2Status.IPAdrCfgErr	Port2 IP Address Setting Error
				ETN_Port2Status.IPAdrDupErr	Port2 IP Address Duplication Error
				ETN_Port2Status.BootpErr	Port2 BOOTP Server Error
				ETN_TcpAppCfgErr	TCP Application Setting Error
				ETN_IPRTblErr	IP Router Table Setting Error
				ETN_DNSCfgErr	DNS Setting Error

Level 5		Level 6		Level 7	
Variable	Name	Variable	Name	Variable	Name
EIP_ErrSta	CIP Communications Error	EIP_Comm1Status.CipErr	CIP Communications1 Error	EIP_Comm1Status.IdentityErr	CIP Communications1 Identity Error
				EIP_Comm1Status.TDLinkCfgErr	CIP Communications1 Tag Data Link Setting Error
				EIP_Comm1Status.TDLinkOpnErr	CIP Communications1 Tag Data Link Connection Failed
				EIP_Comm1Status.TDLinkErr	CIP Communications1 Tag Data Link Communications Error
				EIP_Comm1Status.TagAdrErr	CIP Communications1 Tag Name Resolution Error
		EIP_Comm2Status.CipErr	CIP Communications2 Error	EIP_Comm2Status.IdentityErr	CIP Communications2 Identity Error
				EIP_Comm2Status.TDLinkCfgErr	CIP Communications2 Tag Data Link Setting Error
				EIP_Comm2Status.TDLinkOpnErr	CIP Communications2 Tag Data Link Connection Failed
				EIP_Comm2Status.TDLinkErr	CIP Communications2 Tag Data Link Communications Error
				EIP_Comm2Status.TagAdrErr	CIP Communications2 Tag Name Resolution Error
XBU_ErrSta[*1]	X Bus Unit Common Function Module Error Status	The rest of levels are omitted.			

[*1] Refer to *Specifications for Individual Device Variables* in the *NJ/NX-series CPU Unit Software User’s Manual (Cat. No. W501)* for details of specifications.

6-1-2 Checking for Status of the NX-series EtherNet/IP Unit

You can check the status of the NX-series EtherNet/IP Unit such as if the EtherNet/IP port is available for use, or CIP communications are operating properly.

6-2 Device Variables

The variables are described in the tables as shown below.

Variable name	Meaning	Function	Data type	Range of values	Reference
This is the device variable name. The prefix gives the category name.	This is the meaning of the variable.	The function of the variable is described.	The data type of the variable is given.	The range of values that the variable can take is given.	The page of the individual device variable specifications table is given.

● Functional Classification: NX-series EtherNet/IP Unit Errors

Variable name	Meaning	Function	Data type	Range of values	Reference
ETN_ErrSta	Communications Port Error	This is the error status variable for the communications port. Represents the collective status of the following error flags. [*1] • ETN_Port1Status.PortErr (Communications Port1 Error) • ETN_Port2Status.PortErr (Communications Port2 Error) • ETN_TcpAppCfgErr (TCP Application Setting Error) • ETN_DNSCfgErr (DNS Setting Error) • ETN_IPRTblErr (IP Router Table Setting Error)	WORD	16#0000 to 16#00F0	page 6-16
ETN_Port1Status.PortErr	Communications Port1 Error	This is the error status variable for the communications port 1. Represents the collective status of the following error flags. [*1] • ETN_Port1Status.MacAdrErr (Port1 MAC Address Error) • ETN_Port1Status.LanHwErr (Port1 Communications Controller Error) • ETN_Port1Status.EtnCfgErr (Port1 Basic Ethernet Setting Error) • ETN_Port1Status.IPAdrCfgErr (Port1 IP Address Setting Error) • ETN_Port1Status.IPAdrDupErr (Port1 IP Address Duplication Error) • ETN_Port1Status.BootpErr (Port1 BOOTP Server Error) **Note** If a *Link OFF Detected* occurs, it is recorded in the event log and then the corresponding bit turns ON.	WORD	16#0000 to 16#00F0	page 6-17

Variable name	Meaning	Function	Data type	Range of values	Reference
ETN_Port2Status.PortErr	Communications Port2 Error	This is the error status variable for the communications port 2. Represents the collective status of the following error flags. *1 • ETN_Port2Status.MacAdrErr (Port2 MAC Address Error) • ETN_Port2Status.LanHwErr (Port2 Communications Controller Error) • ETN_Port2Status.EtnCfgErr (Port2 Basic Ethernet Setting Error) • ETN_Port2Status.IPAdrCfgErr (Port2 IP Address Setting Error) • ETN_Port2Status.IPAdrDupErr (Port2 IP Address Duplication Error) • ETN_Port2Status.BootpErr (Port2 BOOTP Server Error) **Note** If a *Link OFF Detected* occurs, it is recorded in the event log and then the corresponding bit turns ON.	WORD	16#0000 to 16#00F0	page 6-17
ETN_Port1Status.MacAdrErr	Port1 MAC Address Error	Indicates that an error occurred when the MAC address was read on the communications port 1 at startup. TRUE: Error FALSE: Normal	BOOL	TRUE or FALSE	page 6-17
ETN_Port2Status.MacAdrErr	Port2 MAC Address Error	Indicates that an error occurred when the MAC address was read on the communications port 2 at startup. TRUE: Error FALSE: Normal	BOOL	TRUE or FALSE	page 6-18
ETN_Port1Status.LanHwErr	Port1 Communications Controller Error	Indicates that a Communications Controller failure occurred on the communications port 1. TRUE: Failure FALSE: Normal	BOOL	TRUE or FALSE	page 6-18
ETN_Port2Status.LanHwErr	Port2 Communications Controller Error	Indicates that a Communications Controller failure occurred on the communications port 2. TRUE: Failure FALSE: Normal	BOOL	TRUE or FALSE	page 6-18
ETN_Port1Status.EtnCfgErr	Port1 Basic Ethernet Setting Error	Indicates that the Ethernet communications speed setting (Speed/Duplex) for the communications port 1 is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page 6-18
ETN_Port2Status.EtnCfgErr	Port2 Basic Ethernet Setting Error	Indicates that the Ethernet communications speed setting (Speed/Duplex) for the communications port 2 is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page 6-18

Variable name	Meaning	Function	Data type	Range of values	Reference
ETN_Port1Status.IPAdrCfgErr	Port1 IP Address Setting Error	Indicates the IP address setting errors for the communications port 1. TRUE: • There is an illegal IP address setting. • A read operation failed. • The IP address obtained from the BOOTP server is inconsistent. FALSE: Normal	BOOL	TRUE or FALSE	page 6-19
ETN_Port2Status.IPAdrCfgErr	Port2 IP Address Setting Error	Indicates the IP address setting errors for the communications port 2. TRUE: • There is an illegal IP address setting. • A read operation failed. • The IP address obtained from the BOOTP server is inconsistent. FALSE: Normal	BOOL	TRUE or FALSE	page 6-19
ETN_Port1Status.IPAdrDupErr	Port1 IP Address Duplication Error	Indicates that the same IP address is assigned to more than one node for the communications port 1. TRUE: Duplication occurred. FALSE: Other than the above.	BOOL	TRUE or FALSE	page 6-19
ETN_Port2Status.IPAdrDupErr	Port2 IP Address Duplication Error	Indicates that the same IP address is assigned to more than one node for the communications port 2. TRUE: Duplication occurred. FALSE: Other than the above.	BOOL	TRUE or FALSE	page 6-19
ETN_Port1Status.BootpErr	Port1 BOOTP Server Error	Indicates that a BOOTP server connection failure occurred on the communications port 1. TRUE: There was a failure to connect to the BOOTP server (timeout). FALSE: The BOOTP is not enabled, or BOOTP is enabled and an IP address was normally obtained from the BOOTP server.	BOOL	TRUE or FALSE	page 6-20
ETN_Port2Status.BootpErr	Port2 BOOTP Server Error	Indicates that a BOOTP server connection failure occurred on the communications port 2. TRUE: There was a failure to connect to the BOOTP server (timeout). FALSE: The BOOTP is not enabled, or BOOTP is enabled and an IP address was normally obtained from the BOOTP server.	BOOL	TRUE or FALSE	page 6-20
ETN_TcpAppCfgErr	TCP Application Setting Error	TRUE: At least one of the set values for a TCP application is incorrect. Or, a read operation failed. FALSE: Normal	BOOL	TRUE or FALSE	page 6-20
ETN_IPRTblErr	IP Router Table Setting Error	Indicates that the default gateway settings or IP router table settings are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page 6-20
ETN_DNSCfgErr	DNS Setting Error	Indicates that the DNS or hosts settings are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page 6-20

Variable name	Meaning	Function	Data type	Range of values	Reference
EIP_ErrSta	CIP Communications Error	This is the error status variable for CIP communications. Represents the collective status of the following error flags. [*1] • EIP_Comm1Status.CipErr (CIP Communications1 Error) • EIP_Comm2Status.CipErr (CIP Communications2 Error)	WORD	16#0000 to 16#00F0	page 6-21
EIP_Comm1Status.CipErr	CIP Communications1 Error	This is the error status variable for CIP communications on the communications port 1. Represents the collective status of the following error flags. [*1] • EIP_Comm1Status.IdentityErr (CIP Communications1 Identity Error) • EIP_Comm1Status.TDLinkCfgErr (CIP Communications1 Tag Data Link Setting Error) • EIP_Comm1Status.TDLinkOpnErr (CIP Communications1 Tag Data Link Connection Failed) • EIP_Comm1Status.TDLinkErr (CIP Communications1 Tag Data Link Communications Error) • EIP_Comm1Status.TagAdrErr (CIP Communications1 Tag Name Resolution Error)	WORD	16#0000 to 16#00F0	page 6-21
EIP_Comm2Status.CipErr	CIP Communications2 Error	This is the error status variable for CIP communications on the communications port 2. Represents the collective status of the following error flags. [*1] • EIP_Comm2Status.IdentityErr (CIP Communications2 Identity Error) • EIP_Comm2Status.TDLinkCfgErr (CIP Communications2 Tag Data Link Setting Error) • EIP_Comm2Status.TDLinkOpnErr (CIP Communications2 Tag Data Link Connection Failed) • EIP_Comm2Status.TDLinkErr (CIP Communications2 Tag Data Link Communications Error) • EIP_Comm2Status.TagAdrErr (CIP Communications2 Tag Name Resolution Error)	WORD	16#0000 to 16#00F0	page 6-21
EIP_Comm1Status.IdentityErr	CIP Communications1 Identity Error	Indicates that the identity information for CIP communications 1 (which you cannot overwrite) is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page 6-21

Variable name	Meaning	Function	Data type	Range of values	Reference
EIP_Comm2Status.IdentityErr	CIP Communications2 Identity Error	Indicates that the identity information for CIP communications 2 (which you cannot overwrite) is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page 6-22
EIP_Comm1Status.TDLinkCfgErr	CIP Communications1 Tag Data Link Setting Error	Indicates that the tag data link settings for CIP communications 1 are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page 6-22
EIP_Comm2Status.TDLinkCfgErr	CIP Communications2 Tag Data Link Setting Error	Indicates that the tag data link setting for CIP communications 2 are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page 6-22
EIP_Comm1Status.TDLinkOpnErr	CIP Communications1 Tag Data Link Connection Failed	Indicates that establishing a tag data link connection for CIP communications 1 failed. TRUE: Establishing a tag data link connection failed due to one of the following causes. • The information registered for a target node in the tag data link parameters is different from the actual node information. • There was no response from the remote node. FALSE: Other than the above.	BOOL	TRUE or FALSE	page 6-22
EIP_Comm2Status.TDLinkOpnErr	CIP Communications2 Tag Data Link Connection Failed	Indicates that establishing a tag data link connection for CIP communications 2 failed. TRUE: Establishing a tag data link connection failed due to one of the following causes. • The information registered for a target node in the tag data link parameters is different from the actual node information. • There was no response from the remote node. FALSE: Other than the above.	BOOL	TRUE or FALSE	page 6-23
EIP_Comm1Status.TDLinkErr	CIP Communications1 Tag Data Link Communications Error	Indicates that a timeout occurred in a tag data link connection for CIP communications 1. TRUE: A timeout occurred. FALSE: Other than the above.	BOOL	TRUE or FALSE	page 6-23
EIP_Comm2Status.TDLinkErr	CIP Communications2 Tag Data Link Communications Error	Indicates that a timeout occurred in a tag data link connection for CIP communications 2. TRUE: A timeout occurred. FALSE: Other than the above.	BOOL	TRUE or FALSE	page 6-23

Variable name	Meaning	Function	Data type	Range of values	Reference
EIP_Comm1Status.TagAdrErr	CIP Communications1 Tag Name Resolution Error	Indicates that the tag resolution for CIP communications 1 failed (i.e., the address could not be identified from the tag name). TRUE: Tag resolution failed (i.e., the address could not be identified from the tag name). The following causes are possible. • The size of the network variable is different from the tag settings. • The I/O direction that is set in the tag data link settings does not agree with the I/O direction of the variable in the NX-series EtherNet/IP Unit. • There is no network variable in the NX-series EtherNet/IP Unit that corresponds to the tag setting. FALSE: Other than the above.	BOOL	TRUE or FALSE	page 6-23
EIP_Comm2Status.TagAdrErr	CIP Communications2 Tag Name Resolution Error	Indicates that the tag resolution for CIP communications 2 failed (i.e., the address could not be identified from the tag name). TRUE: Tag resolution failed (i.e., the address could not be identified from the tag name). The following causes are possible. • The size of the network variable is different from the tag settings. • The I/O direction that is set in the tag data link settings does not agree with the I/O direction of the variable in the NX-series EtherNet/IP Unit. • There is no network variable in the NX-series EtherNet/IP Unit that corresponds to the tag setting. FALSE: Other than the above.	BOOL	TRUE or FALSE	page 6-24

*1. Refer to *Meanings of Error Status Bits* on page 6-10 for the meanings of the error status bits.

● Meanings of Error Status Bits

The meanings of the individual bits in the following error status are the same.

- *ETN_ErrSta* (Communications Port Error)
- *EIP_ErrSta* (CIP Communications Error)
- *ETN_Port1Status.PortErr* (Communications Port1 Error)
- *ETN_Port2Status.PortErr* (Communications Port2 Error)
- *EIP_Comm1Status.CipErr* (CIP Communications1 Error)
- *EIP_Comm2Status.CipErr* (CIP Communications2 Error)

The meanings of the individual bits are shown in the following table.

Bit:	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
WORD	-	-	-	-	-	-	-	-	-	-			-	-	-	-

Bit	Description
15 to 6	Reserved.
5	This bit indicates whether a minor fault level Controller error has occurred. TRUE: A minor fault level Controller error has occurred. FALSE: A minor fault level Controller error has not occurred.
4	This bit indicates whether an observation level Controller error has occurred. TRUE: An observation level Controller error has occurred. FALSE: An observation level Controller error has not occurred.
3 to 0	Reserved.

● Functional Classification: NX-series EtherNet/IP Unit Status

Variable name	Meaning	Function	Data type	Range of values	Reference
ETN_Port1Status.EtnOnlineSta	Port1 Online	Indicates that the EtherNet/IP port's communications can be used via the communications port 1 (that is, the link is ON, IP address is defined, and there are no errors.) TRUE: The EtherNet/IP port's communications can be used. FALSE: The EtherNet/IP port's communications is disabled due to an error in initial processing, restart processing, or link OFF status.	BOOL	TRUE or FALSE	page 6-24
ETN_Port2Status.EtnOnlineSta	Port2 Online	Indicates that the EtherNet/IP port's communications can be used via the communications port 2 (that is, the link is ON, IP address is defined, and there are no errors.) TRUE: The EtherNet/IP port's communications can be used. FALSE: The EtherNet/IP port's communications is disabled due to an error in initial processing, restart processing, or link OFF status.	BOOL	TRUE or FALSE	page 6-24
EIP_Comm1Status.TDLinkRunSta	CIP Communications1 Tag Data Link Communications Status	Indicates that at least one connection is in normal operation in CIP communications 1. TRUE: Normal operation FALSE: Other than the above.	BOOL	TRUE or FALSE	page 6-24
EIP_Comm2Status.TDLinkRunSta	CIP Communications2 Tag Data Link Communications Status	Indicates that at least one connection is in normal operation in CIP communications 2. TRUE: Normal operation FALSE: Other than the above.	BOOL	TRUE or FALSE	page 6-25
EIP_Comm1Status.TDLinkAllRunSta	CIP Communications1 All Tag Data Link Communications Status	Indicates that all tag data links are communicating in CIP communications 1. TRUE: Tag data links are communicating in all connections as the originator. FALSE: An error occurred in at least one connection.	BOOL	TRUE or FALSE	page 6-25
EIP_Comm2Status.TDLinkAllRunSta	CIP Communications2 All Tag Data Link Communications Status	Indicates that all tag data links are communicating in CIP communications 2. TRUE: Tag data links are communicating in all connections as the originator. FALSE: An error occurred in at least one connection.	BOOL	TRUE or FALSE	page 6-25

Variable name	Meaning	Function	Data type	Range of values	Reference
EIP_Comm1Status.RegTargetSta[255]	CIP Communications1 Registered Target Node Information	Gives a list of nodes for which EtherNet/IP connections are registered for CIP communications 1. This variable is valid only when the EtherNet/IP port is the originator. Array[x] is TRUE: The connection to the node with a target node ID of x is registered. Array[x] is FALSE: The connection to the node with a target node ID of x is not registered.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page 6-25
EIP_Comm2Status.RegTargetSta[255]	CIP Communications2 Registered Target Node Information	Gives a list of nodes for which EtherNet/IP connections are registered for CIP communications 2. This variable is valid only when the EtherNet/IP port is the originator. Array[x] is TRUE: The connection to the node with a target node ID of x is registered. Array[x] is FALSE: The connection to the node with a target node ID of x is not registered.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page 6-26
EIP_Comm1Status.EstbTargetSta[255]	CIP Communications1 Normal Target Node Information	Gives a list of nodes that have normally established EtherNet/IP connections for CIP communications 1. Array[x] is TRUE: The connection to the node with a target node ID of x was established normally. Array[x] is FALSE: The connection to the node with a target node ID of x was not established, or an error occurred.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page 6-26
EIP_Comm2Status.EstbTargetSta[255]	CIP Communications2 Normal Target Node Information	Gives a list of nodes that have normally established EtherNet/IP connections for CIP communications 2. Array[x] is TRUE: The connection to the node with a target node ID of x was established normally. Array[x] is FALSE: The connection to the node with a target node ID of x was not established, or an error occurred.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page 6-26
EIP_Comm1Status.TargetPLCModeSta[255]	CIP Communications1 Target PLC Operating Mode	Shows the operating status of the target node Controllers that are connected for CIP communications 1, with the EtherNet/IP port as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. If the corresponding Normal Target Node Information is FALSE, it indicates the previous operating status. Array[x] is TRUE: This is the operating state of the target Controller with a node address of x. Array[x] is FALSE: Other than the above.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page 6-26

Variable name	Meaning	Function	Data type	Range of values	Reference
EIP_Comm2Status.TargetPLCModeSta[255]	CIP Communications2 Target PLC Operating Mode	Shows the operating status of the target node Controllers that are connected for CIP communications 2, with the EtherNet/IP port as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. If the corresponding Normal Target Node Information is FALSE, it indicates the previous operating status. Array[x] is TRUE: This is the operating state of the target Controller with a node address of x. Array[x] is FALSE: Other than the above.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page 6-27
EIP_Comm1Status.TargetPLCErr[255]	CIP Communications1 Target PLC Error Information	Shows the error status (logical OR of fatal and non-fatal errors) of the target node Controllers that are connected for CIP communications 1, with the EtherNet/IP ports as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. The immediately preceding value is retained if this variable is FALSE. Array[x] is TRUE: A fatal or non-fatal error occurred in the target Controller with a target node ID of x. Array[x] is FALSE: Other than the above.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page 6-27
EIP_Comm2Status.TargetPLCErr[255]	CIP Communications2 Target PLC Error Information	Shows the error status (logical OR of fatal and non-fatal errors) of the target node Controllers that are connected for CIP communications 2, with the EtherNet/IP ports as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. The immediately preceding value is retained if this variable is FALSE. Array[x] is TRUE: A fatal or non-fatal error occurred in the target Controller with a target node ID of x. Array[x] is FALSE: Other than the above.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page 6-27

Variable name	Meaning	Function	Data type	Range of values	Reference
EIP_Comm1Status.TargetNodeErr[255]	CIP Communications1 Target Node Error Information	Indicates that the connection for the Registered Target Node Information for CIP communications 1 was not established or that an error occurred in the target Controller. The array elements are valid only when the Registered Target Node Information is TRUE. Array[x] is TRUE: A connection was not normally established with the target node for a target node ID of x (the Registered Target Node Information is TRUE and the Normal Target Node Information is FALSE), or a connection was established with the target node but an error occurred in the target Controller. Array[x] is FALSE: The target node is not registered for a target node ID of x (the Registered Target Node Information is FALSE), or a connection was normally established with the target node (the Registered Target Node Information is TRUE and the Normal Target Node Information is TRUE). An error occurred in the target Controller (the Target PLC Error Information is TRUE).	ARRAY [0..255] OF BOOL	TRUE or FALSE	page 6-28
EIP_Comm2Status.TargetNodeErr[255]	CIP Communications2 Target Node Error Information	Indicates that the connection for the Registered Target Node Information for CIP communications 2 was not established or that an error occurred in the target Controller. The array elements are valid only when the Registered Target Node Information is TRUE. Array[x] is TRUE: A connection was not normally established with the target node for a target node ID of x (the Registered Target Node Information is TRUE and the Normal Target Node Information is FALSE), or a connection was established with the target node but an error occurred in the target Controller. Array[x] is FALSE: The target node is not registered for a target node ID of x (the Registered Target Node Information is FALSE), or a connection was normally established with the target node (the Registered Target Node Information is TRUE and the Normal Target Node Information is TRUE). An error occurred in the target Controller (the Target PLC Error Information is TRUE).	ARRAY [0..255] OF BOOL	TRUE or FALSE	page 6-28

Precautions for Correct Use

Communications Status with Target Node

The communications status of the communications port 1 of the NX-series EtherNet/IP Unit and the target node is shown by the combination of the values of the following four device variables.

- EIP_Comm1Status.RegTargetSta[255] (CIP Communications1 Registered Target Node Information)
- EIP_Comm1Status.EstbTargetSta[255] (CIP Communications1 Normal Target Node Information)
- EIP_Comm1Status.TargetPLCErr[255] (CIP Communications1 Target PLC Error Information)
- EIP_Comm1Status.TargetNodeErr[255] (CIP Communications1 Target Node Error Information)

Value of EIP_Comm1Status.RegTargetSta[255]	Value of EIP_Comm1Status.EstbTargetSta[255]	Value of EIP_Comm1Status.TargetPLCErr[255]	Value of EIP_Comm1Status.TargetNodeErr[255]	Communications status with target node
TRUE	TRUE	FALSE	FALSE	A connection with the target node was established normally and there is no error in the target PLC.
		TRUE	TRUE	A connection with the target node was established but there is an error in the target PLC.
	FALSE	---	TRUE	A connection with the target node was not established normally.
FALSE	---	---	---	The information is not valid because the target node is not registered.

The same applies for the case of communications port 2.

6-3 Specifications for Individual Device Variables

The specifications for each device variable are given as described below.

Variable name	This is the device variable name. The prefix gives the category name.			**Members**	The member names are given for structure variables.
Meaning	This is the meaning of the variable.			**Global/local**	Global: Global variable, Local: Local variable
Function	The function of the variable is described.				
Data type	The data type of the variable is given.			**Range of values**	The range of values that the variable can take is given.
R/W access	R: Read only, RW: Read/write	**Retained**	The Retain attribute of the variable is given.	**Network Publish**	The Network Publish attribute of the variable is given.
Usage in user program	Whether you can use the variable directly in the user program is specified.	**Related instructions**	The instructions that are related to the variable are given. If you cannot use the variable directly in the user program, the instructions that access the variable are given.		

● Functional Classification: NX-series EtherNet/IP Unit Errors

Variable name	ETN_ErrSta				
Meaning	Communications Port Error			**Global/local**	Global
Function	This is the error status variable for the communications port. It represents the collective status of the following error flags. • ETN_Port1Status.PortErr (Communications Port1 Error) • ETN_Port2Status.PortErr (Communications Port2 Error) • ETN_TcpAppCfgErr (TCP Application Setting Error) • ETN_DNSCfgErr (DNS Setting Error) • ETN_IPRTblErr (IP Router Table Setting Error) **Note** Refer to *Meanings of Error Status Bits* on page 6-10 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#00F0
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_Port1Status.PortErr				
Meaning	Communications Port1 Error			**Global/local**	Global
Function	This is the error status variable for the communications port 1. It represents the collective status of the following error flags. • ETN_Port1Status.MacAdrErr (Port1 MAC Address Error) • ETN_Port1Status.LanHwErr (Port1 Communications Controller Error) • ETN_Port1Status.EtnCfgErr (Port1 Basic Ethernet Setting Error) • ETN_Port1Status.IPAdrCfgErr (Port1 IP Address Setting Error) • ETN_Port1Status.IPAdrDupErr (Port1 IP Address Duplication Error) • ETN_Port1Status.BootpErr (Port1 BOOTP Server Error) **Note** If a *Link OFF Detected* occurs, it is recorded in the event log and then the corresponding bit turns ON. Refer to *Meanings of Error Status Bits* on page 6-10 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#00F0
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_Port2Status.PortErr				
Meaning	Communications Port2 Error			**Global/local**	Global
Function	This is the error status variable for the communications port 2. It represents the collective status of the following error flags. • ETN_Port2Status.MacAdrErr (Port2 MAC Address Error) • ETN_Port2Status.LanHwErr (Port2 Communications Controller Error) • ETN_Port2Status.EtnCfgErr (Port2 Basic Ethernet Setting Error) • ETN_Port2Status.IPAdrCfgErr (Port2 IP Address Setting Error) • ETN_Port2Status.IPAdrDupErr (Port2 IP Address Duplication Error) • ETN_Port2Status.BootpErr (Port2 BOOTP Server Error) **Note** If a *Link OFF Detected* occurs, it is recorded in the event log and then the corresponding bit turns ON. Refer to *Meanings of Error Status Bits* on page 6-10 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#00F0
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_Port1Status.MacAdrErr				
Meaning	Port1 MAC Address Error			**Global/local**	Global
Function	Indicates that an error occurred when the MAC address was read on the communications port 1 at startup. TRUE: Error FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_Port2Status.MacAdrErr				
Meaning	Port2 MAC Address Error			**Global/local**	Global
Function	Indicates that an error occurred when the MAC address was read on the communications port 2 at startup. TRUE: Error FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_Port1Status.LanHwErr				
Meaning	Port1 Communications Controller Error			**Global/local**	Global
Function	Indicates that a Communications Controller failure occurred on the communications port 1. TRUE: Failure FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_Port2Status.LanHwErr				
Meaning	Port2 Communications Controller Error			**Global/local**	Global
Function	Indicates that a Communications Controller failure occurred on the communications port 2. TRUE: Failure FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_Port1Status.EtnCfgErr				
Meaning	Port1 Basic Ethernet Setting Error			**Global/local**	Global
Function	Indicates that the Ethernet communications speed setting (Speed/Duplex) for the communications port 1 is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_Port2Status.EtnCfgErr				
Meaning	Port2 Basic Ethernet Setting Error			**Global/local**	Global
Function	Indicates that the Ethernet communications speed setting (Speed/Duplex) for the communications port 2 is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_Port1Status.IPAdrCfgErr				
Meaning	Port1 IP Address Setting Error			**Global/local**	Global
Function	Indicates the IP address setting errors for the communications port 1. TRUE: • There is an illegal IP address setting. • A read operation failed. • The IP address obtained from the BOOTP server is inconsistent. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_Port2Status.IPAdrCfgErr				
Meaning	Port2 IP Address Setting Error			**Global/local**	Global
Function	Indicates the IP address setting errors for the communications port 2. TRUE: • There is an illegal IP address setting. • A read operation failed. • The IP address obtained from the BOOTP server is inconsistent. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_Port1Status.IPAdrDupErr				
Meaning	Port1 IP Address Duplication Error			**Global/local**	Global
Function	Indicates that the same IP address is assigned to more than one node for the communications port 1. TRUE: Duplication occurred. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_Port2Status.IPAdrDupErr				
Meaning	Port2 IP Address Duplication Error			**Global/local**	Global
Function	Indicates that the same IP address is assigned to more than one node for the communications port 2. TRUE: Duplication occurred. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_Port1Status.BootpErr				
Meaning	Port1 BOOTP Server Error			**Global/local**	Global
Function	Indicates that a BOOTP server connection failure occurred on the communications port 1. TRUE: There was a failure to connect to the BOOTP server (timeout). FALSE: The BOOTP is not enabled, or BOOTP is enabled and an IP address was normally obtained from the BOOTP server.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_Port2Status.BootpErr				
Meaning	Port2 BOOTP Server Error			**Global/local**	Global
Function	Indicates that a BOOTP server connection failure occurred on the communications port 2. TRUE: There was a failure to connect to the BOOTP server (timeout). FALSE: The BOOTP is not enabled, or BOOTP is enabled and an IP address was normally obtained from the BOOTP server.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_TcpAppCfgErr				
Meaning	TCP Application Setting Error			**Global/local**	Global
Function	TRUE: At least one of the set values for a TCP application is incorrect. Or, a read operation failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_IPRTblErr				
Meaning	IP Router Table Setting Error			**Global/local**	Global
Function	Indicates that the default gateway settings or IP router table settings are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_DNSCfgErr				
Meaning	DNS Setting Error			**Global/local**	Global
Function	Indicates that the DNS or hosts settings are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.

Variable name	EIP_ErrSta				
Meaning	CIP Communications Error			**Global/local**	Global
Function	This is the error status variable for CIP communications. It represents the collective status of the following error flags. • EIP_Comm1Status.CipErr (CIP Communications1 Error) • EIP_Comm2Status.CipErr (CIP Communications2 Error) **Note** Refer to *Meanings of Error Status Bits* on page 6-10 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#00F0
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm1Status.CipErr				
Meaning	CIP Communications1 Error			**Global/local**	Global
Function	This is the error status variable for CIP communications on the communications port 1. It represents the collective status of the following error flags. • EIP_Comm1Status.IdentityErr (CIP Communications1 Identity Error) • EIP_Comm1Status.TDLinkCfgErr (CIP Communications1 Tag Data Link Setting Error) • EIP_Comm1Status.TDLinkOpnErr (CIP Communications1 Tag Data Link Connection Failed) • EIP_Comm1Status.TDLinkErr (CIP Communications1 Tag Data Link Communications Error) • EIP_Comm1Status.TagAdrErr (CIP Communications1 Tag Name Resolution Error) **Note** Refer to *Meanings of Error Status Bits* on page 6-10 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#00F0
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm2Status.CipErr				
Meaning	CIP Communications2 Error			**Global/local**	Global
Function	This is the error status variable for CIP communications on the communications port 2. It represents the collective status of the following error flags. • EIP_Comm2Status.IdentityErr (CIP Communications2 Identity Error) • EIP_Comm2Status.TDLinkCfgErr (CIP Communications2 Tag Data Link Setting Error) • EIP_Comm2Status.TDLinkOpnErr (CIP Communications2 Tag Data Link Connection Failed) • EIP_Comm2Status.TDLinkErr (CIP Communications2 Tag Data Link Communications Error) • EIP_Comm2Status.TagAdrErr (CIP Communications2 Tag Name Resolution Error) **Note** Refer to *Meanings of Error Status Bits* on page 6-10 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#00F0
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm1Status.IdentityErr				
Meaning	CIP Communications1 Identity Error			**Global/local**	Global
Function	Indicates that the identity information for CIP communications 1 (which you cannot overwrite) is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm2Status.IdentityErr				
Meaning	CIP Communications2 Identity Error			**Global/local**	Global
Function	Indicates that the identity information for CIP communications 2 (which you cannot overwrite) is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm1Status.TDLinkCfgErr				
Meaning	CIP Communications1 Tag Data Link Setting Error			**Global/local**	Global
Function	Indicates that the tag data link settings for CIP communications 1 are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm2Status.TDLinkCfgErr				
Meaning	CIP Communications2 Tag Data Link Setting Error			**Global/local**	Global
Function	Indicates that the tag data link setting for CIP communications 2 are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm1Status.TDLinkOpnErr				
Meaning	CIP Communications1 Tag Data Link Connection Failed			**Global/local**	Global
Function	Indicates that establishing a tag data link connection for CIP communications 1 failed. TRUE: Establishing a tag data link connection failed due to one of the following causes. • The information registered for a target node in the tag data link parameters is different from the actual node information. • There was no response from the remote node. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm2Status.TDLinkOpnErr				
Meaning	CIP Communications2 Tag Data Link Connection Failed			**Global/local**	Global
Function	Indicates that establishing a tag data link connection for CIP communications 2 failed. TRUE: Establishing a tag data link connection failed due to one of the following causes. • The information registered for a target node in the tag data link parameters is different from the actual node information. • There was no response from the remote node. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm1Status.TDLinkErr				
Meaning	CIP Communications1 Tag Data Link Communications Error			**Global/local**	Global
Function	Indicates that a timeout occurred in a tag data link connection for CIP communications 1. TRUE: A timeout occurred. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm2Status.TDLinkErr				
Meaning	CIP Communications2 Tag Data Link Communications Error			**Global/local**	Global
Function	Indicates that a timeout occurred in a tag data link connection for CIP communications 2. TRUE: A timeout occurred. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm1Status.TagAdrErr				
Meaning	CIP Communications1 Tag Name Resolution Error			**Global/local**	Global
Function	Indicates that the tag resolution for CIP communications 1 failed (i.e., the address could not be identified from the tag name). TRUE: Tag resolution failed (i.e., the address could not be identified from the tag name). The following causes are possible. • The size of the network variable is different from the tag settings. • The I/O direction that is set in the tag data link settings does not agree with the I/O direction of the variable in the NX-series EtherNet/IP Unit. • There is no network variable in the NX-series EtherNet/IP Unit that corresponds to the tag setting. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm2Status.TagAdrErr				
Meaning	CIP Communications2 Tag Name Resolution Error			**Global/local**	Global
Function	Indicates that the tag resolution for CIP communications 2 failed (i.e., the address could not be identified from the tag name). TRUE: Tag resolution failed (i.e., the address could not be identified from the tag name). The following causes are possible. • The size of the network variable is different from the tag settings. • The I/O direction that is set in the tag data link settings does not agree with the I/O direction of the variable in the NX-series EtherNet/IP Unit. • There is no network variable in the NX-series EtherNet/IP Unit that corresponds to the tag setting. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

● Functional Classification: NX-series EtherNet/IP Unit Status

Variable name	ETN_Port1Status.EtnOnlineSta				
Meaning	Port1 Online			**Global/local**	Global
Function	Indicates that the EtherNet/IP port's communications can be used via the communications port 1 (that is, the link is ON, IP address is defined, and there are no errors.) TRUE: The EtherNet/IP port’s communications can be used. FALSE: The EtherNet/IP port’s communications is disabled due to an error in initial processing, restart processing, or link OFF status.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	ETN_Port2Status.EtnOnlineSta				
Meaning	Port2 Online			**Global/local**	Global
Function	Indicates that the EtherNet/IP port's communications can be used via the communications port 2 (that is, the link is ON, IP address is defined, and there are no errors.) TRUE: The EtherNet/IP port’s communications can be used. FALSE: The EtherNet/IP port’s communications is disabled due to an error in initial processing, restart processing, or link OFF status.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm1Status.TDLinkRunSta				
Meaning	CIP Communications1 Tag Data Link Communications Status			**Global/local**	Global
Function	Indicates that at least one connection is in normal operation in CIP communications 1. TRUE: Normal operation FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm2Status.TDLinkRunSta				
Meaning	CIP Communications2 Tag Data Link Communications Status			**Global/local**	Global
Function	Indicates that at least one connection is in normal operation in CIP communications 2. TRUE: Normal operation FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm1Status.TDLinkAllRunSta				
Meaning	CIP Communications1 All Tag Data Link Communications Status			**Global/local**	Global
Function	Indicates that all tag data links are communicating in CIP communications 1. TRUE: Tag data links are communicating in all connections as the originator. FALSE: An error occurred in at least one connection.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm2Status.TDLinkAllRunSta				
Meaning	CIP Communications2 All Tag Data Link Communications Status			**Global/local**	Global
Function	Indicates that all tag data links are communicating in CIP communications 2. TRUE: Tag data links are communicating in all connections as the originator. FALSE: An error occurred in at least one connection.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm1Status.RegTargetSta[255]				
Meaning	CIP Communications1 Registered Target Node Information			**Global/local**	Global
Function	Gives a list of nodes for which EtherNet/IP connections are registered for CIP communications 1. This variable is valid only when the EtherNet/IP port is the originator. Array[x] is TRUE: The connection to the node with a target node ID of x is registered. Array[x] is FALSE: The connection to the node with a target node ID of x is not registered.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm2Status.RegTargetSta[255]				
Meaning	CIP Communications2 Registered Target Node Information			**Global/local**	Global
Function	Gives a list of nodes for which EtherNet/IP connections are registered for CIP communications 2. This variable is valid only when the EtherNet/IP port is the originator. Array[x] is TRUE: The connection to the node with a target node ID of x is registered. Array[x] is FALSE: The connection to the node with a target node ID of x is not registered.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm1Status.EstbTargetSta[255]				
Meaning	CIP Communications1 Normal Target Node Information			**Global/local**	Global
Function	Gives a list of nodes that have normally established EtherNet/IP connections for CIP communications 1. Array[x] is TRUE: The connection to the node with a target node ID of x was established normally. Array[x] is FALSE: The connection to the node with a target node ID of x was not established, or an error occurred.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm2Status.EstbTargetSta[255]				
Meaning	CIP Communications2 Normal Target Node Information			**Global/local**	Global
Function	Gives a list of nodes that have normally established EtherNet/IP connections for CIP communications 2. Array[x] is TRUE: The connection to the node with a target node ID of x was established normally. Array[x] is FALSE: The connection to the node with a target node ID of x was not established, or an error occurred.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm1Status.TargetPLCModeSta[255]				
Meaning	CIP Communications1 Target PLC Operating Mode			**Global/local**	Global
Function	Shows the operating status of the target node Controllers that are connected for CIP communications 1, with the EtherNet/IP port as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. If the corresponding Normal Target Node Information is FALSE, it indicates the previous operating status. Array[x] is TRUE: This is the operating state of the target Controller with a node address of x. Array[x] is FALSE: Other than the above.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm2Status.TargetPLCModeSta[255]				
Meaning	CIP Communications2 Target PLC Operating Mode			**Global/local**	Global
Function	Shows the operating status of the target node Controllers that are connected for CIP communications 2, with the EtherNet/IP port as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. If the corresponding Normal Target Node Information is FALSE, it indicates the previous operating status. Array[x] is TRUE: This is the operating state of the target Controller with a node address of x. Array[x] is FALSE: Other than the above.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm1Status.TargetPLCErr[255]				
Meaning	CIP Communications1 Target PLC Error Information			**Global/local**	Global
Function	Shows the error status (logical OR of fatal and non-fatal errors) of the target node Controllers that are connected for CIP communications 1, with the EtherNet/IP ports as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. The immediately preceding value is retained if this variable is FALSE. Array[x] is TRUE: A fatal or non-fatal error occurred in the target Controller with a target node ID of x. Array[x] is FALSE: Other than the above.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm2Status.TargetPLCErr[255]				
Meaning	CIP Communications2 Target PLC Error Information			**Global/local**	Global
Function	Shows the error status (logical OR of fatal and non-fatal errors) of the target node Controllers that are connected for CIP communications 2, with the EtherNet/IP ports as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. The immediately preceding value is retained if this variable is FALSE. Array[x] is TRUE: A fatal or non-fatal error occurred in the target Controller with a target node ID of x. Array[x] is FALSE: Other than the above.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

Variable name	EIP_Comm1Status.TargetNodeErr[255]				
Meaning	CIP Communications1 Target Node Error Information			**Global/local**	Global
Function	Indicates that the connection for the Registered Target Node Information for CIP communications 1 was not established or that an error occurred in the target Controller. The array elements are valid only when the Registered Target Node Information is TRUE. Array[x] is TRUE: A connection was not normally established with the target node for a target node ID of x (the Registered Target Node Information is TRUE and the Normal Target Node Information is FALSE), or a connection was established with the target node but an error occurred in the target Controller. Array[x] is FALSE: The target node is not registered for a target node ID of x (the Registered Target Node Information is FALSE), or a connection was normally established with the target node (the Registered Target Node Information is TRUE and the Normal Target Node Information is TRUE). An error occurred in the target Controller (the Target PLC Error Information is TRUE).				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

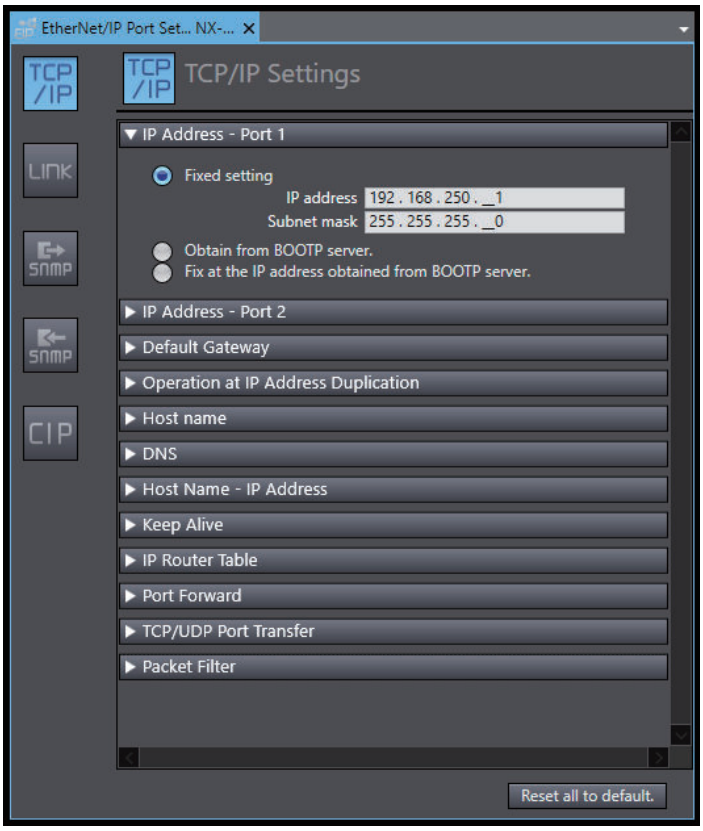
Variable name	EIP_Comm2Status.TargetNodeErr[255]				
Meaning	CIP Communications2 Target Node Error Information			**Global/local**	Global
Function	Indicates that the connection for the Registered Target Node Information for CIP communications 2 was not established or that an error occurred in the target Controller. The array elements are valid only when the Registered Target Node Information is TRUE. Array[x] is TRUE: A connection was not normally established with the target node for a target node ID of x (the Registered Target Node Information is TRUE and the Normal Target Node Information is FALSE), or a connection was established with the target node but an error occurred in the target Controller. Array[x] is FALSE: The target node is not registered for a target node ID of x (the Registered Target Node Information is FALSE), or a connection was normally established with the target node (the Registered Target Node Information is TRUE and the Normal Target Node Information is TRUE). An error occurred in the target Controller (the Target PLC Error Information is TRUE).				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Do not publish.
Usage in user program	Possible.	**Related instructions**	---		

7

Sysmac Studio Settings for the EtherNet/IP Port

This section describes the EtherNet/IP port settings with the Sysmac Studio.
The EtherNet/IP port settings are made for each NX-series EtherNet/IP Unit that is connected to the CPU Unit on the Sysmac Studio. Make the EtherNet/IP port settings on the Sysmac Studio under **Configurations and Setup** - **CPU/Expansion Racks** - **CPU Rack: X Bus** - **Unit No.: NX-EIP201 ()** - **EtherNet/IP Port Settings**.

7-1 TCP/IP Settings Display



▼ IP Address - Port 1

● Fixed setting

IP address 192 . 168 . 250 . 1

Subnet mask 255 . 255 . 255 . 0

○ Obtain from BOOTP server.

○ Fix at the IP address obtained from BOOTP server.

● IP Address - Port 1

Set an IP address for the EtherNet/IP port 1.

Setting	Description	Default
IP address setting method	Select one of the following IP address setting methods for the EtherNet/IP port 1. • Fixed setting • Obtain from BOOTP server. • Fix at the IP address obtained from BOOTP server.	Fixed setting
IP address[*1]	Set the IP address for the EtherNet/IP port 1. [*2]	192.168.250.1
Subnet mask[*2]	Set the subnet mask for the EtherNet/IP port 1.	255.255.255.0

[*1] This setting is required if you set IP address setting method to **Fixed setting**.

[*2] Refer to *8-1-2 EtherNet/IP Port IP Address Settings* on page 8-4 for details on setting IP addresses.

● IP Address - Port 2

Set an IP address for the EtherNet/IP port 2.

Setting	Description	Default
Use Port 2	Select the check box to use the EtherNet/IP port 2.	Selected (use)

Setting	Description	Default
IP address setting method	Select one of the following IP address setting methods for the EtherNet/IP port 2. • Fixed setting • Obtain from BOOTP server. • Fix at the IP address obtained from BOOTP server.	Fixed setting
IP address[*1]	Set the IP address for the EtherNet/IP port 2. [*2]	192.168.251.1
Subnet mask[*2]	Set the subnet mask for the EtherNet/IP port 2.	255.255.255.0

*1. This setting is required if you set IP address setting method to **Fixed setting**.

*2. Refer to *8-1-2 EtherNet/IP Port IP Address Settings* on page 8-4 for details on setting IP addresses.

Precautions for Correct Use

- You cannot set IP addresses that make two EtherNet/IP ports belong to the same network.
- You can set IP addresses that make EtherNet/IP ports on two or more NX-series EtherNet/IP Units that are connected to the X Bus belong to the same network. However, in that case, you cannot perform communications by specifying the destination by the IP via the NX-series EtherNet/IP Units.

● Default Gateway

Setting	Description	Default
Default gateway[*1]	Set the IP address of the default gateway for the EtherNet/IP port. [*2] This setting is not required when the default gateway is not used.	None

*1. If you select **Obtain from BOOTP server** or **Fix at the IP address obtained from BOOTP server** for the IP address setting method, the default gateway obtained from a BOOTP server is enabled.

*2. Even if you are using both of port 1 and port 2, you can set the default gateway for only one of the ports.

● Operation at IP Address Duplication

Setting	Description	Default
Use of duplicated IP address	When you set an IP address for the EtherNet/IP port and find an IP address conflict with another node, select whether to stop the use of the IP address. • Stop If the IP address conflict is not resolved for a certain length of time, the use of the IP address is stopped, and an IP Address Duplication Error will occur. • Do not stop IP Address Duplication Error does not occur and you continue to use the IP address that you set. This setting is used if you want to avoid that communications are stopped because the same IP address is assigned to more than one node.	Stop

Precautions for Correct Use

If this setting is **Do not stop**, it is not notified that the same IP address is assigned to more than one node to the user. Also, if the same IP address is assigned to more than one node while this setting is **Do not stop**, the communications may become unstable, such as being temporarily unavailable. If it is unacceptable for the communication to be unstable, detect that the same IP address is assigned to more than one node to the remote node.

Host Name

Setting	Description	Default
Host Name	Set the host name for the local Unit. The local host name can be set for each Unit. The set host name is set to *sysName* of the system group and *lldpLocSysName* of the lldp group in the MIB (Management Information Base). [*1][*2] (Single-byte alphanumeric characters, dots, and hyphens: 63 characters max.)	None[*3]

[*1] Since the local host name identifies the Unit, set the name so that it does not use the same name in the same network.

[*2] Refer to *11-1-4 MIB Specifications* on page 11-4 for details on the MIB.

[*3] If you do not set the local host name, the model of the Unit will be the local host name.

DNS

Setting	Description	Default
Use/ Do not use DNS	When you specify a host name for SNMP function, select the **Use** Option if you use DNS for resolving host name. A DNS server is required to use DNS.	Do not use
Priority DNS server[*1]	Set the IP address of the DNS server. You can set priority and secondary IP addresses.	None
Secondary DNS server		None
Domain name[*1]	Set the domain name of the domain to which the EtherNet/IP port belongs. (Single-byte alphanumeric characters, dots, and hyphens: 48 characters max.)	None

[*1] These settings are required if you select the **Use** Option for **DNS**.

Host Name - IP Address

Setting	Description	Default
Host Name	Addresses are converted according to this setting when a host name is used to specify remote communications nodes. Host names can be set whether DNS is used or not. You can set up to six host names. (Single-byte alphanumeric characters, dots, and hyphens: 200 characters max. with up to 63 single-byte alphanumeric characters between dots.)	None
IP Address	Set the IP address of the registered host name.	None

● Keep Alive

Setting	Description	Default
Keep Alive	Set whether to use the remote node Keep Alive function of connected servers and clients (such as Sysmac Studio and FINS/TCP) for each connection number. If the **Use** Option is selected for **Keep Alive** and no communications are performed with the remote node for the **Keep Alive monitoring time**, transmission of Keep Alive packets is started. The connection will be disconnected if the remote node does not respond for longer than five times the total time of Keep Alive packet transmission + five seconds for resending.[*1] The connection to the remote node is left open if the power supply to the remote node is turned OFF without warning. Select the **Use** Option for Keep Alive wherever possible. • Use • Do not use	Use
Keep Alive monitoring time	This is a set period of time before the transmission of Keep Alive packets is started. Setting range: 1 to 65,535 (seconds)	300
Linger option	Set whether to specify the Linger Option. If the Linger Option is specified, the port number is immediately opened even before the port number is released after the TCP port closes (approx. 1 minute). • Specify • Do not specify	Do not specify

[*1] If the remote node does not respond, the connection is disconnected after the Keep Alive monitoring time + 30 seconds.

● IP Router Table

Setting	Description	Default
Destination IP Address	Set these settings when the EtherNet/IP port is used for tag data links or CIP message communications with nodes on other IP network segments via an IP router. You can set up to 64 combinations of an IP address and a gateway address. Specify 0 for the host portions of the IP addresses.	None
Destination Mask IP Address		
Gateway Address		None

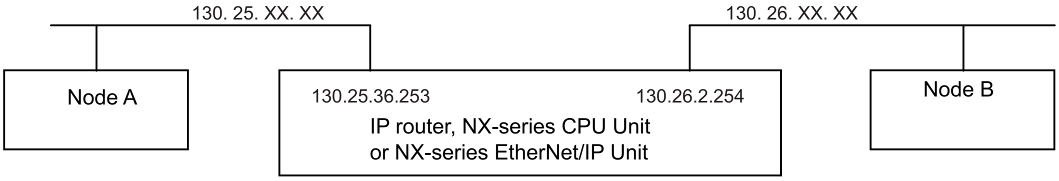
Additional Information

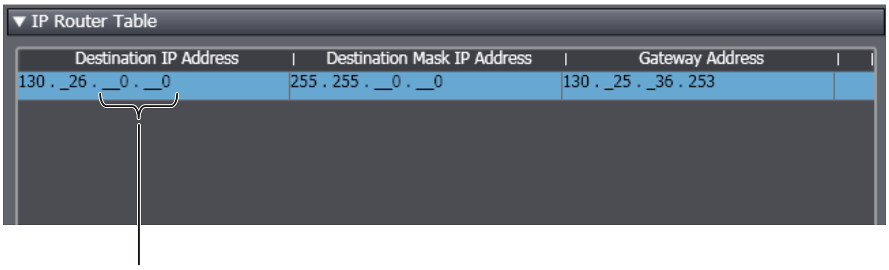
IP Router Table Setting Example

Set the following IP router table on the node A device to use tag data links or CIP message communications between node A and node B through the IP router.

For an NX-series CPU Unit or an NX-series EtherNet/IP Unit, set **Port Forward** - **IP Forward** to **Use**.

If you set the IP router table and execute a communications instruction from node A to node B, node A sends packets addressed to the gateway IP address (130.25.36.253).





Destination IP Address	Destination Mask IP Address	Gateway Address
130 . _26 . __0 . __0	255 . 255 . __0 . __0	130 . _25 . _36 . 253

The host fields are set to 0 in the destination IP address.

● Port Forward

Setting	Description	Default
IP Forward	Select whether to transfer IP packets between communications ports.	Do not use

The following shows the applications that are not supported by the NX-series EtherNet/IP Unit, and they are classified by whether this function is valid or invalid. In applications for which this function is invalid, the IP packets are not transferred even if the **Use** Option is selected.

Valid/Invalid	Application
Valid	Socket communications, secure socket communications, FTP server, FTP client, NTP client, DB connection service, Modbus/TCP communications, MQTT communications
Invalid	FINS/UDP, FINS/TCP, DHCP client, OPC UA, SECS/GEM connection service, Robot integrated

● TCP/UDP Port Transfer

Setting	Description	Default
Port	Set the TCP port or UDP port that is used for TCP/IP communications if you want to access the CPU Unit via the EtherNet/IP port on the NX-series EtherNet/IP Unit from an external device such as a computer. This setting is set for each EtherNet/IP port. *1*2 • Port1 • Port2	None
Protocol	Set the protocol used for communications. • TCP • UDP	None

Setting	Description	Default
Port Number	Set the port number used for communications. *3 Setting range: 1 to 65,535	None

*1. To use this function, select the **Use** Option for **IP Forward** in the port forward. If the **Do not use** Option is selected, the sent frames will be discarded.

*2. On the client side of the external device, specify the IP address of the EtherNet/IP port on the NX-series EtherNet/IP Unit and send the frame.

*3. Specify a port number that is not used by the NX-series EtherNet/IP Units. Refer to *A-7 TCP/UDP Port Numbers Used for the NX-series EtherNet/IP Unit* on page A-55 for details on the TCP/UDP port numbers that are used by the NX-series EtherNet/IP Units.

The following shows the applications that are not supported by the NX-series EtherNet/IP Unit, and they are classified by whether this function is valid or invalid. The invalid applications cannot access the CPU Unit even if the **Protocol** or **Port Number** are set.

Valid/Invalid	Application
Valid	Socket communications, secure socket communications, FTP server, MQTT communications
Invalid	FTP client, NTP client, FINS/UDP, FINS/TCP, DB connection service, Modbus/TCP communications, DHCP client, OPC UA, SECS/GEM connection service, Robot integrated

● Packet Filter

For information on usage and restrictions of Packet Filter, refer to *8-4 Packet Filter* on page 8-15.

Setting		Description	Default
Packet Filter		Select whether to use Packet Filter or not. Use Do not use	Do not use
Source		Set the conditions for the source.	---
	IP Address Specification Method	Select the method for specifying the IP address of the source. any*1 IP address specification	any
	IP Address	If the IP address specification method is **IP address specification**, set the source IP address.*2	None
	Mask	If the IP address specification method is **IP address specification**, set the mask of source IP address.*3	None
Destination		Set the conditions for the destination.	---
	IP Address Specification Method	Same as those for the source.	
	IP Address		
	Mask		
Protocol		Set the communications protocol. any*4 tcp udp igmp*5 icmp*6	any
Source Port		If **tcp** or **udp** is selected for Protocol, set the source port conditions.	---

Setting		Description	Default
	Specification Method	Select the method for specifying the IP packets of the source port. any[7] Port specification	any
	Range Specification	Specify whether or not to set the port range if the specification method selected is **Port specification**. If it is selected, reception from the source ports from the **Start Number** to the **End Number** is allowed. If it is not selected, reception from the source port specified by the **Start Number** is allowed. No check. Checked.	No check.
	Start Number	Set the start number when **Port specification** is selected for the specification method. 1 to 65535	None
	End Number	Set the end number when the specification method is **Port specification** and the range specification is selected. 1 to 65535	None
Destination Port		Set the conditions for the destination port if **tcp** or **udp** is selected for Protocol. Same as the settings for the source port.	
	Specification Method		
	Range Specification		
	Start Number		
	End Number		

*1. If you select any, packets from any IP addresses will be allowed.

*2. The allowed IP address is calculated by the logical AND of the **IP address** and the **Mask**. If you want to allow more than one IP address, mask a part of the IP address by setting the **Mask**. In this case, set 0 to the bits to be masked in the **IP address** and **Mask**.

The following is an example of how to calculate the allowed IP addresses.

Example 1. Allowing IP address 192.168.250.1

If you want to allow one IP address, set 255.255.255.255 to the mask.

Setting	Decimal notation	Binary notation
IP address	192.168.250.1	11000000.10101000.11111010.00000001
Mask	255.255.255.255	11111111.11111111.11111111.11111111

Example 2. Allowing IP address 192.168.250.***

Set 255.255.255.0 to the mask to mask the lower 8 bits of the IP address.

Setting	Decimal notation	Binary notation
IP address	192.168.250.0	11000000.10101000.11111010.00000000
Mask	255.255.255.0	11111111.11111111.11111111.00000000

Example 3. Allowing IP address 192.168.250.1 to 192.168.250.31

Set 255.255.255.224 to the mask to mask the lower 5 bits if the IP address.

Setting	Decimal notation	Binary notation
IP address	192.168.250.0	11000000.10101000.11111010.00000000
Mask	255.255.255.224	11111111.11111111.11111111.11100000

*3. Set 0 to the bits to be masked in **Mask**. Multiple bits can be masked, but only bits from the least significant can be masked. It is not possible to mask the higher bits, such as 0.255.255.255, or the middle bits, such as 255.0.255.255.

The following are examples of setting a mask.

Example 1. Masking the lower 8 bits

Set 0 to the lower 8 bits.

Setting	Decimal notation	Binary notation
Mask	255.255.255.0	11111111.11111111.11111111.00000000

Example 2. Masking the lower 24 bits

Set 0 to the lower 24 bits.

Setting	Decimal notation	Binary notation
Mask	255.0.0.0	11111111.00000000.00000000.00000000

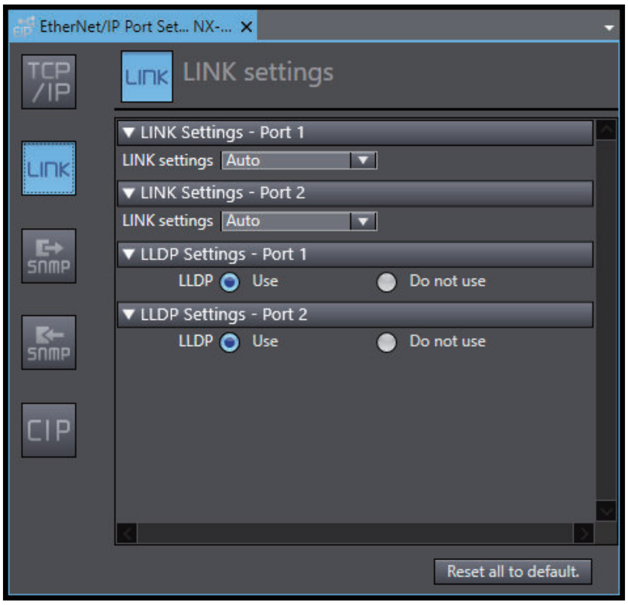
*4. If you select any, packets from tcp, udp, igmp, and icmp will be allowed.

*5. Select igmp when EtherNet/IP tag data links are used for multicast and the EtherNet/IP is specified as the originator.

*6. Select icmp for receiving Ping requests.

*7. If you select any, packets from any TCP/UDP port are allowed.

7-2 LINK Settings Display



▼ LINK Settings - Port 1

LINK settings: Auto

▼ LINK Settings - Port 2

LINK settings: Auto

▼ LLDP Settings - Port 1

LLDP ● Use ○ Do not use

▼ LLDP Settings - Port 2

LLDP ● Use ○ Do not use

● Link Settings - Port 1 and Port 2

Set for each EtherNet/IP port.

Setting	Description	Default
LINK settings	Set the baud rate for the EtherNet/IP ports. • Auto	Auto

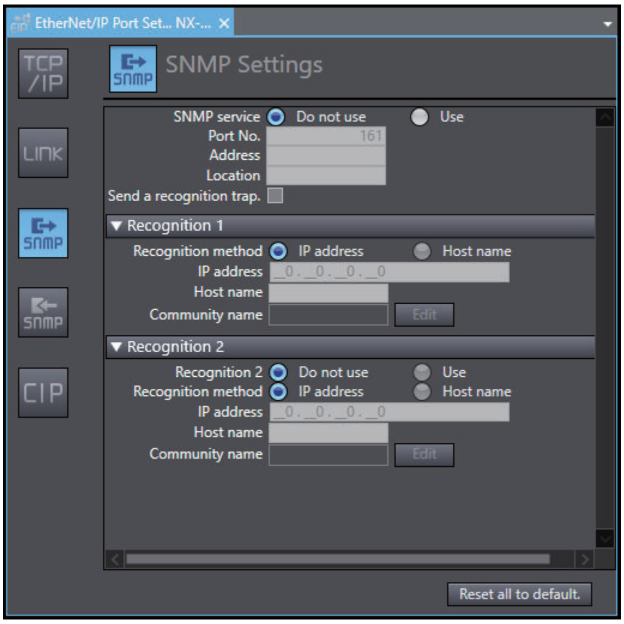
● LLDP Settings - Port 1 and Port 2

Set for each EtherNet/IP port.

Setting	Description	Default
LLDP[*1]	Select whether to use LLDP (Link Layer Discovery Protocol) function. • Use • Do not use	Use

[*1] When the LLDP function is used, the Controller can exchange various information such as identification information with the network devices that are located within the range of physical communication. Information on network devices can be obtained with the SNMP function.

7-3 SNMP Settings Display



SNMP service ● Do not use ○ Use
Port No. 161
Address
Location
Send a recognition trap. ☐

▼ Recognition 1
Recognition method ● IP address ○ Host name
IP address 0. 0. 0. 0
Host name
Community name

▼ Recognition 2
Recognition 2 ● Do not use ○ Use
Recognition method ● IP address ○ Host name
IP address 0. 0. 0. 0
Host name
Community name

● SNMP

Setting	Description	Default
SNMP service	Specify whether to use the SNMP monitor service.[*1] If the **Do not use** Option is selected, an SNMP manager cannot connect from an external device.	Do not use
Port No.[*2]	Set the port number to use to connect to the SNMP server that is used to connect from an SNMP manager. This setting does not normally need to be changed.	161
Address	Set the communications device administrator's name and installation location as text information. You do not necessarily have to input all items. This information is read by the SNMP manager. (You can input up to 255 single-byte alphanumeric characters for each item.)	None
Location		None
Send a recognition trap	Set whether to send an authentication trap. If you select **Send a recognition trap** and there is access from an SNMP manager that is not set in Recognition 1 or Recognition 2, an authentication trap is sent to the SNMP manager. If you select **Send a recognition trap**, specify the SNMP trap settings on the **SNMP Trap** Tab.	Not selected

[*1] If you select the Use Option for the SNMP service, you also have to set Recognition 1 and 2 as described below.

[*2] The following ports are used by the system and cannot be set by the user: 25, 53, 68, 110, 2222, 2223, 2224, 9600, and 44818.

Additional Information

Refer to *Section 11 SNMP Agent* on page 11-1 for details on the SNMP service.

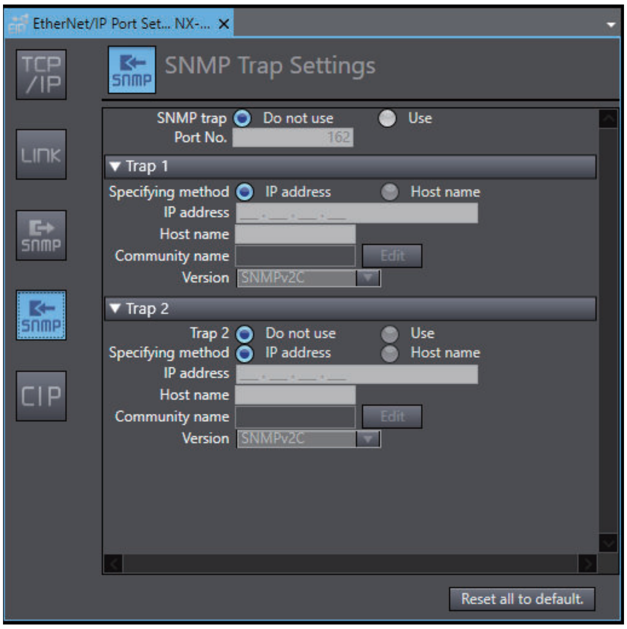
● Recognition 1

Setting	Description	Default
Recognition method	Set the method to use to specify SNMP managers for which access is permitted. • IP address • Host name Make these settings to permit access by only certain SNMP managers. Access is not allowed unless an IP address or host name is set.	IP address
IP address	Set the IP address of the SNMP manager. If the default setting of 0.0.0.0 is used, access by all SNMP managers is permitted. (Set this setting if **Recognition method** in Recognition 1 is set to the **IP address** Option.)	None
Host name	Set the host name of the SNMP manager. (Set this setting if **Recognition method** in Recognition 1 is set to the **Host name** Option.) (Single-byte alphanumeric characters, dots, and hyphens: 200 characters max. with up to 63 single-byte alphanumeric characters between dots.)	None
Community name	Set the community name to enable the SNMP manager to access information from the EtherNet/IP port. (Single-byte alphanumeric characters, dots, and hyphens: 255 characters max.)	public

● Recognition 2

Setting		Description	Default
Recognition 2		Specify whether to use the recognition 2 settings. • Use • Do not use	Do not use
	Recognition method	Set the method to use to specify SNMP managers for which access is permitted. • IP address • Host name Make these settings to permit access by only certain SNMP managers. Access is not allowed unless an IP address or host name is set.	IP address
	IP address	Set the IP address of the SNMP manager. If the default setting of 0.0.0.0 is used, access by all SNMP managers is permitted. (Set this setting if **Recognition method** in Recognition 2 is set to the **IP address** Option.)	None
	Host name	Set the host name of the SNMP manager. (Set this setting if **Recognition method** in Recognition 2 is set to the **Host name** Option.) (Single-byte alphanumeric characters, dots, and hyphens: 200 characters max. with up to 63 single-byte alphanumeric characters between dots.)	None
	Community name	Set the community name to enable the SNMP manager to access information from the EtherNet/IP port. (Single-byte alphanumeric characters, dots, and hyphens: 255 characters max.)	public

7-4 SNMP Trap Settings Display



SNMP Trap Settings

SNMP trap ● Do not use ○ Use
Port No. 162

▼ Trap 1
Specifying method ● IP address ○ Host name
IP address ___.___.___.___
Host name
Community name
Version SNMPv2C

▼ Trap 2
Trap 2 ● Do not use ○ Use
Specifying method ● IP address ○ Host name
IP address ___.___.___.___
Host name
Community name
Version SNMPv2C

● SNMP Trap

Setting	Description	Default
SNMP trap	Specify whether to use the SNMP trap (network error detection).[*1] If the **Do not use** Option is selected for SNMP trap, SNMP traps are not sent to the SNMP manager	Do not use
Port No.[*2]	Set the port number to use to connect to the SNMP server. It is normally not necessary to change this setting.	162

*1. If you specify to use the SNMP trap, you also have to set Trap 1 and Trap 2 as described below.

*2. The following ports are used by the system and cannot be set by the user: 25, 53, 68, 110, 2222, 2223, 2224, 9600, and 44818.

Additional Information

Refer to *11-1-1 Overview* on page 11-2 for details on the SNMP trap.

● Trap 1

If the **Use** Option is selected for **SNMP trap**, you need to make the following settings.

Setting	Description	Default
Specifying method	Set the specifying method for the SNMP manager destination for SNMP traps. • IP address • Host name	IP address
IP address	Set the IP address of the SNMP manager. (Set this setting if the **Specifying method** in the Trap 1 settings is set to the **IP address** Option.)	None

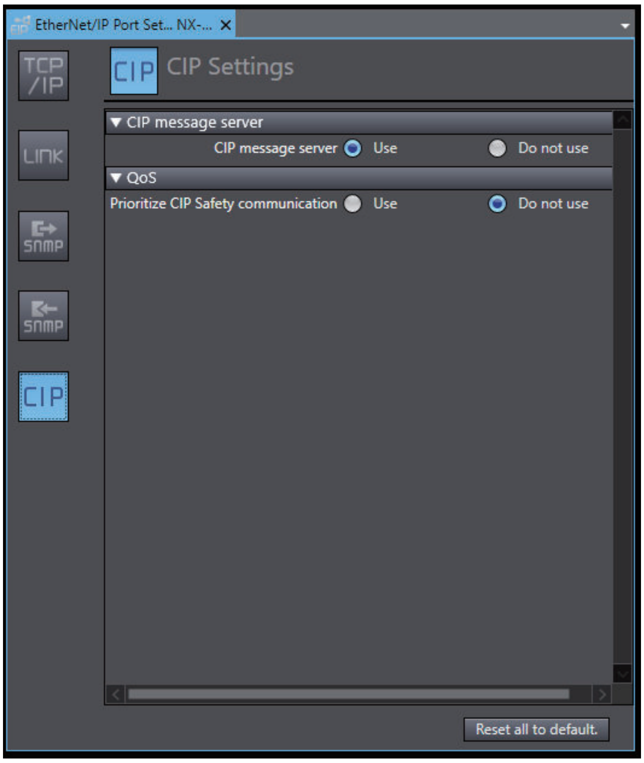
Setting	Description	Default
Host name	Set the host name of the SNMP manager. (Set this setting if the **Specifying method** in the Trap 1 settings is set to the **Host name** Option.) (Single-byte alphanumeric characters, dots, and hyphens: 200 characters max. with up to 63 single-byte alphanumeric characters between dots.)	None
Community name	Set the community name. (You can use up to 255 single-byte alphanumeric characters.)	public
Version	Set the version of the SNMP manager. • SNMPv1 • SNMPv2C	SNMPv2C

Trap 2

If the **Use** Option is selected for **SNMP trap**, you need to make the following settings.

Setting	Description	Default
Trap 2	Specify whether to use the Trap 2 settings. • Use • Do not use	Do not use
Specifying method	Set the specifying method for the SNMP manager destination for SNMP traps. • IP address • Host name	IP address
IP address	Set the IP address of the SNMP manager. (Set this setting if the **Specifying method** in the Trap 2 settings is set to the **IP address** Option.)	None
Host name	Set the host name of the SNMP manager. (Set this setting if the **Specifying method** in the Trap 2 settings is set to the **Host name** Option.) (Single-byte alphanumeric characters, dots, and hyphens: 200 characters max. with up to 63 single-byte alphanumeric characters between dots.)	None
Community name	Set the community name. (You can use up to 255 single-byte alphanumeric characters.)	public
Version	Set the version of the SNMP manager. • SNMPv1 • SNMPv2C	SNMPv2C

7-5 CIP Settings Display



▼ CIP message server

CIP message server ● Use ○ Do not use

▼ QoS

Prioritize CIP Safety communication ○ Use ● Do not use

● CIP Message Server

Setting	Description	Default
CIP Message Server	Specify whether to use the CIP message server or not. If the **Use** Option is selected, the following ports will be opened. • UDP 2222 • UDP 44818 • TCP 44818	Use

Refer to *10-3 Server Function of CIP Message Communications* on page 10-23 for restrictions when the **Do not use** Option is selected for CIP message server.

● QoS

Setting	Description	Default
Prioritize CIP Safety communication	Select whether to prioritize CIP Safety communications in QoS.	Do not use

8

TCP/IP Functions

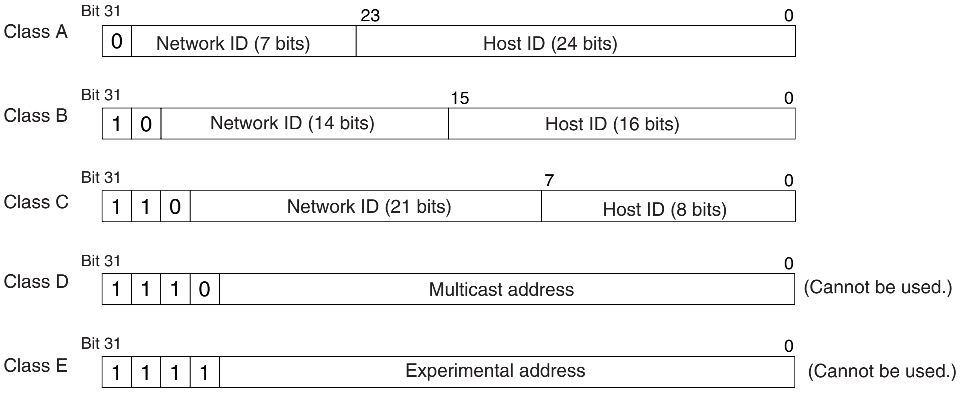
8-1 Determining IP Addresses

8-1-1 IP Addresses

IP Address Configuration

IP addresses are made up of 32 bits of binary data that specify the network number (net ID) and host number (host ID). The net ID is an address used for identifying a network. The host ID is an address used for identifying a host (node).

IP addresses 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 number of networks in each class and the number of hosts 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 binary data in an IP address are divided into four sections of eight bits each. IP addresses are represented by the decimal equivalent of each of the four octets in the 32-bit address, each separated by a period.

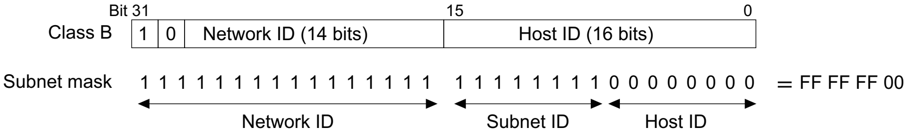
For example, the binary address 10000010 00111010 00010001 00100000 would be represented as 130.58.17.32.

Allocating IP Addresses

You must assign IP addresses nodes so that each IP address is assigned only once in the network or between several networks.

Subnet Mask

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. 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 the class-B IP address.



Set the same subnet mask for all of the nodes on the subnetwork. The 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.
If subnetworks are not used, set the following subnet mask values for IP address classes A to C.

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

A network address is information derived from a subnet mask and used to identify each network. A network address enables users to determine whether multiple nodes belong to the same network. A network address is calculated by performing a logical AND operation on the IP address and subnet mask of a node.
The following are examples of network address calculation.
In this example, the IP address of node 1 is set to *192.168.250.20*, the IP address of node 2 is set to *192.168.245.30*, and the subnet mask is set to *255.255.240.0*. The network addresses of the two nodes are calculated as follows.

- Calculating network address of node 1

Item	Decimal notation	Binary notation
IP address	192.168.250.20	11000000.10101000.11111010.00010100
Subnet Mask	255.255.240.0	11111111.11111111.11110000.00000000
Network address	192.168.240.0	11000000.10101000.11110000.00000000

- Calculating network address of node 2

Item	Decimal notation	Binary notation
IP address	192.168.245.30	11000000.10101000.11111010.00010100
Subnet Mask	255.255.240.0	11111111.11111111.11110000.00000000
Network address	192.168.240.0	11000000.10101000.11110000.00000000

As shown in the above tables, node 1 and node 2 have the same network address, which means these nodes belong to the same network.

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 network 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...) is used.

Subnet Mask Range
192.0.0.0 to 255.255.255.252

8-1-2 EtherNet/IP Port IP Address Settings

Determining IP Addresses

Use one of the following methods to set an IP address of an EtherNet/IP port.

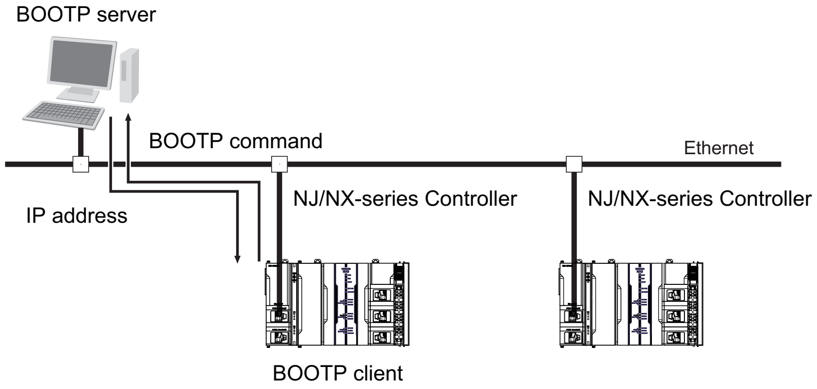
● Setting a User-specified IP Address

If you need to change the default IP address of the EtherNet/IP port or if you need to use the EtherNet/IP port with another EtherNet/IP node, set the IP address to a required value.
You cannot set IP addresses that make two EtherNet/IP ports belong to the same network.

● Automatically Obtaining an IP Address from the BOOTP Server

There are two methods to automatically obtain an IP address.

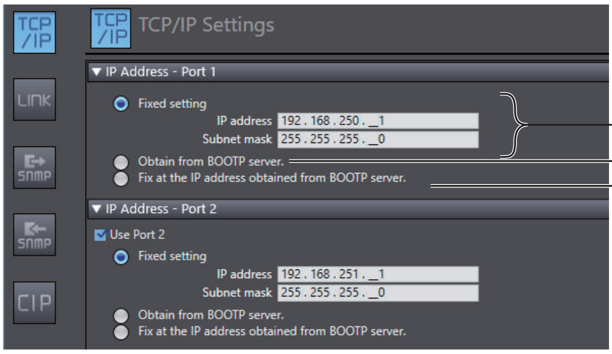
- Obtain an IP address from the BOOTP server each time the power is turned ON.
- Obtain an IP address from the BOOTP server at initial power on and set the address as a fixed IP address.



Setting IP Addresses

Use the Sysmac Studio to set an IP address of the EtherNet/IP port.

1 Select a method for setting the IP address.
Select the IP address setting method as follows on the **TCP/IP Settings** Display under **Configurations and Setup** - **CPU/Expansion Racks** - **CPU Rack: X Bus** - **Unit No.: NX-EIP201 ()** - **EtherNet/IP Port Settings**.



TCP/IP Settings

▼ IP Address - Port 1

● Fixed setting
IP address 192 . 168 . 250 . _1
Subnet mask 255 . 255 . 255 . _0
○ Obtain from BOOTP server.
○ Fix at the IP address obtained from BOOTP server.

▼ IP Address - Port 2

☑ Use Port 2
● Fixed setting
IP address 192 . 168 . 251 . _1
Subnet mask 255 . 255 . 255 . _0
○ Obtain from BOOTP server.
○ Fix at the IP address obtained from BOOTP server.

Used to set a user-specified IP address.

Used to obtain the IP address from the BOOTP server each time the power is turned ON.

Used to obtain the IP address from the BOOTP server and use the address without changing it.

The IP addresses must be set separately for EtherNet/IP ports 1 and 2.

Precautions for Correct Use

- You cannot set IP addresses that make two EtherNet/IP ports belong to the same network.
- You can set IP addresses that make EtherNet/IP ports on two or more NX-series EtherNet/IP Units that are connected by the X Bus belong to the same network. However, in that case, you cannot perform communications by specifying the destination by the IP via the NX-series EtherNet/IP Units.

2 Connect the Sysmac Studio.

3 Connect the Sysmac Studio online to the CPU Unit.
Refer to *Online Connection* on page 8-6 for the procedure to connect online.

4 Use one of the following methods to download the IP address setting that was set on the Sysmac Studio to the CPU Unit.

1) Go online with the Controller, and then select **Synchronization** from the **Controller** Menu. The data on the computer and the data in the physical Controller are compared automatically.
2) Click the **Transfer to Controller** Button.

Note Use the "synchronization" of the Sysmac Studio to upload and download data.
Note Since only the IP address for the NX-series EtherNet/IP Unit is set here, do not select **Do not transfer the following. (All items are not transferred.)** Check Box in the Synchronization Window on the Sysmac Studio.

5 After the IP address settings are downloaded, the IP address is reflected in the NX-series EtherNet/IP Unit as follows:

- **Setting a User-specified IP Address**

  After the IP address settings are downloaded, the set IP address is automatically reflected in the NX-series EtherNet/IP Unit.

- **Obtaining the IP Address from the BOOTP Server Each Time the Power Is Turned ON**

  After the IP address settings are downloaded, the IP address from the BOOTP server is automatically reflected in the NX-series EtherNet/IP Unit.

  Each time the power supply is turned ON, the IP address from the BOOTP server is automatically reflected in the NX-series EtherNet/IP Unit.

Additional Information

If the Unit cannot obtain the IP address from the BOOTP server or the obtained IP address is not correct, select the **Fixed setting** Option in the **IP Address** Area and manually set the IP address, subnet mask, and default gateway.
Requests to the BOOTP server for an IP address will continue if connecting to the BOOTP server fails.

- **Obtaining the IP Address from the BOOTP Server When the Power Is Turned ON and Fixing at It**

  After the IP address settings are downloaded, the IP address from the BOOTP server is automatically reflected in the Controller and set for **Fixed setting**.

Additional Information

- The **TCP/IP Settings** Display is not updated even if the IP address is obtained normally from the BOOTP server.
  To check the IP address that was obtained from the BOOTP server, upload the project from the NJ/NX-series Controller and check the Controller Status Pane.
- If you cannot obtain the IP address from the BOOTP server, the **Fix at the IP address obtained from BOOTP server** Option is selected on the **TCP/IP Settings** Display.
  To stop obtaining the IP address from the BOOTP server, select **Fixed setting** in the **IP Address** Area and manually set the IP address, subnet mask, and default gateway.
- If the Controller power supply is turned OFF and then ON after the IP address was not normally obtained from the BOOTP server, the setting remains at **Fix at the IP address obtained from BOOTP server**.
- After you select **Fix at the IP address obtained from BOOTP server** and download the IP address from the BOOTP server, the EtherNet/IP port IP address setting is automatically set to **Fixed setting**. Therefore, the IP address will not match when the program is verified on the Sysmac Studio.
- To use the Packet Filter, you must allow packets (UDP:68) used for BOOTP. Refer to *8-4-4 Settings for Devices That Access the Controller* on page 8-17 for details on the settings.

Online Connection

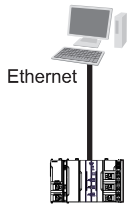
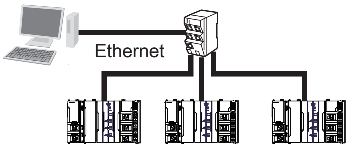
Connect the Sysmac Studio online to the CPU Unit.

Additional Information

For the procedure to go online to the CPU Unit from the Sysmac Studio, refer to *Online Connections to a Controller* in the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)*.

● Types of Connection between the CPU Unit and Computer That Runs the Sysmac Studio

The CPU Unit and the computer that runs Sysmac Studio are connected via Ethernet as shown below:

Direct Connection via Ethernet (1:1 Connection with Auto IP)	Ethernet Connection via a Hub (1:N Connection)
 *1. An Ethernet switch is not necessarily required. *2. You can use a straight or cross Ethernet cable to connect. *3. 1:1 connection is supported only for the built-in EtherNet/IP port 1 on the NX502 CPU Units.	 *1. An Ethernet switch is required to connect. Refer to *5-1-4 Precautions for Ethernet Switch Selection* on page 5-4 for details.

Precautions for Correct Use

If you connect the computer that runs the Sysmac Studio to the EtherNet/IP port on the NX-series EtherNet/IP Unit, you cannot use direct connection via Ethernet. Use the Ethernet connection via a hub through an Ethernet switch. In that case, you must specify the destination IP address.

Precautions for Correct Use

If there is more than one node with the same IP address in the EtherNet/IP network, the EtherNet/IP port will connect to the node that is detected first.
Note that an IP Address Duplication Error will not be detected in this case.

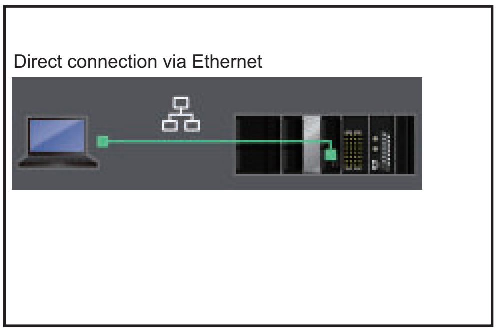
● Online Connection Procedure

Connect the CPU Unit and the computer that runs the Sysmac Studio via Ethernet, and then perform the following procedure.

1 Select **Controller** - **Communications Setup** and click the **OK** Button in the Sysmac Studio Project Window.

1:1 Connection

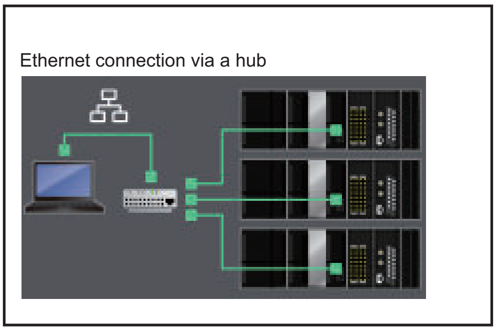
Direct Connection



Direct connection via Ethernet

1:N Connection

Ethernet Connection



Ethernet connection via a hub

Additional Information

If there is any error in the set IP address, the CPU Unit behaves as follows:

- The NET RUN indicator on the CPU Unit does not light and the NET ERR indicator flashes red. Indicators will indicate the status of each EtherNet/IP port.
- An *IP Address Setting Error* is recorded in the event log.

Precautions for Correct Use

- If the IP address is duplicated or not set correctly, communications are not possible via the EtherNet/IP network. Set the IP address again.
- The IP address range shown below is used by the system and cannot be specified.
  169.254.0.0 to 169.254.255.255
  192.168.255.0 to 192.168.255.255
- Due to Ethernet restrictions, you cannot specify the following IP addresses.
  a) An IP address that is all 0's or all 1's
  b) IP addresses that start with 127, 0, or 255 (decimal)
  c) IP addresses that have a host ID that is all 0's or all 1's
  d) Class-D IP addresses (224.0.0.0 to 239.255.255.255)
  e) Class-E IP addresses (240.0.0.0 to 255.255.255.255)

● Connecting from a Saved Project

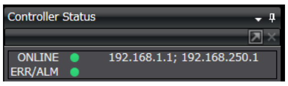
The connection configuration that is set (via EtherNet/IP) is saved in the project.

When you open a saved project on the Sysmac Studio, you can connect to the EtherNet/IP network without redoing the settings.

Checking the Current IP Address

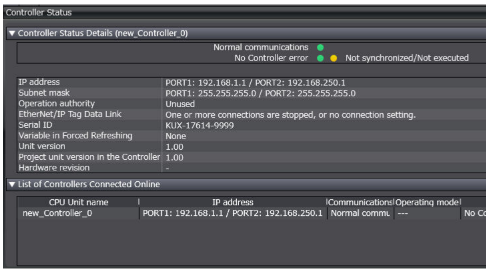
The current IP address can be confirmed in the Controller Status Pane of the Sysmac Studio, whether it is manually set or obtained from the BOOTP server.

- Basic Controller Status Pane



ONLINE ● 192.168.1.1; 192.168.250.1
ERR/ALM ●

- Controller Status Pane with Details


Controller Status
▼ Controller Status Details (new_Controller_0)
▼ List of Controllers Connected Online

Normal communications ●
No Controller error ● ● Not synchronized/Not executed

IP address	PORT1: 192.168.1.1 / PORT2: 192.168.250.1
Subnet mask	PORT1: 255.255.255.0 / PORT2: 255.255.255.0
Operation authority	Unused
EtherNet/IP Tag Data Link	One or more connections are stopped, or no connection setting.
Serial ID	KUX-17614-9999
Variable in Forced Refreshing	None
Unit version	1.00
Project unit version in the Controller	1.00
Hardware revision	-

CPU Unit name	IP address	Communications	Operating mode	
new_Controller_0	PORT1: 192.168.1.1 / PORT2: 192.168.250.1	Normal commu	---	No Co

Additional Information

- If the IP address of the EtherNet/IP port is not registered due to the following reasons, the IP address field shows "0.0.0.0".
  - The IP address was not obtained from the BOOTP server.
  - The EtherNet/IP port is disabled. Refer to *7-1 **TCP/IP Settings** Display* on page 7-2 for details on the settings for the IP address of the EtherNet/IP port.

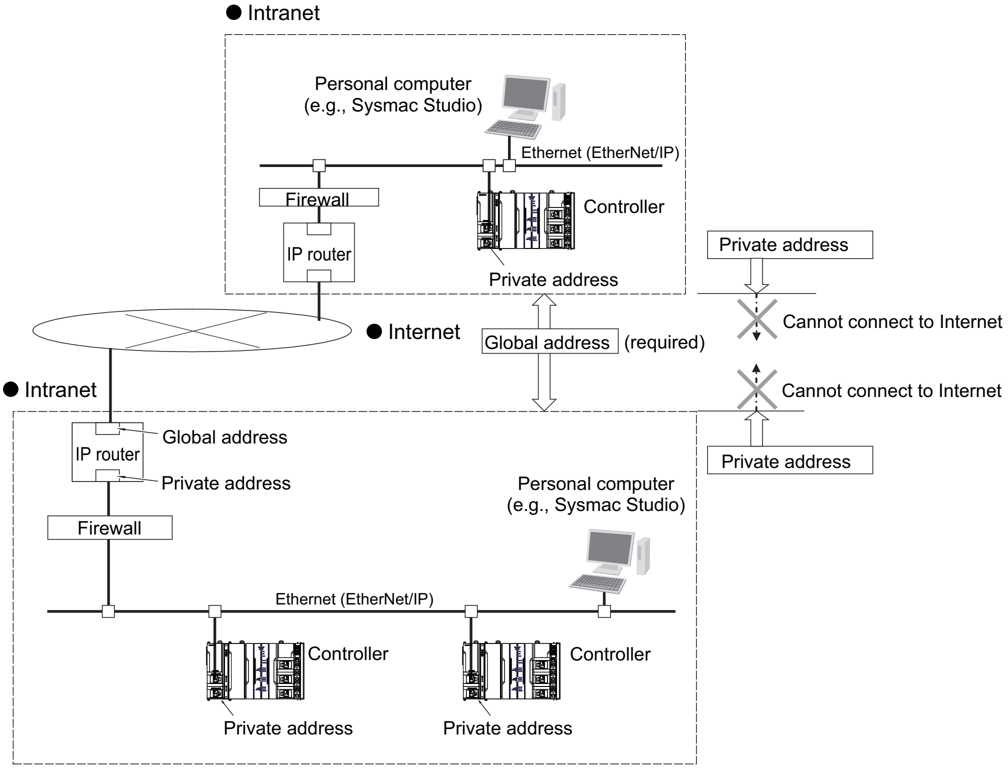
8-1-3 Private and Global Addresses

Private and Global Addresses

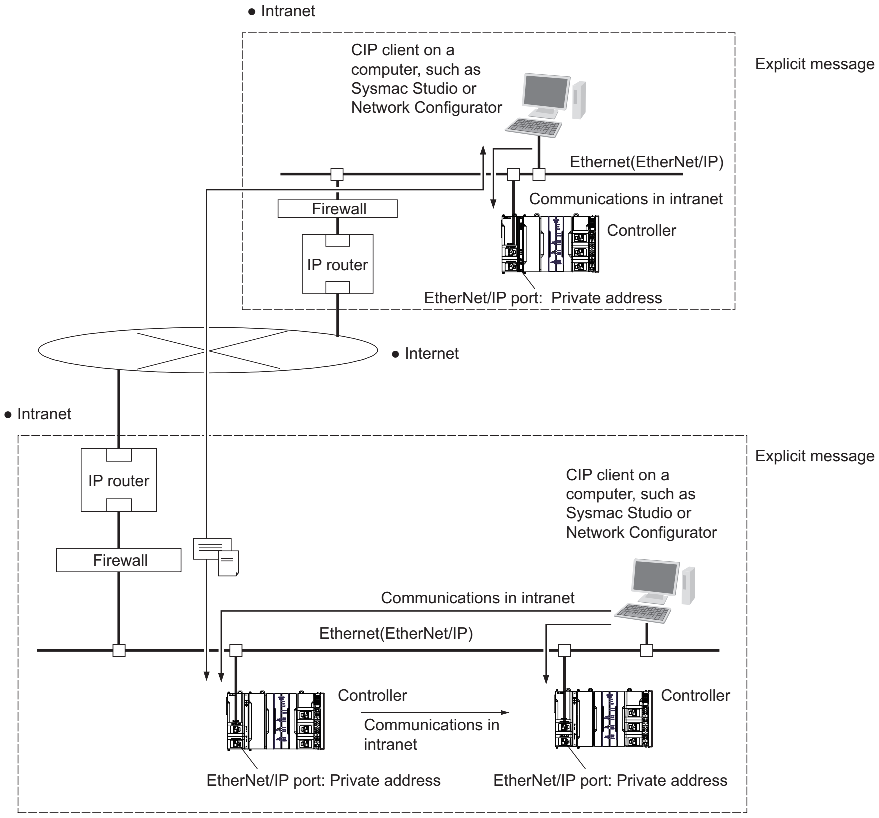
There are two kinds of IP addresses, private and global.

Global address	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 billion can be allocated worldwide.
Private address	These are IP addresses for Intranet (LAN) use. Direct connection to the Internet is not possible. 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) interfaced with the Internet. All other nodes in the intranet, which includes the EtherNet/ IP port, are allocated private addresses.



Using a Private Address for the EtherNet/IP Port


● Intranet
CIP client on a computer, such as Sysmac Studio or Network Configurator
Explicit message
Ethernet(EtherNet/IP)
Firewall
Communications in intranet
Controller
IP router
EtherNet/IP port: Private address
● Internet
● Intranet
Explicit message
IP router
CIP client on a computer, such as Sysmac Studio or Network Configurator
Firewall
Communications in intranet
Ethernet(EtherNet/IP)
Controller
Controller
Communications in intranet
EtherNet/IP port: Private address
EtherNet/IP port: Private address

● Conditions for Communications Applications

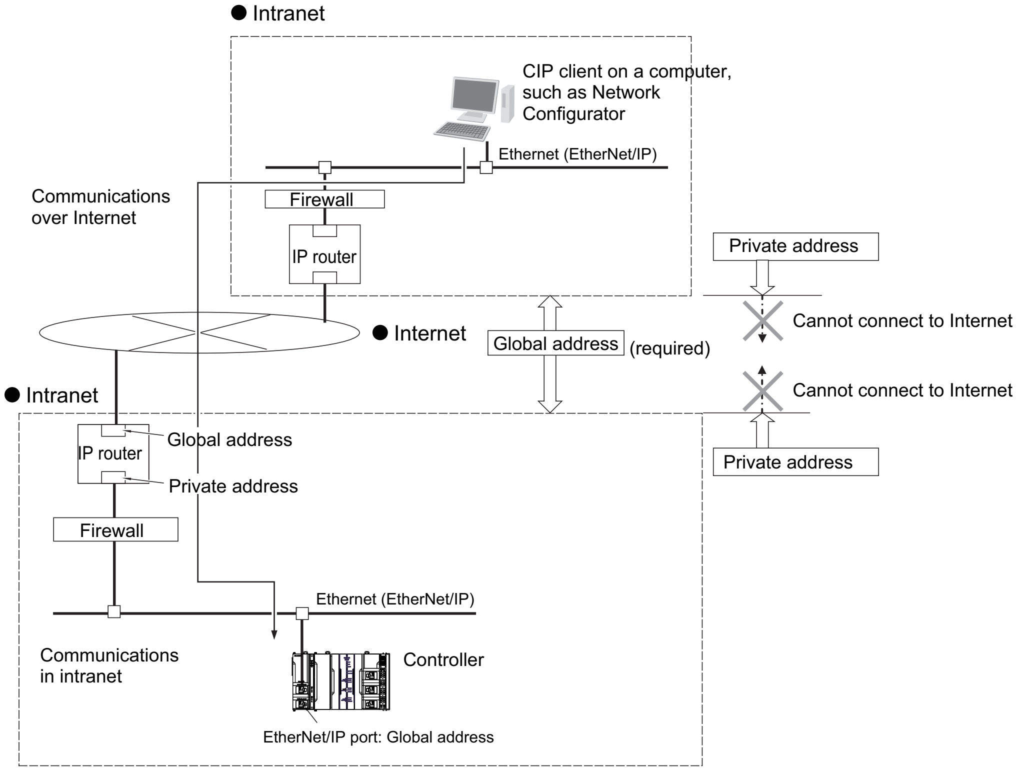
If the EtherNet/IP port uses a private address, you can use explicit message communications service under the following conditions.

- The explicit message communications service can be executed on the intranet between 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 port that has a private address.
  Explicit message communications are also not possible over the Internet between EtherNet/IP ports with private addresses.

Precautions for Correct Use

- To set up an intranet through a global address involves network security considerations. Be sure to consult with a network specialist in advance and consider installation of a firewall.
- Some communication applications may not be available depending on the firewall settings made by the communications company. If there are communication applications that cannot be used, be sure to check with your communications company.
- When sending and receiving data over a global address, use secure communications, such as secure socket communications and OPC UA, that ensure confidentiality and integrity.

Using a Global Address for the EtherNet/IP Port



● Conditions for Communications Applications

You can use the explicit message communications service over the Internet under the following conditions.

- 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 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 because it is prohibited by a firewall in the communications path.

Precautions for Correct Use

- To set a global IP address for an EtherNet/IP port involves network security considerations. It is recommended that the user contract with a communications company for a dedicated line, rather than for 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.
- Some communication applications may not be available depending on the firewall settings made by the communications company. If there are communication applications that cannot be used, be sure to check with your communications company.
- When sending and receiving data over a global address, use secure communications, such as secure socket communications and OPC UA, that ensure confidentiality and integrity.

8-2 Default States of TCP/UDP Ports and the Changing Procedure

The following table shows the applications that use TCP/UDP ports for which a user can change the port state, port numbers, default port states, usages, and how to change a port from open to close and close to open.
Refer to *A-7 TCP/UDP Port Numbers Used for the NX-series EtherNet/IP Unit* on page A-55 for information on all TCP/UDP ports of the NX-series EtherNet/IP Unit.

Application	UDP port number	TCP port number	Default port state	Usage	How to change from open to close	How to change from close to open
SNMP	161	---	Close	Used when using the SNMP agent.	On the Sysmac Studio, select **EtherNet/IP Port Settings** - **SNMP Settings**, and then select **Do not use** for **SNMP service**.	On the Sysmac Studio, select **EtherNet/IP Port Settings** - **SNMP Settings**, and then select **Use** for **SNMP service**.
HTTPS server	---	443	Open	Used for communications with the Sysmac Studio.	Use the Packet Filter. [*1]	Use the Packet Filter.
Sysmac Studio	9600	---	Open	Used for communications with the Sysmac Studio.	Use the Packet Filter. [*2]	Use the Packet Filter.
CIP messages	44818	44818	Open	Used for the CIP messages.	On the Sysmac Studio, select **EtherNet/IP Port Settings** - **CIP Settings**, and then select **Do not use** for **CIP Message Server**.	On the Sysmac Studio, select **EtherNet/IP Port Settings** - **CIP Settings**, and then select **Use** for **CIP Message Server**.

*1. Closing the port may prevent communications with the Sysmac Studio and the NA-series HMI. Refer to *Troubleshooting when support software cannot go online* in the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* on how to make corrections.

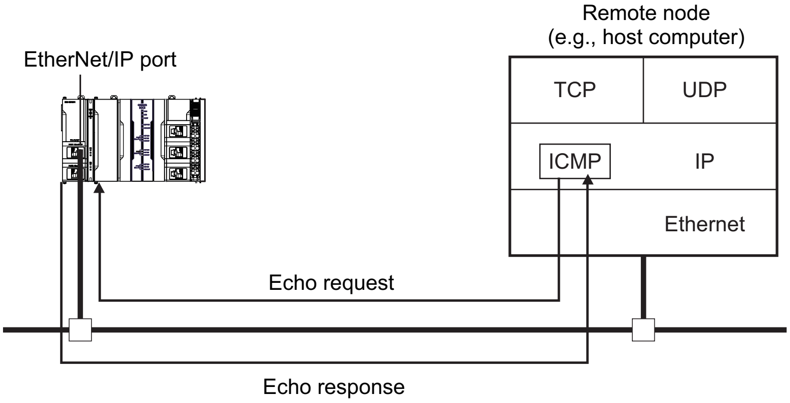
*2. Closing the port may prevent communications with the Sysmac Studio. Refer to *Troubleshooting When You Cannot Go Online from the Sysmac Studio* in the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* on how to make corrections.

8-3 Testing Communications

If the basic settings (in particular the IP address and subnet mask) are made correctly for the EtherNet/IP port, then it is 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 port.

8-3-1 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 communications are normal. The PING command uses the ICMP echo request and response. The echo response packet is automatically returned in the ICMP.
The PING command is normally used to check the connections of remote nodes when you set up a network. The EtherNet/ IP port supports both the ICMP echo request and response functions.
If the remote node returns a normal response to the PING command, then the node is physically connected correctly and Ethernet node settings are correct.



8-3-2 Using the PING Command

The EtherNet/IP port automatically returns an echo response packet in response to an echo request packet by a PING command sent by another node (e.g., host computer).

Precautions for Correct Use

When the **Use** Option is selected for Packet Filter of the EtherNet/IP port, PING command cannot be received unless **icmp** is selected for **Protocol** of Pacekt Filter settings. Refer to *Packet Filter* on page 7-7 for details on the settings.

8-3-3 Host Computer Operation

The PING command can be executed from the host computer to an EtherNet/IP port.
The following example shows how to use the PING command in the host computer.

Application 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.

Additional Information

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

```
$ ping   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,   0 packets   received,   100% packets   loss
$
```

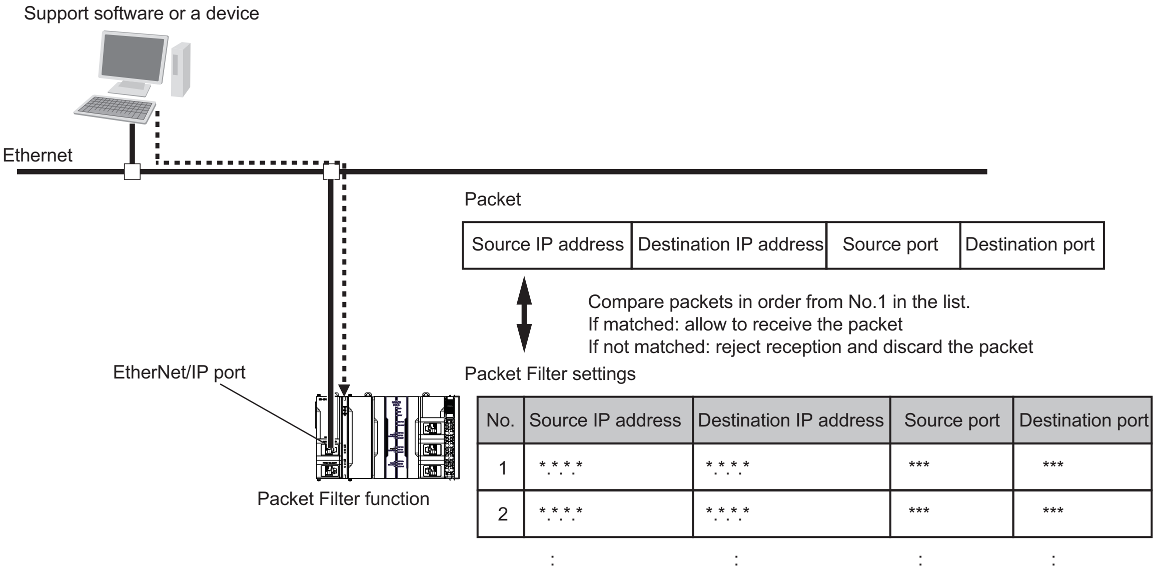
Refer to the command reference manual for your computer's OS for details on using the PING command.

8-4 Packet Filter

This section provides an overview of Packet Filter, explains the specifications, settings, and usage examples.

8-4-1 Introduction to Packet Filter

IP packets are filtered in the receive processing at the EtherNet/IP ports.
Packet Filter settings are configured in the permit list. If **any** is set in Packet Filter, all packets are allowed. If a value other than **any** is set in Packet Filter, the received packet is compared with Packet Filter settings. When a matching packet is received, reception is permitted. When a non-matching packet is received, reception is prohibited and the packet is discarded. Packet Filter settings include the source IP address, destination IP address, and TCP/UDP port number.



Source IP address	Destination IP address	Source port	Destination port

Compare packets in order from No.1 in the list.
If matched: allow to receive the packet
If not matched: reject reception and discard the packet

Packet Filter settings

No.	Source IP address	Destination IP address	Source port	Destination port
1	*.*.*.*	*.*.*.*	***	***
2	*.*.*.*	*.*.*.*	***	***
	:	:	:	:

Precautions for Correct Use

- If you cannot go online with the Sysmac Studio because of forgetting the registered IP address, you can disable this function tentatively by starting the Unit in Safe Mode. Refer to *Troubleshooting When You Cannot Go Online from the Sysmac Studio* in the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* for details.
- The Packet Filter function supports the stateful inspection. Therefore, for DNS, DB connection services, and communication instructions, where the Controller is specified as a client, you do not need to add the responses from other devices to Packet Filter settings.

8-4-2 Packet Filter Specifications

The specifications for Packet Filter are given below.

Item	Specification	Remarks
Filtering system	Permit list	The system enables reception of packets registered in Packet Filter settings and prohibits reception of unregistered packets.

Item	Specification	Remarks
Location to perform filtering	Receive processing at the EtherNet/IP port (The setting can be configured for each EtherNet/IP port.)	• No filtering is applied to the sending process of the EtherNet/IP port. • Stateful inspection is supported.
Number of Packet Filter tables	32	
Settings for Packet Filter tables	• Source IP Address/Mask • Destination IP Address/Mask • Protocol (tcp, udp, igmp, icmp) If tcp or udp is selected for Protocol, specify the source port and destination port.	Range specification can be set for the IP address and TCP/UDP ports.

8-4-3 Packet Filter Settings

For details on Packet Filter settings, refer to *Packet Filter* on page 7-7.

Additional Information

- For set values of **Destination Port** for each communication, refer to *8-4-4 Settings for Devices That Access the Controller* on page 8-17.
- Refer to *Case Where Packet Filter Is Used* in the *NJ/NX-series CPU Unit Built-in EtherNet/IP Port User’s Manual (Cat. No. W506)* for set values for each case of using the Packet Filter.

8-4-4 Settings for Devices That Access the Controller

This section shows the set values of Packet Filter for each device that accesses the Controller.

Settings for Connecting Sysmac Studio

The following table shows the setting values for the destination port of Packet Filter when the Sysmac Studio is connected.

Connection type[1]	**Destination port settings**				
	Protocol	**Destination Port Specification Method**	**Destination Port Range Specification**	**Destination Port Start Number**	**Destination Port End Number**
Ethernet connection via a hub	tcp	Port specification	No check.	443	---

[1] Select **Controller** – **Communications Setup** – **Connection type** on the Sysmac Studio to make this setting.

Settings for Connecting Support Software Other Than Sysmac Studio

The settings for connecting the Support Software other than Sysmac Studio are as follows.

Support Software	**Connection type**	**Destination port settings**				
		Protocol	**Destination Port Specification Method**	**Destination Port Range Specification**	**Destination Port Start Number**	**Destination Port End Number**
Network Configurator for EtherNet/IP	**Ethernet I/F**	tcp*Settings for Connecting Support Software Other Than Sysmac Studio* on page 8-17	Port specification	No check.	44818	---
		udp[1]	Port specification	No check.	44818	---
		icmp*Settings for Connecting Support Software Other Than Sysmac Studio* on page 8-17	---	---	---	---
Sysmac Conrtoller Log Upload Tool	**Ethernet connection via a hub**	Same settings as for Sysmac Studio. Refer to *Settings for Connecting Sysmac Studio* on page 8-17 for settings for the Sysmac Studio. Allow tcp: 443 for the destination port.				

[1] When filtering by IP address is used, allow the following IP addresses.
Source IP address: Computer's IP address, Destination IP address: Local broadcast to the computer's network (When the computer's IP address is 192.168.250.100/24, allow 192.168.250.255.)

Settings for Connecting a Programmable Terminal

The settings for connecting Programmable Terminals are as follows.

Programmable Terminal	Destination port settings				
	Protocol	Destination Port Specification Method	Destination Port Range Specification	Destination Port Start Number	Destination Port End Number
NA-series	tcp	Port specification	No check.	80 or 443*1	---

*1. For NA Runtime version 1.161 and NA5 system program version 10.0.0 or higher, set the destination port start number to 443.

Settings for Each Communications Protocol

The settings for each communications protocol are as follows.

Communications protocol	Destination port settings				
	Protocol	Destination Port Specification Method	Destination Port Range Specification	Destination Port Start Number	Destination Port End Number
BOOTP client	udp	Port specification	No check.	68	---
SNMP agent	udp	Port specification	Checked.	161*1	162*1

*1. If the port number has been changed, the new port number must be set.

Settings for Using EtherNet/IP Communications

Make the following settings to use EtherNet/IP communications.

Communications	Communications protocol	Condition	Destination port settings				
			Protocol	Destination Port Specification Method	Destination Port Range Specification	Destination Port Start Number	Destination Port End Number
CIP messages	UCMM	Server	tcp	Port specification	No check.	44818	---
			icmp*1	---	---	---	---
	Class3	Server	tcp	Port specification	No check.	44818	---
			icmp*1	---	---	---	---
Tag data links	Class1	Originator	igmp*2	---	---	---	---
		Target	tcp	Port specification	No check.	44818	---
			icmp*3	---	---	---	---
CIP Safety communications	Class0	Originator	igmp*2	---	---	---	---
		Target	tcp	Port specification	No check.	44818	---

*1. Select this if CX-Compolet/SYSMAC Gateway is a client.

*2. Select this for Multicast.

*3. Select this when SYSMAC Gateway is the originator.

8-5 Port Forward via NX-series EtherNet/IP Units

The NX-series EtherNet/IP Unit supports IP routing. This enables the following three types of port forward via the NX-series EtherNet/IP Units between the NX502 CPU Unit and external devices and between multiple external devices.

- The CPU Unit becomes the client and accesses the server of an external device via the EtherNet/IP port on the NX-series EtherNet/IP Unit. In this case, the port forward is performed between the CPU Unit and NX-series EtherNet/IP Unit.
- The external device becomes the client and accesses the server function in the CPU Unit via the EtherNet/IP port on the NX-series EtherNet/IP Unit. In this case, the port forward is performed between the NX-series EtherNet/IP Unit and the CPU Unit.
- The port forward is performed between the built-in EtherNet/IP port on the CPU Unit and the EtherNet/IP port on the NX-series EtherNet/IP Unit. Or, the port forward is performed between EtherNet/IP ports on multiple NX-series EtherNet/IP Units.

When you use these types of port forward, you must select the **Use** Option for **IP Forward** from **EtherNet/IP Port Settings** - **TCP/IP Settings** - **Port Forward** on the Sysmac Studio.

Also, IP addresses must be set so that each Unit does not have the same network address.

8-5-1 Port Forward on Which a CPU Unit Is a Client

When a CPU Unit becomes a client and accesses a server on an external device with special instructions such as FTP client instructions or socket communications instructions, the access can be made through the EtherNet/IP port on the NX-series EtherNet/IP Unit instead of the built-in EtherNet/IP port on the CPU Unit.

The IP packets are transferred from the CPU Unit to the EtherNet/IP port on the NX-series EtherNet/IP Unit by specifying the IP address of the server on the external device with each special instruction.

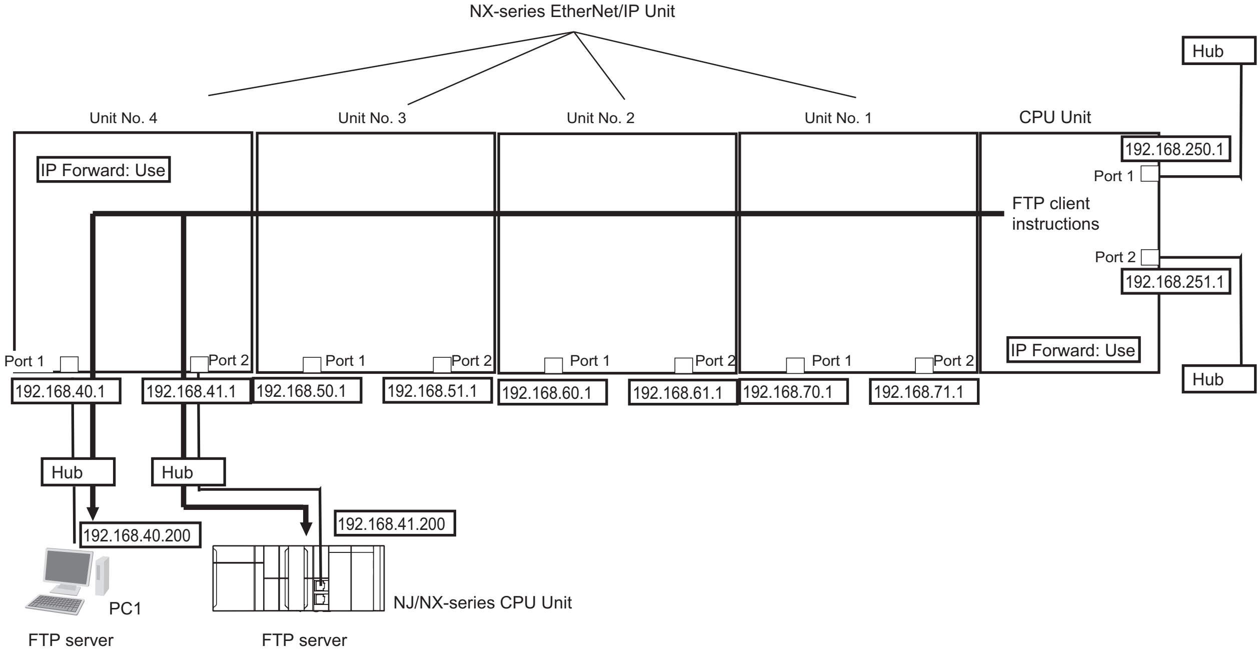
Also, the response IP packets from the external device that are received by the NX-series EtherNet/IP Unit are transferred to the CPU Unit.

The applicable FTP communications mode depends on the connection configuration of the communications network.

Case	Network connection configuration	Applicable FTP communications mode
Case 1	When accessing from the EtherNet/IP port on the NX-series EtherNet/IP Unit that is connected to the CPU Unit via the Ethernet port on the computer to the FTP server, then via the built-in EtherNet/IP port on the other CPU Unit to the FTP server in order.	Passive Mode
Case 2	When accessing from the built-in EtherNet/IP port on the CPU Unit via the EtherNet/IP port on the NX-series EtherNet/IP Unit that is connected to the other CPU Unit to the FTP server on the other CPU Unit.	Active Mode

Case 1

As shown in the following figure, the FTP servers are accessed from the EtherNet/IP port on the NX-series EtherNet/IP Unit that is connected to the CPU Unit via the Ethernet port on the computer, then via the built-in EtherNet/IP port on the other CPU Unit in order.

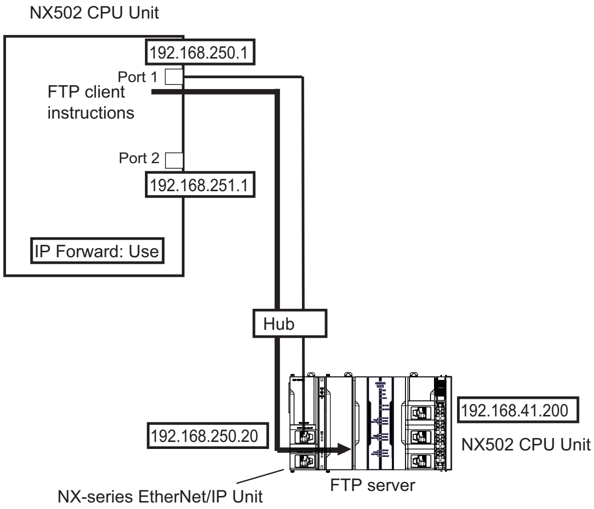


When the CPU Unit executes the FTP client instruction specifying PC1 with IP address 192.168.40.200, an IP packet is transferred to PC1, which is the FTP server, via the EtherNet/IP port 1 on the NX-series EtherNet/IP Unit with unit number 4 in the same network segment.
You need to set the FTP communications mode to Passive Mode for this configuration. Active Mode is not applicable. The details of the settings are as follows.

FTP communications mode	Setting
Active Mode	Not applicable.
Passive Mode	• Set **IP Forward** in **Port Forward** to **Use** for both the CPU Unit and the NX-series EtherNet/IP Unit. • Execute the FTP client instruction in Passive Mode.

Case 2

As shown in the following figure, the FTP server on the other CPU Unit is accessed from the built-in EtherNet/IP port on the CPU Unit via the EtherNet/IP port on the NX-series EtherNet/IP Unit that is connected to the other CPU Unit.

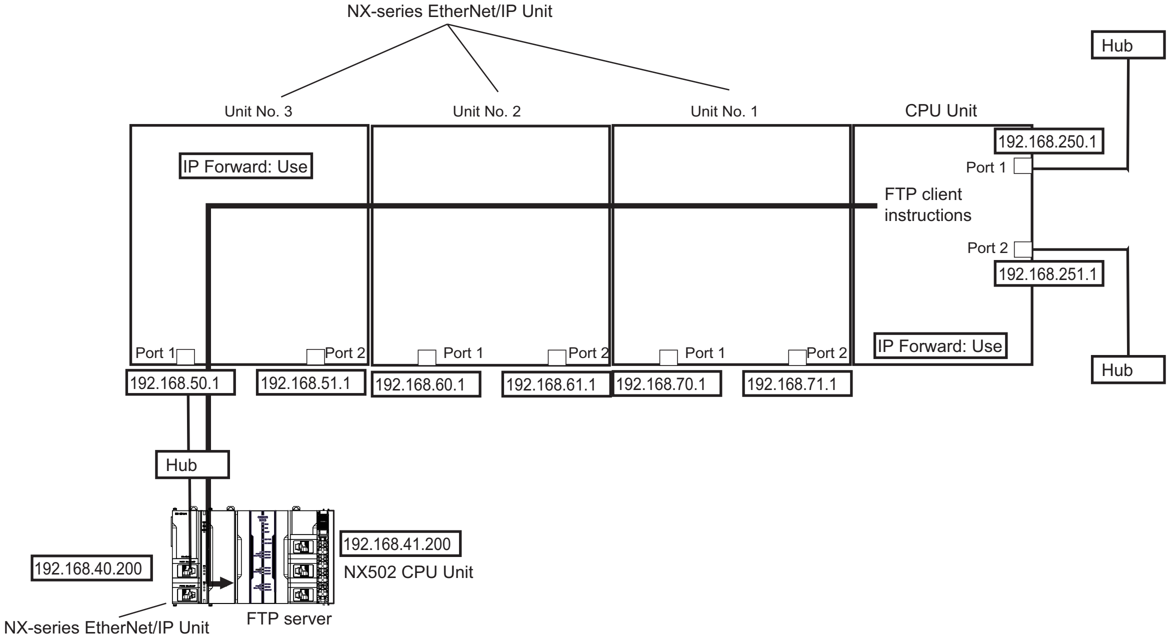


When the CPU Unit executes the FTP client instruction specifying the NX5 CPU Unit with IP address 192.168.41.200, an IP packet is transferred to the NX5 CPU Unit, which is the FTP server, via the EtherNet/IP port 1 on the NX-series EtherNet/IP Unit in the same network segment.
You need to set the FTP communications mode to Active Mode for this configuration. Passive Mode is not applicable. The details of the settings are as follows.

FTP communications mode	Setting
Active Mode	• Set **IP Forward** in **Port Forward** to **Use** for both CPU Units and the NX-series EtherNet/IP Unit on the remote node. • Execute the FTP client instruction in Active Mode. • Set **TCP/UDP Port Transfer** of the remote node NX-series EtherNet/IP Unit as follows. Port: Port1 Protocol: TCP Port Number: 20
Passive Mode	Not applicable.

Precautions for Correct Use

As in the following figure, if the connection was configured so that packets are transferred via the EtherNet/IP port on the NX-series EtherNet/IP Unit on both the FTP client and FTP server sides, the FTP communications cannot be performed in either of Active Mode or Passive Mode.



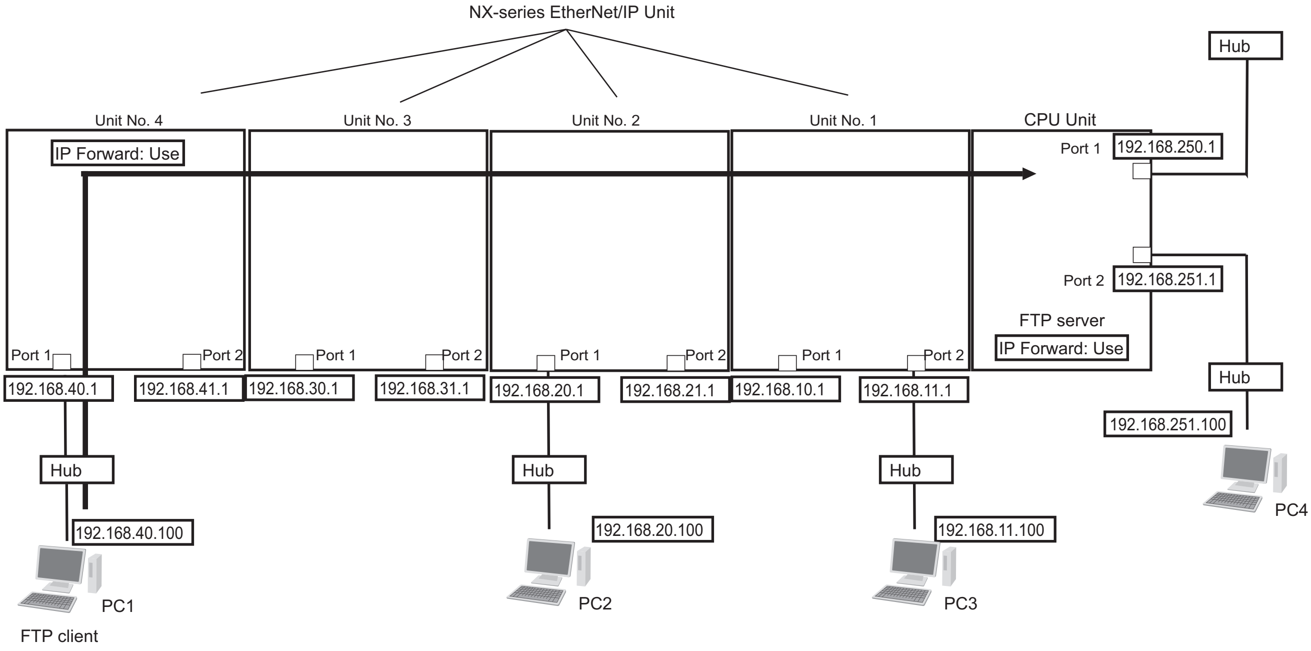
8-5-2 Port Forward on Which an External Device Is a Client

In port forward where the external device is a client, an access from an external device such as a computer is made to the server of the CPU Unit through the EtherNet/IP port on the NX-series EtherNet/IP Unit. In this case, when the TCP or UDP port that is used with TCP/IP communications is specified, TCP or UDP frames received by the NX-series EtherNet/IP Unit are transferred to the CPU Unit. The TCP and UDP ports to be used must be specified for each EtherNet/IP port on the NX-series EtherNet/IP Units. The external device that is the client must specify the IP address of the EtherNet/IP port on the NX-series EtherNet/IP Unit to pass through.

To specify the TCP and UDP ports, select **EtherNet/IP Port Settings** - **TCP/IP Settings** - **TCP/UDP Port Transfer** on the Sysmac Studio.

If the **Do not use** Option for **IP Forward** is selected under **EtherNet/IP Port Settings** - **TCP/IP Settings** - **Port Forward** on the Sysmac Studio, the port forward is not performed. The frame received by the NX-series EtherNet/IP Unit is discarded.

The following figure shows the case where the IP address 192.168.40.1 of the EtherNet/IP port 1 on the NX-series EtherNet/IP Unit with unit number 4 is specified from the FTP client of PC1. The frame received by the NX-series EtherNet/IP Unit is transferred to the CPU Unit.



The following settings are required for this configuration.

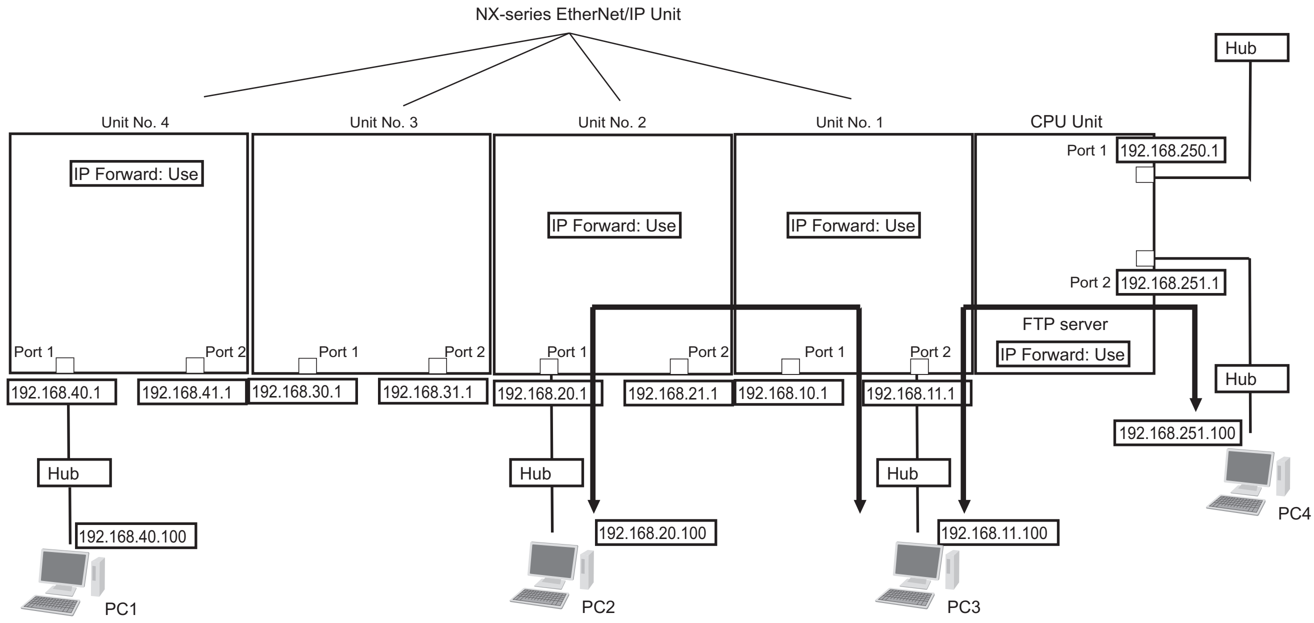
FTP communications mode	Setting
Active Mode	• Set **IP Forward** in **Port Forward** to **Use** for both the CPU Unit and the NX-series EtherNet/IP Unit. • PC1, which is the FTP client, is set to Active Mode. • Set **TCP/UDP Port Transfer** of the NX-series EtherNet/IP Unit with unit number 4 connected to PC1 as follows. Port: Port1 Protocol: TCP Port Number: 21
Passive Mode	Not applicable

8-5-3 Port Forward Between CPU Unit and NX-series EtherNet/IP Unit or Between EtherNet/IP Ports on NX-series EtherNet/IP Units

The port forward can be performed between the built-in EtherNet/IP port on the CPU Unit and the EtherNet/IP port on the NX-series EtherNet/IP Unit or between multiple NX-series EtherNet/IP Units. If the network addresses of the Units are duplicated, the IP router table settings are required. If there are no duplicates, no IP router table settings are required.

The following figure shows communications between PC2 and PC3 and between PC3 and PC4.

In this case, PC2 needs to make route settings to PC3 192.168.11.100. Similarly, PC3 needs to make route settings to PC2 192.168.20.100 and PC4 192.168.251.100, and PC4 needs to make route settings to PC3 192.168.11.100.


NX-series EtherNet/IP Unit
Hub
Unit No. 4
Unit No. 3
Unit No. 2
Unit No. 1
CPU Unit
Port 1
192.168.250.1
IP Forward: Use
IP Forward: Use
IP Forward: Use
Port 2
192.168.251.1
FTP server
IP Forward: Use
Port 1
Port 2
Port 1
Port 2
Port 1
Port 2
Port 1
Port 2
Hub
192.168.40.1
192.168.41.1
192.168.30.1
192.168.31.1
192.168.20.1
192.168.21.1
192.168.10.1
192.168.11.1
192.168.251.100
Hub
Hub
Hub
PC4
192.168.40.100
192.168.20.100
192.168.11.100
PC1
PC2
PC3

9

Tag Data Link Functions

9-1 Introduction to Tag Data Links

9-1-1 Tag Data Links

Tag data links enable cyclic tag data exchanges on an EtherNet/IP network between Controllers or between Controllers and other devices. Variables are assigned to tags. (You can also assign I/O memory addresses to tags.)

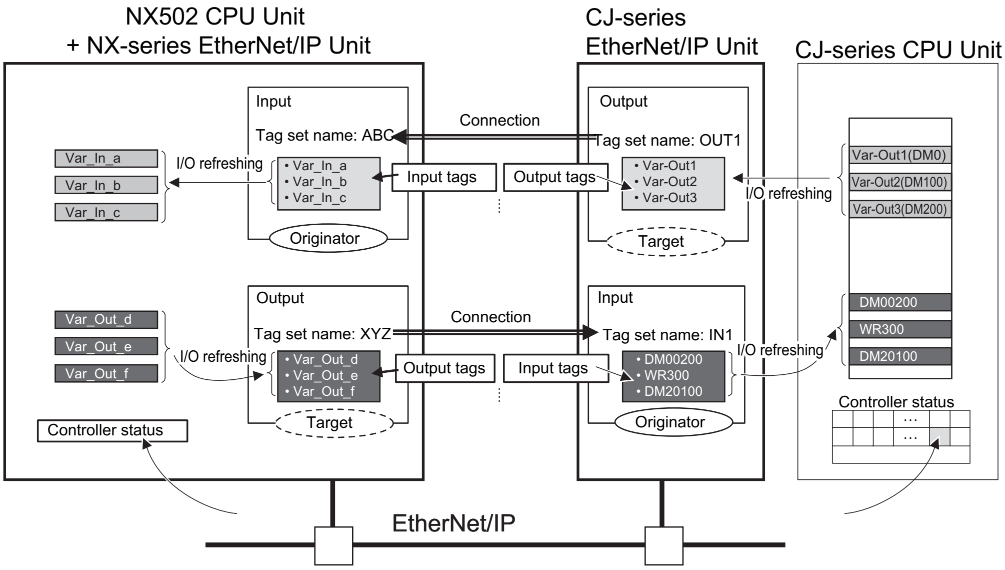
The settings for tag data links are made with the Network Configurator. Refer to *9-2 Setting Tag Data Links* on page 9-15 for information on how to make the settings.

Additional Information

You can also use the Sysmac Studio to set the tag data links.
Refer to *A-3 Use the Sysmac Studio to Set the Tag Data Links (EtherNet/IP Connections)* on page A-6 for details on setting the tag data links on the Sysmac Studio.

With a tag data link, one node requests the connection of a communications line to exchange data with another node.

The node that requests the connection is called the originator, and the node that receives the request is called the target.



For communications between Controllers, the connection information is set in the EtherNet/IP port of the Controller that receives (consumes) the data (i.e., the originator).

Additional Information

For communications between a Controller and an I/O device, the connection information is set in the 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 *A-4 EDS File Management* on page A-43 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.

Precautions for Correct Use

- Select the **Use** Option for the CIP message server of the EtherNet/IP port. If the **Do not use** Option for the CIP message server is selected, tag data links cannot be performed. For the details on the settings, refer to *CIP Message Server* on page 7-15.
- If the **Use** Option is selected for Packet Filter of the EtherNet/IP port, make sure to permit packets to be used for tag data links. If they are not permitted, tag data links are not possible. For the details on the settings, refer to *Packet Filter* on page 7-7.
- During tag data link communications, data transfer between the CPU Unit and the X Bus Unit is performed during I/O refresh of the primary periodic task. I/O refresh processing can be assigned to the priority-16 periodic task for each tag set in the settings for exclusive control of variables in tasks. Refer to *I/O Refreshing of X Bus Function Module* in the *NJ/NX-series CPU Unit Software User's Manual (Cat. No. W501)* for details on task execution time and I/O refreshing.

9-1-2 Data Link Data Areas

Tags

A tag is a unit that is used to exchange data with tag data links.

Data is exchanged between the local network variables and remote network variables specified in the tags or between specified I/O memory areas.

Precautions for Correct Use

To maintain concurrency in the values of network variables that are assigned to tags, you must set refreshing tasks.
Refer to *9-1-7 Concurrency of Tag Data Link Data* on page 9-12 for details.

Tag Sets

When a data link connection is established, one or more tags (up to eight tags including Controller status) are configured as a collective set of tags for the connection. This is called a tag set. Each tag set represents a unit of data for one tag data link connection.

Tag data links are therefore created through a connection between one tag set and another tag set. A tag set name must be set for each tag set.

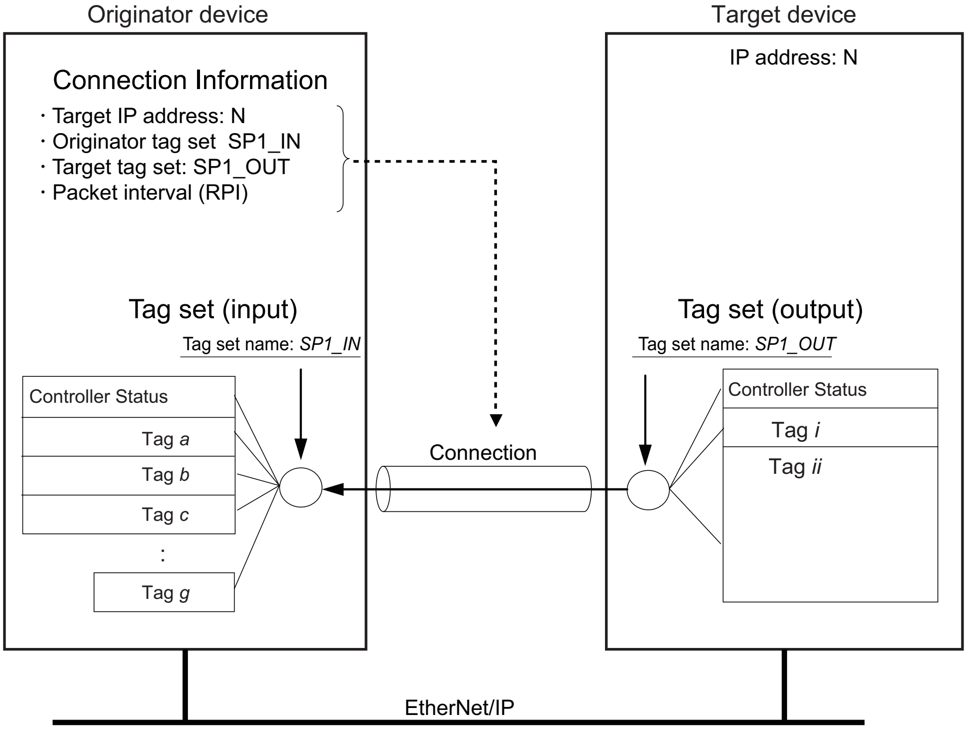
Note A connection is used to exchange data as a unit within which data concurrency is maintained.
Thus, data concurrency is maintained for all the data exchanged for one or more tags in one tag set.

Precautions for Correct Use

Data with tags is exchanged in the order that the tags are registered in the tag set. Register the tags in the same order of the input and output tag sets.

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.

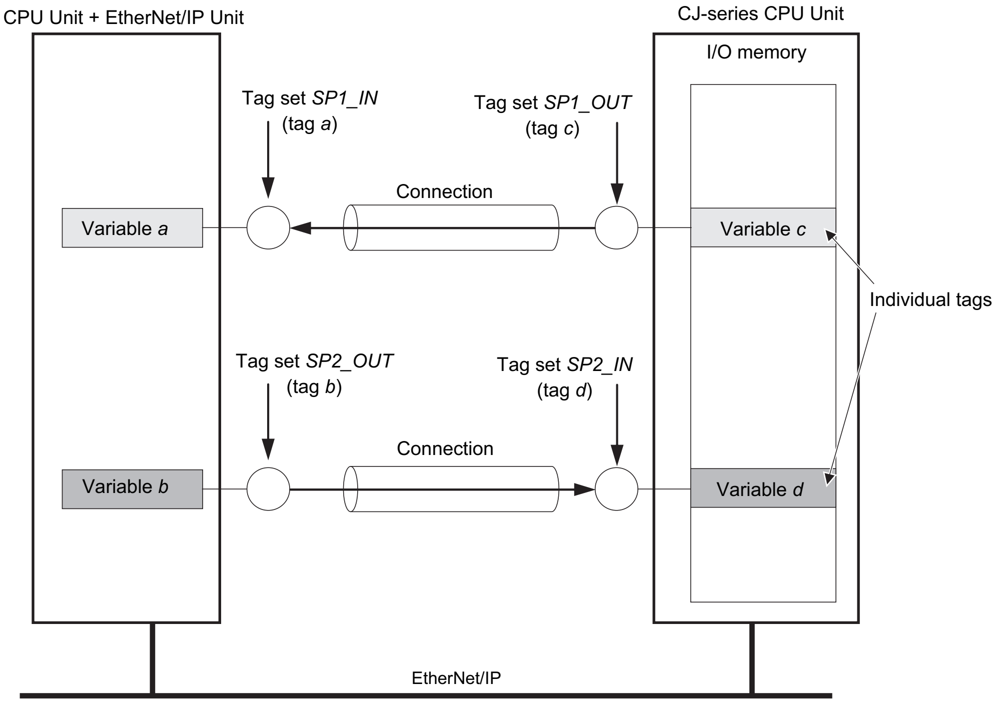


There are input (consume) and output (produce) tag sets. Each tag set can contain either input tags or output tags. The same input tag cannot be included in more than one input tag set.

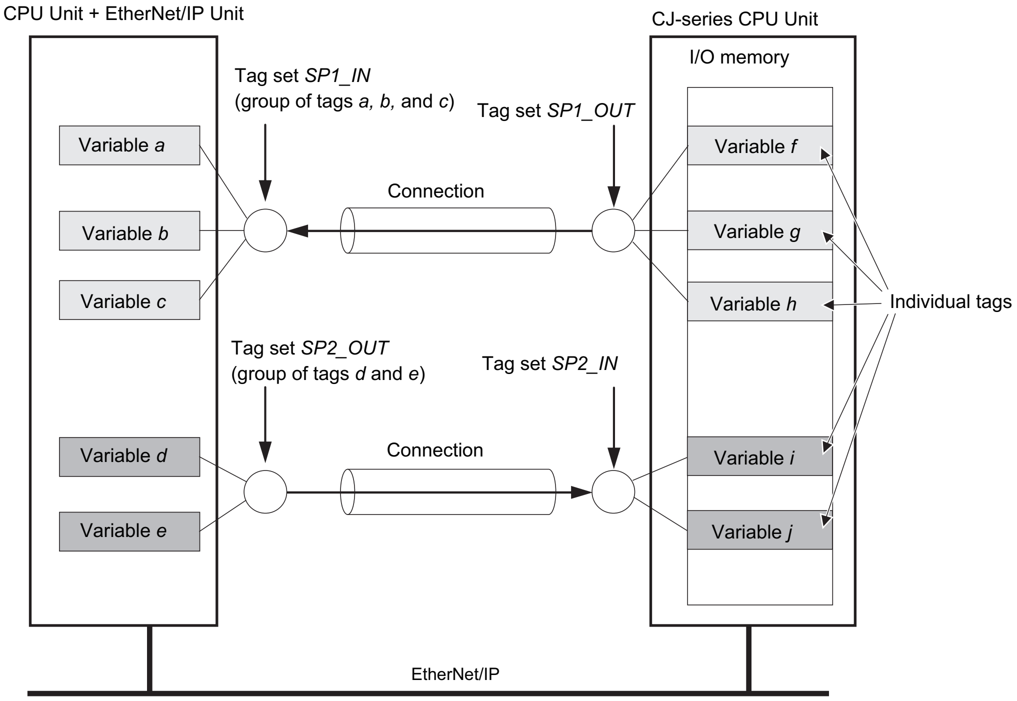
Number of Tags in Tag Sets

You can set one or more tags for each of the input and output tag sets for one connection.
For example, you can set the input tag set with one tag, and the output tag set with more than one tag.

- Tag Set with Only One Tag Each
  With basic Network Configurator procedures, each tag set contains only one tag.



- Tag Sets Each with Multiple Tags
  As shown below, multiple tags can be grouped. You can assign up to eight tags (up to 722 words in total) in one tag set.



Note To enable a connection, each tag set must include only one of ether input tags or output tags. (Both input and output tags cannot be included in one tag set.)

9-1-3 Tag Data Link Functions and Specifications

The tag data link and performance specifications of the NX-series EtherNet/IP Unit are given below.

Item		Specification
		NX-EIP201
Communications type		Standard EtherNet/IP implicit communications (connection-type cyclic communications)
Setting method		After you have set tags, tag sets, and connections with the Network Configurator, you must download tag data link parameters to all devices on the EtherNet/IP network. After the parameters are downloaded, the EtherNet/IP Units are restarted to start the tag data links. You can export network variables that you created on the Sysmac Studio to a CSV file. You can then import the file to the Network Configurator and assign the network variables to the tags.
Tags[*1]	Supported variable types	You can specify the following network variables as tags.[*2], [*3] • Global variables
	Maximum number of words per tag	722 words (1,444 bytes)
	Maximum number of tags	1,024 (total of 2,048 with two ports)
Tag sets	Maximum number of tags per tag set	64 (63 when Controller status is included)
	Maximum number of words per tag set	722 words (1,444 bytes)
	Maximum number of tag sets	256 (total of 512 with two ports)
Connection		Maximum number of connections per Unit: 512 (256 per port)
Connection type		Each connection can be set for 1-to-1 (unicast) or 1-to-N (multicast) communications.
Packet interval (RPI)[*4]		1.0 to 10,000 ms in 1.0-ms increments The packet interval can be set separately for each connection.
Allowed communications bandwidth per Unit (pps)		40,000 pps[*5] [*6] Note: The heartbeat and the CIP Safety routing are included.

*1. When you specify a specific I/O memory address for a tag, create a variable with an AT specification for the I/O memory address on the Sysmac Studio, and then specify the variable with the AT specification for the tag. You need to set memory used for CJ-series Unit to use the I/O memory address.
For details on memory settings used for CJ-series Unit, refer to the *NJ/NX-series CPU Unit Software User's Manual (Cat. No. W501)*.

*2. You can import network variables created in the Sysmac Studio to the Network Configurator as tags.
If variables for which Network publish attribute is set on the Sysmac Studio contain I/O memory addresses, such as "0000" and "H0000", they are not exported to CSV files.

*3. The following table lists variables that you can specify as tags.

Data types		Example	Specification
Variables with basic data types		aaa	Supported
Enumerated variables		bbb	Supported
Array variables	**Arrays**	ccc	Supported
	Elements	ccc[2]	Supported
Structure variables	**Structures**	ddd	Supported
	Members	ddd.xxx	Supported

Data types		Example	Specification
Union variables	**Unions**	eee	Supported
	Members	eee.yyy	Supported

*4. The approximate I/O response time of the tag data link is determined by the relationship between the packet interval and the number of connections. Refer to *12-3 Tag Data Link I/O Response Time* on page 12-23 for details.

*5. If the two EtherNet/IP ports are used simultaneously, the maximum communications data size means the maximum data size of the total of the two ports.

*6. When the Unit is performing tag data link communications where the allowable communications bandwidth per Unit is close to or greater than 30,000 pps, the following functions may not be used properly. In that case, use the built-in EtherNet/IP port on the CPU Unit or an EtherNet/IP port of a different NX-series EtherNet/IP Unit.

- Connecting the Sysmac Studio online from the EtherNet/IP port of the NX-series EtherNet/IP Unit
- Connecting the Network Configurator online from the EtherNet/IP port of the NX-series EtherNet/IP Unit
- Connecting the NA-series Programmable Terminal online from the EtherNet/IP port of the NX-series EtherNet/IP Unit
- Port forward via the NX-series EtherNet/IP Unit
- CIP message communications
- SNMP function

These functions of the NX-series EtherNet/IP Unit can be used via X Bus from the built-in EtherNet/IP port on the CPU Unit or an EtherNet/IP port of a different NX-series EtherNet/IP Unit.

9-1-4 Overview of Operation

In this manual, the connection information that is set is called tag data link parameters.
This section describes how to set tag data links with the Sysmac Studio and the Network Configurator.

Setting Network Variables (Sysmac Studio)

First, create any variables that you want to use for tag data links as network variables on the Sysmac Studio.

1 Set the Network Publish attribute to **Input** or **Output** in the Global Variable Table for variables you want to use for tag data links (i.e., as tags).

2 To maintain concurrency in tag data within a tag set, set all tags (i.e., variables with a Network Publish attribute) within the same tag set as follows:
Set a refreshing task for variables with a Network Publish attribute to maintain concurrency for tag data link data as described below.

- Maintain concurrency in the tag data in a tag set.
- The timing of updating network variables that are assigned to tags is synchronized with the execution period of a program that accesses the network variables.

Refer to *9-1-7 Concurrency of Tag Data Link Data* on page 9-12 for details on the concurrency of tag data link data.
In addition to ensuring concurrency, set the tasks in which to perform I/O refreshing to reduce the effect of I/O refresh time on the task execution time. Refer to *I/O Refreshing of X Bus Function Module* in the *NJ/NX-series CPU Unit Software User's Manual (Cat. No. W501)* for details on the settings.

Precautions for Correct Use

- If a variable with an AT specification is used as a tag, you do not need to set a refreshing task.
  It is refreshed in the primary periodic task.
- You cannot use the following notation, which specifies an I/O memory address, in the variable name of any variable used in a tag data link.
  a) Variable names that contain only single-byte numerals (Example: 001)
  b) Variable names with the following single-byte letters (uppercase or lowercase) followed by single-byte numerals
    1) H (Example: H30)
    2) W (Example: w30)
    3) D (Example: D100)
    4) E0_ to E18_
- When the server function of CIP message communications is disabled, the tag data links cannot be used. Enable the server function of CIP message communications. Refer to *CIP Message Server* on page 7-15 for details on setting CIP message server.
- NX-series EtherNet/IP Unit performs I/O refreshing in synchronization with the task of the CPU Unit. If the event *I/O Refreshing Timeout Error* (65900000 hex) occurs, it means that the processing load in the NX-series EtherNet/IP Unit is high and I/O refreshing synchronized with the task cycle cannot be executed. In that case, take measures such as setting tasks in which to perform I/O refreshing for tag sets to use exclusive control of variables in tasks. Refer to *I/O Refreshing of X Bus Function Module* in the *NJ/NX-series CPU Unit Software User's Manual (Cat. No. W501)* for details on the settings. For more information about the event *I/O Refreshing Timeout Error* (65900000 hex), refer to the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)*.

Setting and Downloading Tag Data Link Parameters (Network Configurator or Sysmac Studio)

The following tag data link parameters (e.g., connection information) are created with the Network Configurator or the Sysmac Studio, and then the parameters are downloaded to all originator devices on the EtherNet/IP network.
When the tag data links are used on EtherNet/IP ports, use the Network Configurator to make the following settings.

1 Creating the Configuration Information
Register EtherNet/IP ports and EtherNet/IP Units to create connections that define the tag data links. For details, refer to *9-2-3 Registering Devices* on page 9-17.

2 Setting Tags
Create CPU Unit variables for input (consume) tags and output (produce) tags.
You can import and export network variables that are created on the Sysmac Studio to CSV files. This allows you to register them as tags on the Network Configurator.
Output (produce) tags can be defined to clear output data to 0 or to hold the output data from before the error when a fatal error occurs in the CPU Unit.

3 Setting Tag Sets
Create output tag sets and input tag sets and assign tags to them. (You can create up to eight I/O tag sets.) You can specify the Controller status that indicates the CPU Unit's operating status (operating information and error information) in a tag set.

4 Setting connections

Link the output tag sets for the target device and the input tag sets for the originator device as connections.

● Connection Setting Parameters

The connection settings in step 4 above have the following setting parameters.

- Setting the Requested Packet Interval (RPI)
  The RPI (Requested Packet Interval) is the I/O data refresh cycle on the Ethernet line when tag data links are established. With EtherNet/IP, data is exchanged on the communications line at the RPI that is set for each connection, regardless of the number of nodes.
  With the EtherNet/IP port, you can set RPI for each connection.

- Setting Multi-cast or Unicast Communications
  You can select a multicast connection or unicast (point-to-point) connection as the connection type in the tag data link connection settings.
  With a multicast connection, you can send an output tag set in one packet 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, multicast connections can decrease the communications load if one output tag set is sent to multiple nodes.
  To use a multicast connection and send an output tag set in one packet to multiple nodes, the following settings for the receiving node must be the same as the settings of the sending node: the connection type (multicast), the connection I/O type, packet internal (RPI), and timeout value.

Precautions for Correct Use

- 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 *12-2 Adjusting the Communications Load* on page 12-7*Checking the Device Bandwidth Usage* on page A-26 and set an appropriate packet interval (RPI).
- If multicast connections are used, however, use an Ethernet switch that has multicast filtering, unless packets are received by all nodes in the network.
  If an Ethernet switch without multicast filtering is used, multicast packets are broadcast to the entire network, and so the packets are sent to nodes that do not require them, which will cause the communications load on those nodes to increase.
- If you use data tag links with multicast traffic at a baud rate over 100 Mbps, use an Ethernet switch that supports a baud rate of 1000 Mbps.
  If there is an Ethernet device on the same network that communicates at 100 Mbps or less, the device may affect tag data link communications and cause tag data links to be broken, even if the device is not related to tag data link communications.

Additional Information

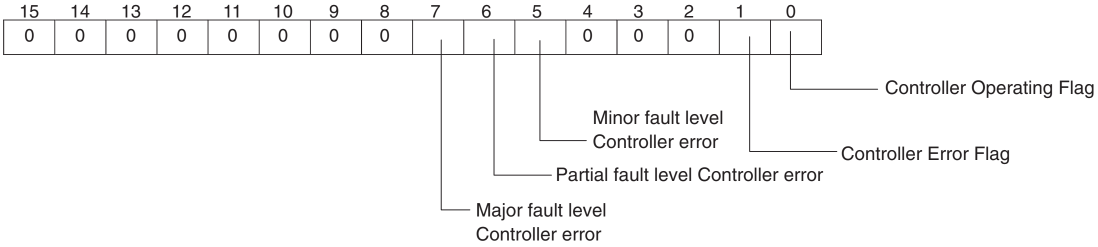
- To calculate the number of connections of each connection type, refer to *12-1-2 Calculating the Number of Connections* on page 12-5.
- If the maximum number of connections is exceeded, you must review the number of connections for the built-in EtherNet/IP port, or the number of nodes. Also consider adding NX-series EtherNet/IP Units.

9-1-5 Starting and Stopping Tag Data Links

Tag data links are automatically started when the data link parameters are downloaded from the Network Configurator and the power supply to the CPU Unit is turned ON.
Thereafter, you can start and stop tag data links 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.
Furthermore, you can execute instructions from the user program to start and stop the entire network. Refer to *9-2-12 Starting and Stopping Tag Data Links* on page 9-61 for details.

9-1-6 Controller Status

You can include the Controller status as a member of a tag set in the data sent and received.
The Controller status is a set of flags that indicate the operating status of the CPU Unit (operating information, error information, Controller error level).
If the Controller status is specified as an output (produce) tag, the Controller status is added to the start of the tag set in the following format.
(Select the **Include** Option for **Controller Status** in the upper right of the **Edit Tag Set** Dialog Box.)

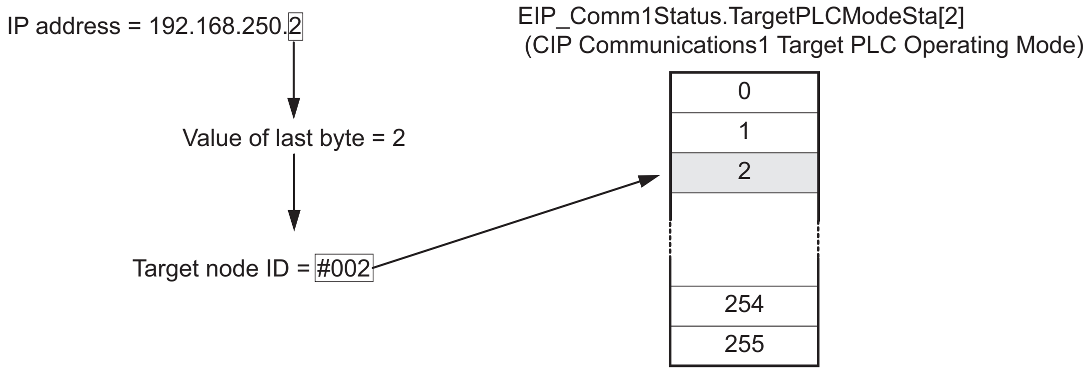

15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
0 0 0 0 0 0 0 0 0 0 0
Controller Operating Flag
Minor fault level Controller error
Controller Error Flag
Partial fault level Controller error
Major fault level Controller error

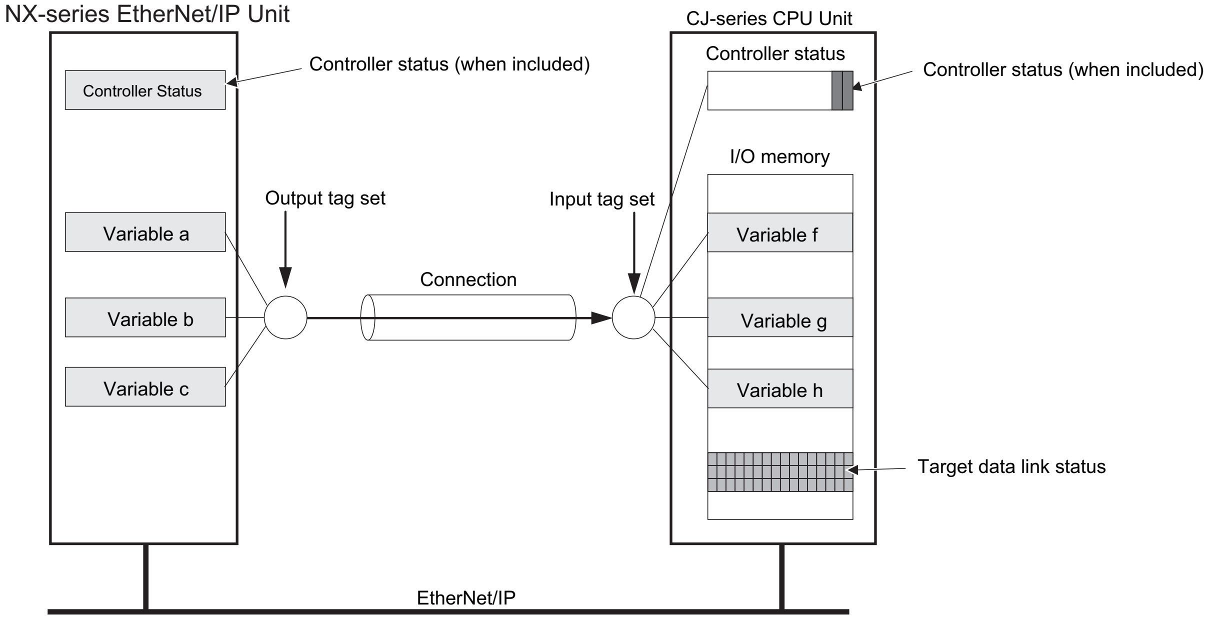
Note Of the flags in bits 5 to 7 that indicate the current error level, only the flag for the highest error level changes to TRUE.
For example, if a minor fault level Controller error and a major fault level Controller error occur at the same time, only the flag for the major fault level Controller error (bit 7) will change to TRUE and the flag for the minor fault level Controller error (bit 5) will remain as FALSE.

To receive the Controller status, specify the Controller status for the In - Consume Tab Page in the dialog box used to edit the receive tag set.
(Select the **Include** Option for **Controller Status** in the upper right of the **Edit Tag Set** Dialog Box.)
When a tag data link is started, the contents of the Controller status is stored in the device variables that are given below.

- CIP Communications1 Target PLC Operating Mode: *EIP_Comm1Status.TargetPLCModeSta[255]*
- CIP Communications2 Target PLC Operating Mode: *EIP_Comm2Status.TargetPLCModeSta[255]*
- CIP Communications1 Target PLC Error Information: *EIP_Comm1Status.TargetPLCErr[255]*
- CIP Communications2 Target PLC Error Information: *EIP_Comm2Status.TargetPLCErr[255]*

Example: Using an NX-series EtherNet/IP Unit with unit number 1 to send the CIP Communications1 Target PLC Operating Mode of the Target Node with an IP Address of 192.168.250.2


IP address = 192.168.250.2
Value of last byte = 2
Target node ID = #002
EIP_Comm1Status.TargetPLCModeSta[2]
(CIP Communications1 Target PLC Operating Mode)
0
1
2
254
255



Additional Information

The target node ID may be duplicated depending on the IP address of the target node. In this case, it is necessary to change the target node ID on the Network Configurator so that the same address could not be used by more than one node.
For information on how to change the target node ID, refer to Step 4 under *Registering Devices in the Register Device List* in *Connection Settings* in *9-2-5 Connection Settings* on page 9-32.

When you use multiple connections to communicate with one specific node, the information of the Controller status is stored in the following variables if the Controller status is specified in the input tags and the output tags for all the connections.

Controller status	Variable name	Description of operation
Controller Operating Flag	• *EIP_Comm1Status.TargetPLCModeSta[255]* (CIP Communications1 Target PLC Operating Mode) • *EIP_Comm2Status.TargetPLCModeSta[255]* (CIP Communications2 Target PLC Operating Mode)	This flag shows the operation information of the Controller at the target node. (When the EtherNet/IP Port Is the Originator of the Connection) The array element that corresponds to the target node ID at the target is set to TRUE when all information for all the connections to the relevant target node shows operating status. You can change the target node ID for the IP address from the Network Configurator. This status information is enabled when the Controller status is included in the communications data for both the originator and the target node. This variable is updated when necessary.
Controller Error Flag	• *EIP_Comm1Status.TargetPLCErr[255]* (CIP Communications1 Target PLC Error Information) • *EIP_Comm2Status.TargetPLCErr[255]* (CIP Communications2 Target PLC Error Information)	This variable shows the error status (logical OR of fatal and non-fatal errors) of the target node Controllers. (When the EtherNet/IP Port Is the Originator of the Connection) You can change the target node ID for the IP address from the Network Configurator. The Controller Error Flags are enabled when the Controller status is included in the communications data for both the originator and target node. This variable is updated when necessary.

Additional Information

Even if you specify including the Controller status in output (produce) tags, you do not necessarily need to include the Controller status in input (consume) tags.
If you do not include the Controller status in an input (consume) tag, the contents of the Controller status are not updated in the Target PLC Operating Mode and Target PLC Error Information variables, but they are sent in the input (consume) tag.
Therefore, you can use the Controller status data that was received in the input (consume) tag as receive data.

9-1-7 Concurrency of Tag Data Link Data

To maintain the concurrency of data in a tag data link, you must set a refreshing task for each network variable that is assigned to a tag.

- Maintain concurrency in tag data in a tag set.
- The timing of updating network variables that are assigned to tags is synchronized with the execution period of the program that accesses the network variables

Additional Information

A refreshing task maintains concurrency of the value of a global variable from all tasks that access that global variable. This is achieved by specifying a single task that can write to that global variable and not allowing any other task to write to that global variable.
For details on refreshing tasks, refer to the *NJ/NX-series CPU Unit Software User's Manual (Cat. No. W501)*.

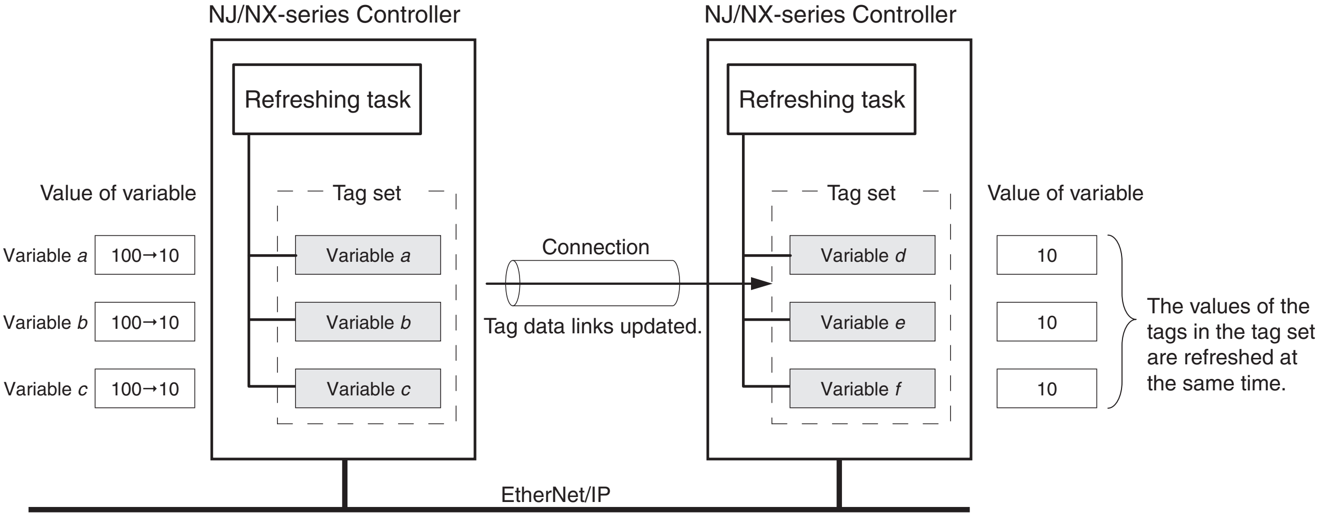
Maintaining Concurrency in the Tag Data in a Tag Set

To maintain concurrency in the values of multiple tags in a tag set, the tags (variables with a Network Publish attribute) must satisfy all of the following conditions.

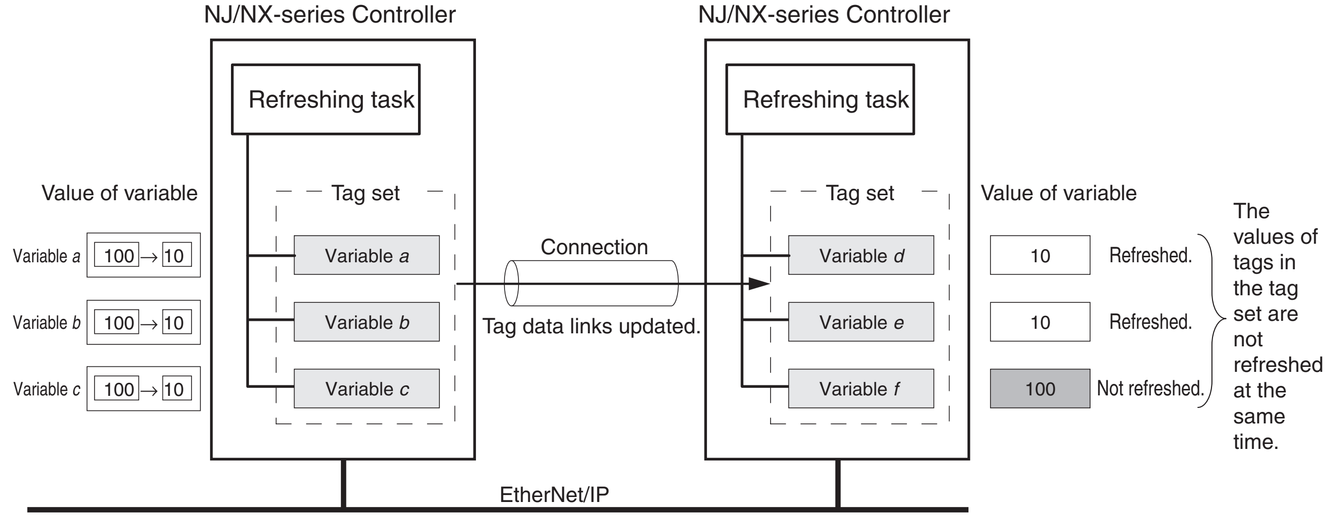
a. The tags must be assigned to the same tag set (connection).

b. A refreshing task must be set for network variables assigned to the tags, and the refreshing task must be the same for all the tags in the tag set.

- Setting Refreshing Tasks for Tags (Network Variables)
  Concurrency of the tags in the tag set is maintained.



- Not Setting Refreshing Tasks for Tags (Network Variables)
  Concurrency of the tags in the tag set is not maintained.



Synchronization of Tag Set Update and User Program Execution Period

The tag set update timing is synchronized with the execution period of the task to which the tag set is assigned as a network variable. The tag set and the task to which it is assigned are determined as follows.

- In **Setting for Exclusive Control of Variable in Tasks** under **Configurations and Setup** - **Task Settings** on the Sysmac Studio, tag sets containing variables assigned to the primary periodic task are assigned to the primary periodic task.
- Tag sets other than the above are assigned to the priority-16 periodic task.
- All tag sets are assigned to the primary periodic task if the priority-16 periodic task is not existed in the user program.

Precautions for Correct Use

For a tag set that contains variables assigned to the setting for exclusive control of variables in tasks, whether or not processing is included in the I/O refresh processing time of the primary periodic task depends on the setting. Consider the effect on task execution time and configure the settings for exclusive control of variables in tasks.

Update Timing of Tag Sets

The tag set update timing is determined by the task period of the task to which the tag set is assigned and the set value of the packet interval (RPI) as follows.

Relationship between RPI and task period of the task to which the tag set is assigned	Update timing of the tag set
RPI ≥ task period	At least once per RPI period, a tag set update and a refreshing of the NX-series EtherNet/IP Unit are performed on the CPU Unit.
RPI < task period	At least one time per task period, a tag set update and a refreshing of the NX-series EtherNet/IP Unit are performed on the CPU Unit.

Additional Information

The tag set update is performed outside of the variable access time. Therefore, the tag set update timing is not affected by the variable access time setting.

9-2 Setting Tag Data Links

Additional Information

You can also use the Sysmac Studio to set the tag data links.
Refer to *A-3 Use the Sysmac Studio to Set the Tag Data Links (EtherNet/IP Connections)* on page A-6 for details on setting the tag data links on the Sysmac Studio.

9-2-1 Starting the Network Configurator

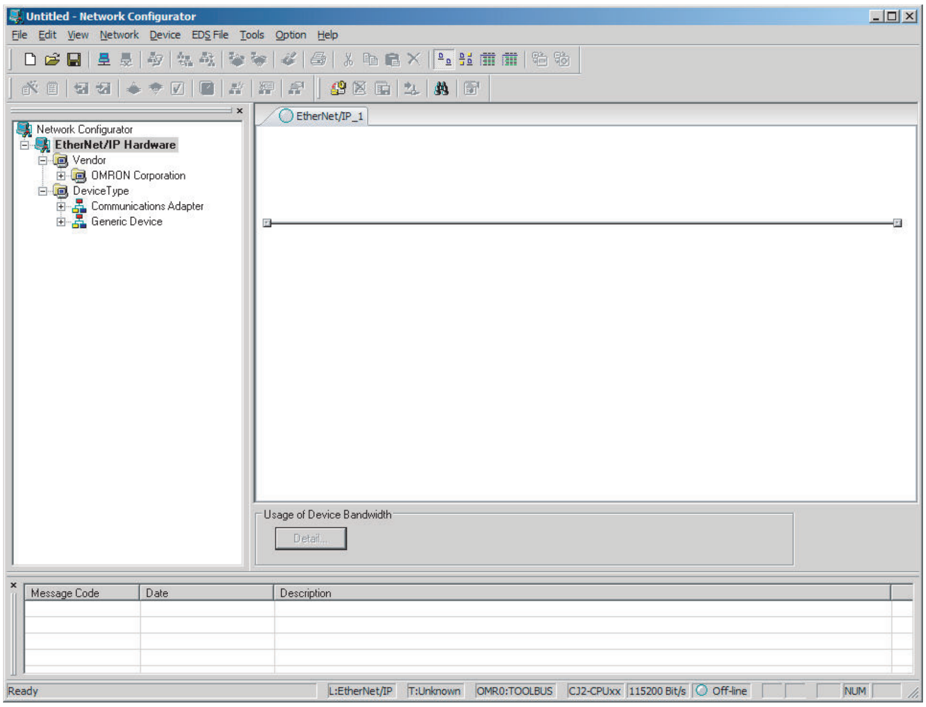
Procedure

Tag data links are set from the Network Configurator. Use the following procedure to start the Network Configurator.

- **Using the Windows Start Menu**

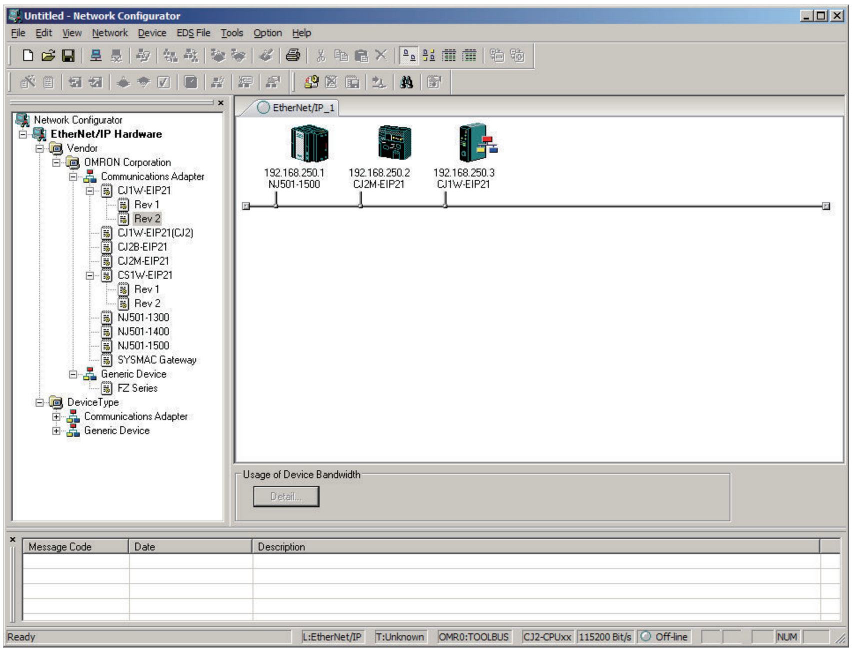
To start the Network Configurator, select **OMRON** – **Sysmac Studio** – **Network Configurator for EtherNetIP** – **Network Configurator**.

When the Network Configurator starts, the following window is displayed.

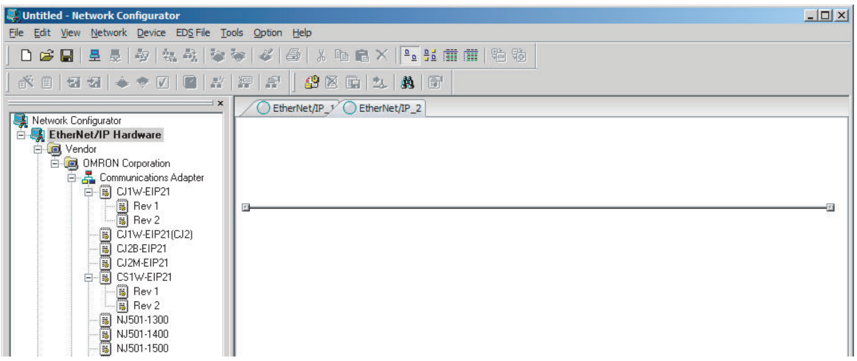


Main Window

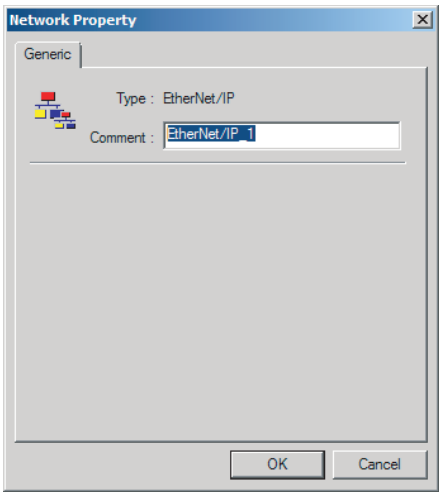
The Main Window consists of a Hardware List and a Network Configuration Pane, as shown in the following diagram.



To manage two or more networks, you can select **Network** – **Add**. You can add a new Network Configuration Pane.



To change the network name displayed in the Network Tab Page, select **Network** – **Property**. You can change the network name as set in the Comment Field of the Network Property Dialog Box.



Type : EtherNet/IP

Comment : EtherNet/IP_1

9-2-2 Tag Data Link Setting Procedure

This section describes the procedure to set tag data links (i.e., connection information).
For data links between Controllers, the connection information is set only in the originator, i.e., the node that receives data.

1 **Create the network configuration.**

1. Register all the EtherNet/IP ports for which to create connections, in the EtherNet/IP Network Configuration Pane. (Refer to *9-2-3 Registering Devices* on page 9-17.)
   Note If a system has already been installed, connect online to the EtherNet/IP network and upload the network configuration. (Refer to *9-2-10 Uploading Tag Data Link Parameters* on page 9-54)

↓

2 **Create the tag and tag set connections.**

1. Create tags and tag sets for all the registered devices (EtherNet/IP ports). (Refer to *9-2-4 Creating Tags and Tag Sets* on page 9-19.)
2. Create a connection for the originator device (i.e., the registered device that receives data as input data). (Refer to *9-2-5 Connection Settings* on page 9-32)

↓

3 **Download the tag data link parameters. (Refer to *9-2-9 Downloading Tag Data Link Parameters* on page 9-51)**

↓

4 **Make sure that the tag data links are operating normally, by using the indicators for the EtherNet/IP port (refer to the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)*) and the device monitor function of the Network Configurator. (Refer to *14-6-1 The Network Configurator's Device Monitor Function* on page 14-47.)**

↓

5 **Make sure that the output tag data is reflected in the input tags by checking the Watch Tab Page on the Sysmac Studio.**

Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for the procedure.

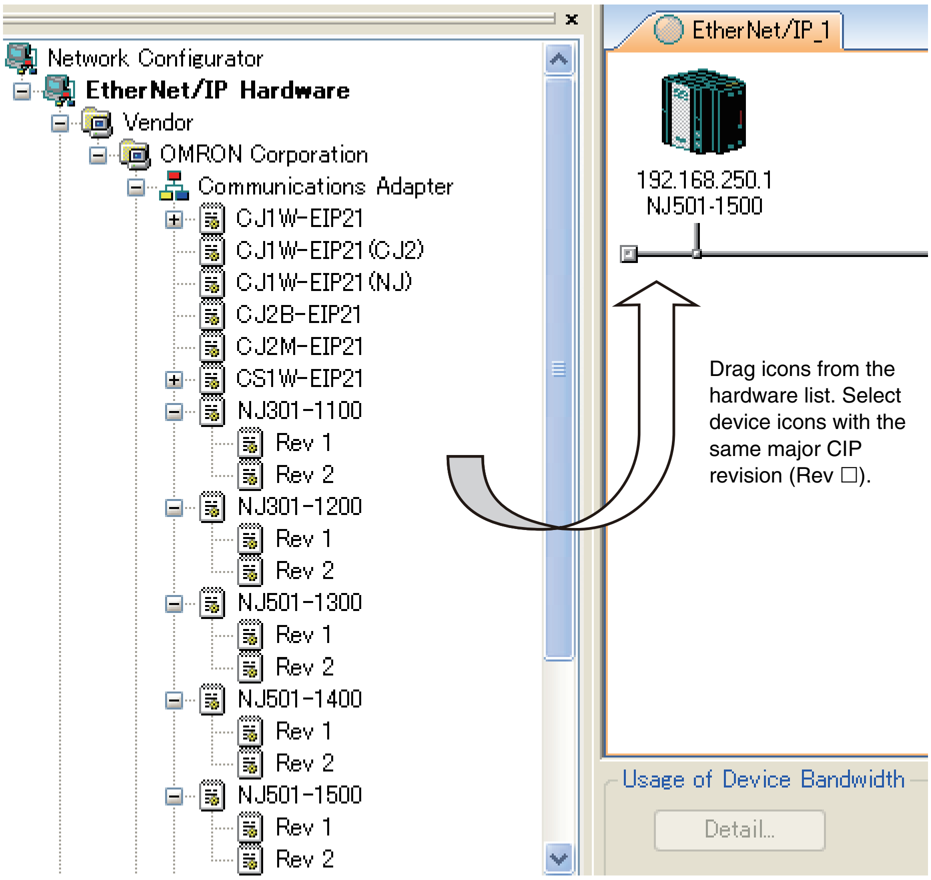
Additional Information

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 *A-6 Tag Data Link Settings with Generic Devices* on page A-50 for information on how to make the settings with the Generic Device.

9-2-3 Registering Devices

Register all of the devices required in the equipment (such as EtherNet/IP Units performing tag data links) in the network configuration.

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 Pane on the right. (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.)
You can also select a device in the Hardware List and press the Enter Key to register it. The icon of the device is displayed in the Network Configuration Pane, as shown in the following picture.



Drag icons from the hardware list. Select device icons with the same major CIP revision (Rev □).

The device names and major CIP revisions (Rev □) are displayed in the hardware list.
For the NJ/NX-series Controllers, device names of Units and major CIP revisions are as shown in the following table.

Device name in Hardware List	Unit version	CIP revisions	
		Major revision	Revision name in Hardware List
NX701	Unit version 1.10 or later	2	None
NX502-□□□□	Unit version 1.60 or later	2	None
NX102-□□□□	Unit version 1.30 or later	2	None
NX1P2	Unit version 1.13 or later	2	None
NJ501-□□□□	Unit version 1.00 to 1.02	1	Rev1
	Unit version 1.03 or later	2	Rev2
NJ301-□□□□	Unit version 1.01 or 1.02	1	Rev1
	Unit version 1.03 or later	2	Rev2
NJ101	Unit version 1.10 or later	2	None
NX-EIP201	Unit version 1.00 or later	2	None

Precautions for Correct Use

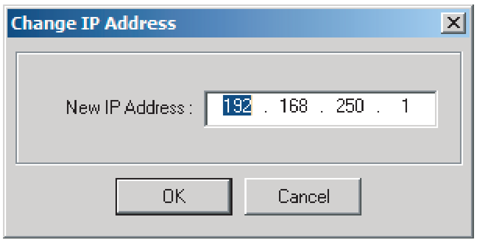
Make sure that you select the devices with the same device names and the same major CIP revisions as the devices you use in the actual operation. The following will occur if any device name or CIP revision is incorrect when you attempt to download tag data link parameters on the Network Configurator.

- If a device name is incorrect, an error message will be displayed saying "**Specified device can not be accessed, or wrong device type**", and the download will fail.
- If a revision is incorrect, a message will be displayed saying "**Wrong unit revision**", and the download will fail.

Similarly, the above will occur when performing upload or comparison of the tag data link parameters.

In any of the above cases, refer to *9-2-17 Changing Devices* on page 9-70 and change the device.

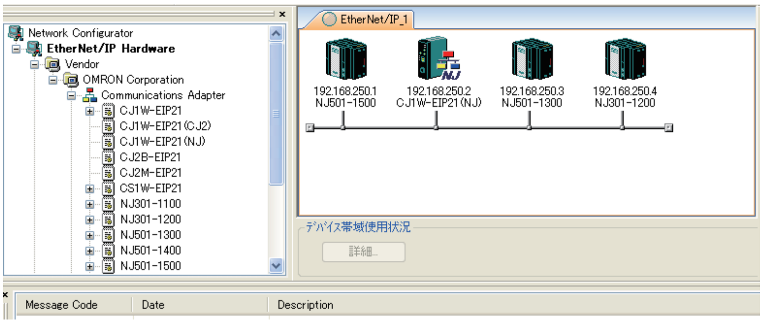
2 Right-click the registered device's icon to display the pop-up menu, and select **Change IP Address**.



New IP Address : 192 . 168 . 250 . 1

3 Set the IP address to match the node address (IP address) actually used in the device, and click the **OK** Button.

4 Repeat steps 1 to 3, and register all devices to which tag data links are made.



9-2-4 Creating Tags and Tag Sets

You must create tag sets and member tags that are required to create connections for a registered EtherNet/IP port and EtherNet/IP Unit. You can set the network variables used in control programs for tags.

This section first describes the basic procedure to create tags and tag sets, as described in (1) below. Then it explains how to import variables with a Network Publish attribute from the Sysmac Studio to the Network Configurator, as described in (2) below.

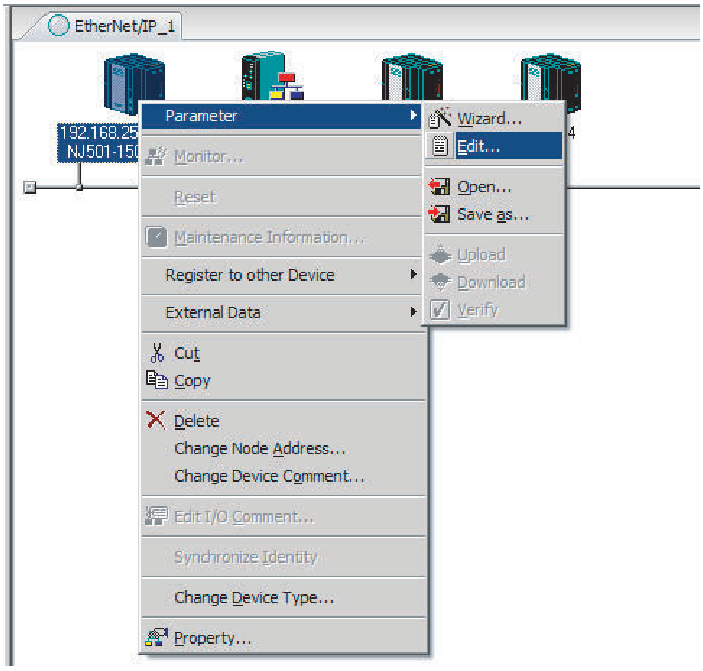
1. Creating Tags and Tag Sets with the Network Configurator's Device Parameter Editing Function

2. Importing Variables with a Network Publish Attribute Created in the Sysmac Studio to the Network Configurator

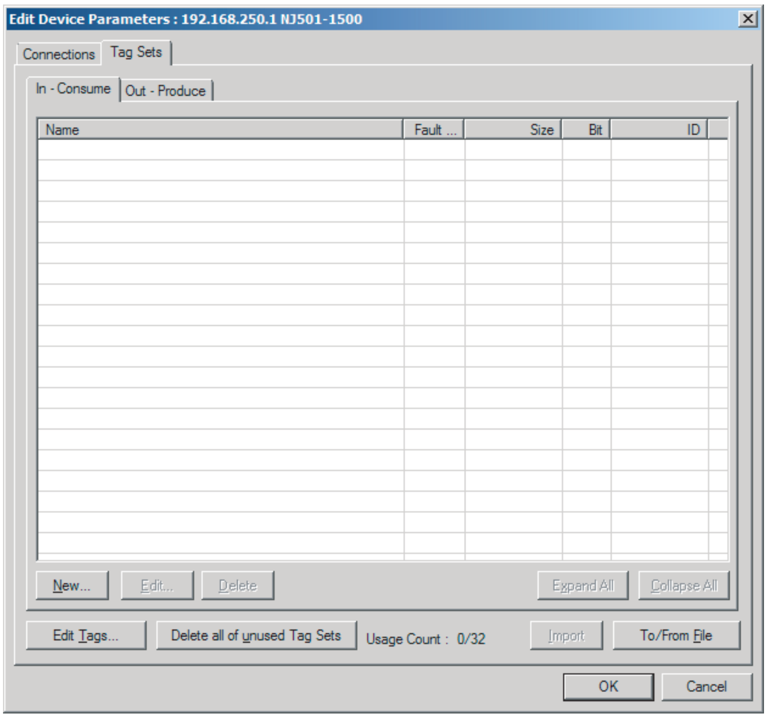
(1) Creating Tags and Tag Sets with the Network Configurator's Device Parameter Editing Function

● Creating a Tag Set

1 Double-click the icon of the device for which to create a tag set to display the **Edit Device Parameters** Dialog Box. Or, right-click the icon to display the pop-up menu, and select **Parameter** – **Edit**.



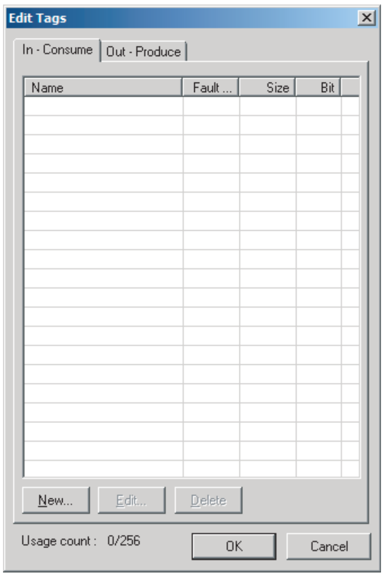
2 Click the **Tag Sets** Tab at the top of the **Edit Device Parameters** Dialog Box.
There are two kinds of tag sets: input (consume) and output (produce).



● Creating and Adding Tags

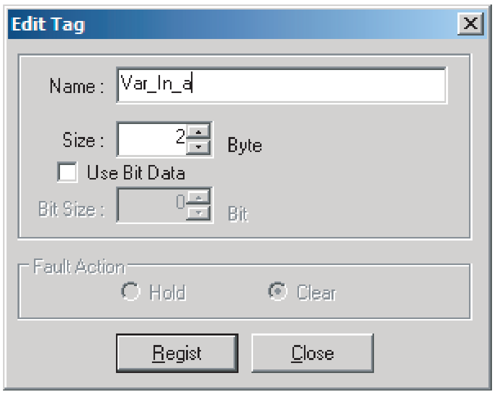
1 Click the **Edit Tags** Button.

The **Edit Tags** Dialog Box is displayed. Register input (consume) tags and output (produce) tags separately.



2 Click the **In - Consume** Tab, and then click the **New** Button.

The **Edit Tag** Dialog Box is displayed.



Name : Var_In_a

Size : 2 Byte

☐ Use Bit Data

Bit Size : 0 Bit

Fault Action
○ Hold ● Clear

3 Enter the variable name directly into the **Name** Box. (Example: Var_In_a)

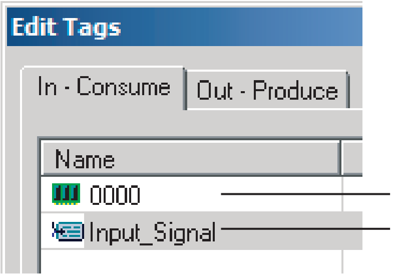
Additional Information

- You can use the following characters in tag names.
  0 to 9, A to Z, a to z, single-byte kana, _ (underbar), and multi-byte characters (e.g., Japanese)
- You cannot use the following characters in tag names.
  ! “ # $ & ‘ ( ) * + , - . / : ; < = > ? @ [ ] ^ ‘ % spaces or text strings that start with numerals (0 to 9)
- The maximum length of a tag name is 255 bytes.
- Specify array variables, structure variables, and union variables, if any, as shown below.
  - Specifying array elements
    Example: array [2][3] (or array [2,3]) and array [2][3][4] (or array [2,3,4])
  - Specifying structure members
    Example: Struct.member (Separate the member name with a period.)
  - Specifying union members
    Example: Union.member (Separate the member name with a period.)

Precautions for Correct Use

- To specify an I/O memory address for a tag, create a variable with an AT specification of the I/O memory address on the Sysmac Studio, and then specify the variable with the AT specification for the tag.
  You need to set memory used for CJ-series Unit to use the I/O memory address. For details on memory settings used for CJ-series Unit, refer to the *NJ/NX-series CPU Unit Software User's Manual (Cat. No. W501)*.
- If you enter the following I/O memory addresses for tag names on the Network Configurator, the tags are directly assigned to the I/O memory addresses in the CPU Unit, and not to the variables. Always specify variable names for tags.
  a) Variable names that contain only single-byte numerals from 0000 to 6143
  b) Variable names with the following single-byte letters (uppercase or lowercase) followed by single-byte numerals
    - H (H000 to H511)
    - W (W000 to W511)
    - D (D00000 to D32767)
    - E0_ to E18_ (E0_00000 to E0_32767, to E18_00000 to E18_32767)

  You can check the memory address or variable to which a tag is assigned, with icons in the **Edit Tags** Dialog Box.



Tag that is directly assigned to an I/O memory address

Tag that is assigned to a variable with a Network Publish attribute

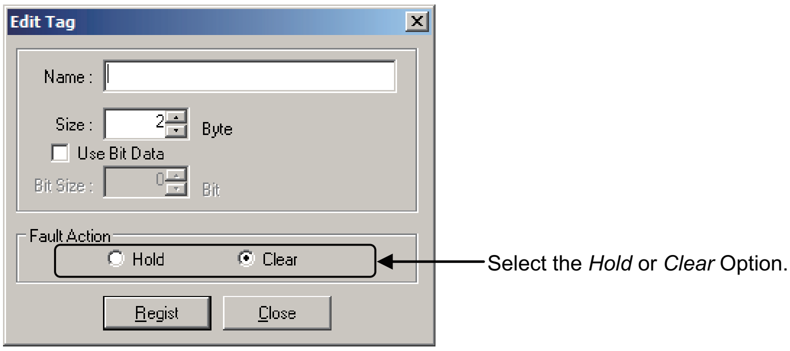
4 Input the size of the tag in bytes in the **Size** Field.
Specify the tag size to be the same as the data type size of the variable.
To use a BOOL variable, select the **Use Bit Data** Check Box, and enter *1* in the **Size** Field.

5 Click the **Regist** Button to register the tag.
If an I/O memory address is specified as the tag name, another **Edit Tag** Dialog Box will be displayed with the next address as the tag name so that you can register the next tag consecutively.
After you register the tags, click the **Close** Button.

6 Click the **Out - Produce** Tab, and then click the **New** Button.
The **Edit Tag** Dialog Box is displayed. Input output tags in the same way.
In case a major fault occurs in the CPU Unit, use the **Fault Action** setting of the output (produce) tag to select whether to clear output data or continue to send data.

The **Fault Action** setting is not required for input (consume) tag sets.

- Retain output after major fault: **Hold** (default)
  Output data maintains its previous status even after a major fault occurs.
- Clear output at major fault: **Clear**
  Output data is cleared to 0 when a major fault occurs.



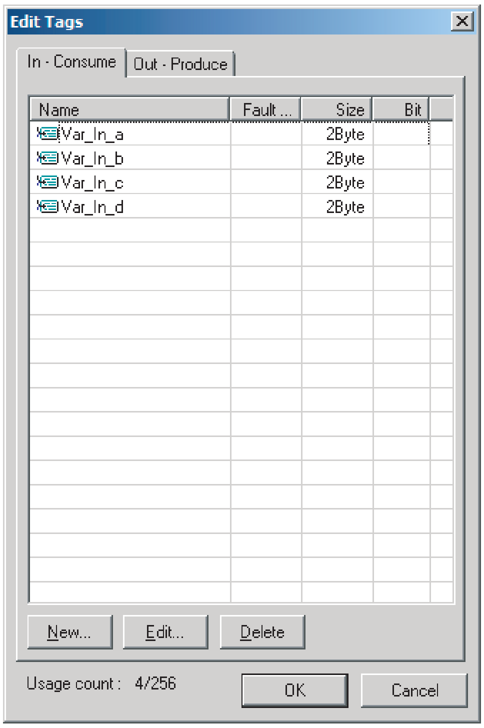
Select the *Hold* or *Clear* Option.

Precautions for Correct Use

Connections are cut off if any of the following errors occurs in the CPU Unit that is the originator while tag data links are active.

- Major fault level Controller error
- Partial fault level Controller error

7 After you register all of the required tags, click the **OK** Button in the **Edit Tags** Dialog Box.



Name	Fault ...	Size	Bit
Var_In_a		2Byte	
Var_In_b		2Byte	
Var_In_c		2Byte	
Var_In_d		2Byte	

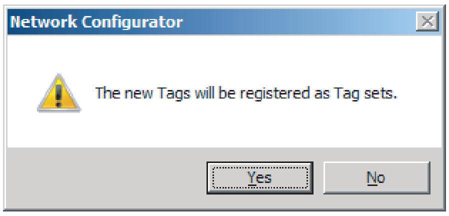
Usage count : 4/256

Precautions for Correct Use

Make the following settings to refresh all of the tag data in one tag set at the same time.

- Use the Sysmac Studio, in advance, to specify the same refreshing task for all of the variables that are assigned to tags in the tag set.
- Do not place tag variables that have AT specifications in I/O memory and tag variables that do not have AT specifications in the same tag set.

8 At this point, a confirmation dialog box is displayed to check whether the registered tag names are used as the tag set names. A tag set can contain up to eight tags, but tag sets are registered with one tag per tag set if the tag names are registered as tag set names. In this case, click the **Yes** Button.

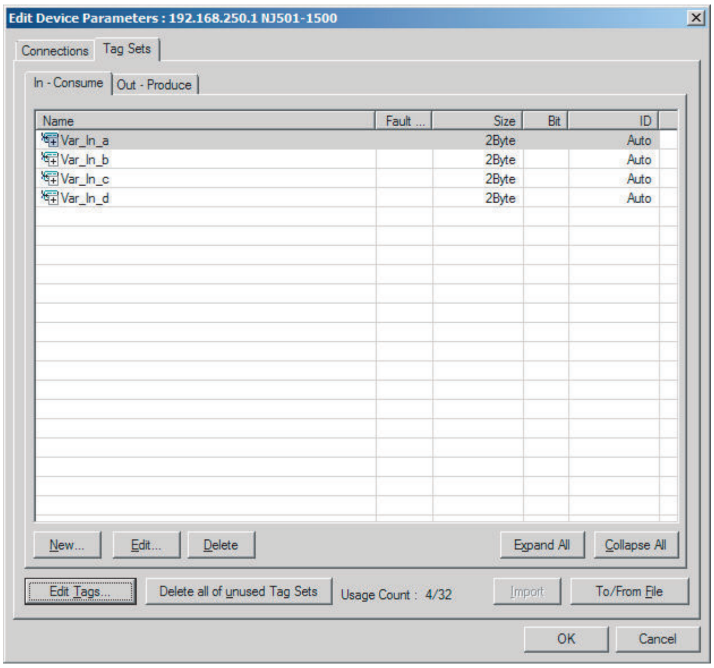


The new Tags will be registered as Tag sets.

If the **No** Button is clicked, you can add more tags to the tag set. Refer to step 8 in Changing and Registering Tag Sets for details on how to register new tags first and add more tags to the tag set later.

● Changing and Registering Tag Sets

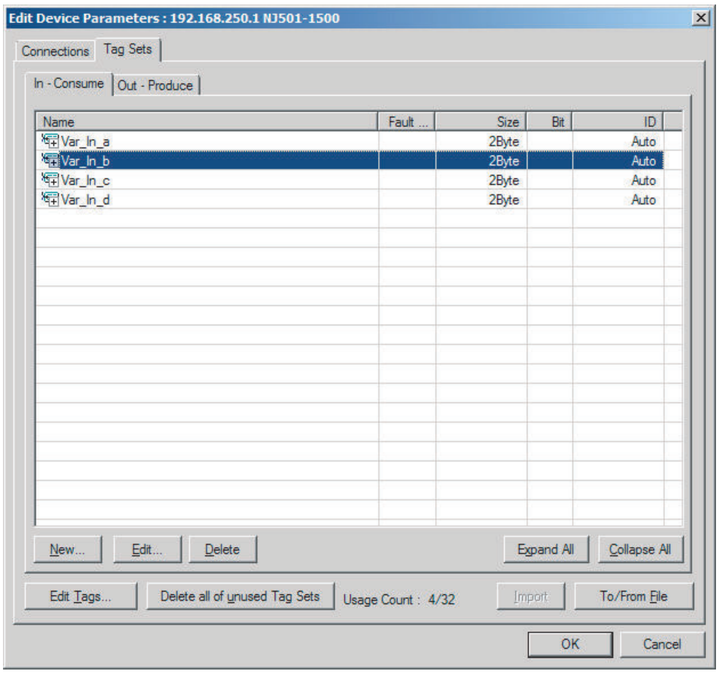
1 The following dialog box is displayed when the tags in the **Edit Tags** are registered directly as tag sets.



Name	Fault ...	Size	Bit	ID
Var_In_a		2Byte		Auto
Var_In_b		2Byte		Auto
Var_In_c		2Byte		Auto
Var_In_d		2Byte		Auto

Usage Count : 4/32

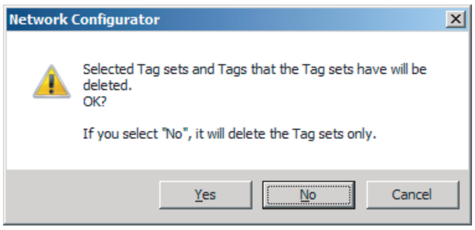
2 If an input tag is already registered in an input tag set, and you want to change its registration to a different input tag set, it is necessary to delete the tag from the tag set in which it was originally registered.
Open the **Edit Device Parameters** Dialog Box, select the tag set containing the tag that you want to delete on the **Tag Sets** Tab Page, and click the **Delete** Button. (If there are other tags registered in the 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.)



Name	Fault ...	Size	Bit	ID
Var_In_a		2Byte		Auto
Var_In_b		2Byte		Auto
Var_In_c		2Byte		Auto
Var_In_d		2Byte		Auto

Usage Count : 4/32

A confirmation message is displayed.

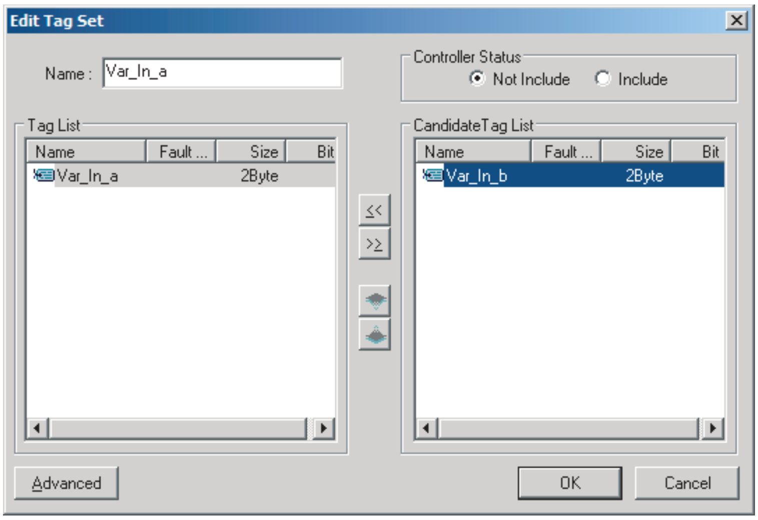


Selected Tag sets and Tags that the Tag sets have will be deleted.
OK?

If you select "No", it will delete the Tag sets only.

If the **No** Button is clicked, only the selected tag set is deleted. Click the **No** Button.

3 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 is displayed.



Name : Var_In_a

Controller Status: ● Not Include ○ Include

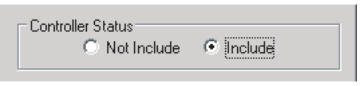
Name	Fault ...	Size	Bit
Var_In_a		2Byte	

Name	Fault ...	Size	Bit
Var_In_b		2Byte	

The **Tag List** on the left side of the dialog box shows tags that are already registered, and the **Candidate Tag List** on the right side of the dialog box shows the other tags that are not registered yet.

To add a tag, select it in the **Candidate Tag List** and click the ≪ Button.

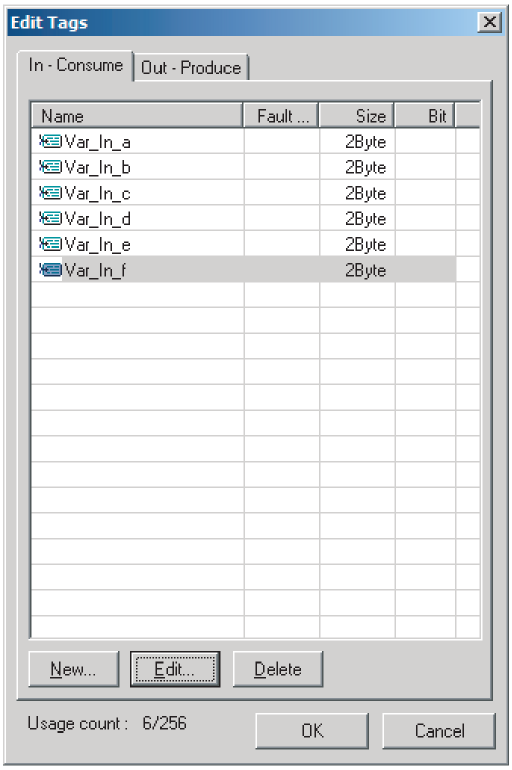
4 To include the Controller status in the tag set, select the **Include** Option for the **Controller Status** at the upper-right corner of the **Edit Tag Set** Dialog Box.



5 To confirm the change, click the **OK** Button in the **Edit Tag Set** Dialog Box.

6 Click the **OK** Button in the **Edit Device Parameters** Dialog Box.

7 If you want to just add a new tag and register it in an existing tag set, first register the new tag by following steps 1 in Creating a Tag Set to 7 in Creating and Adding Tags. In this example, input tags, Var_In_e and Var_In_f, are newly added.

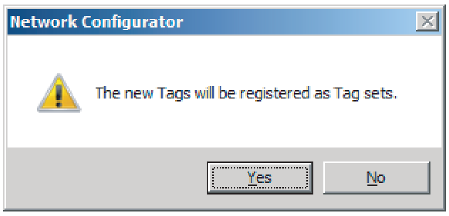


Name	Fault ...	Size	Bit
Var_In_a		2Byte	
Var_In_b		2Byte	
Var_In_c		2Byte	
Var_In_d		2Byte	
Var_In_e		2Byte	
Var_In_f		2Byte	

Usage count : 6/256

8 After you register the tags, click the **OK** Button in the **Edit Tags** Dialog Box.

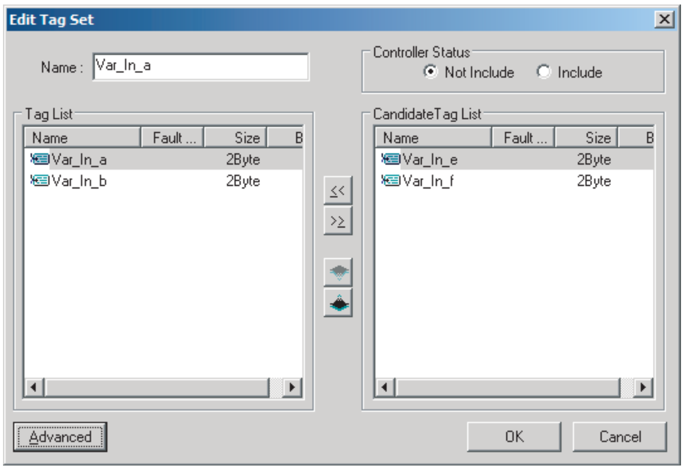
9 At this point, a confirmation dialog box is displayed to check whether you want to use the registered tag names as tag set names. They are supposed to be added as tags in this case, so click the **No** Button. Then, the tags are registered just as tags but not as tag sets.



Network Configurator

The new Tags will be registered as Tag sets.

10 To register the newly added tags in an existing tag set, either double-click the desired tag set, or select the tag set and click the **Edit** Button.



Edit Tag Set

Name : Var_In_a

Controller Status: ● Not Include ○ Include

Tag List

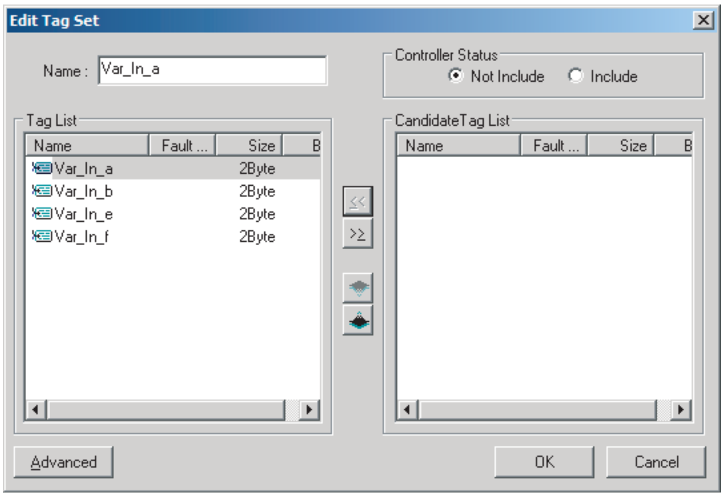
Name	Fault ...	Size	B
Var_In_a		2Byte	
Var_In_b		2Byte	

CandidateTag List

Name	Fault ...	Size	B
Var_In_e		2Byte	
Var_In_f		2Byte	

The Tag List on the left side of the dialog box shows tags that are already registered in the tag set, and the Candidate Tag List on the right side of the dialog box shows the other tags that are not registered yet.

11 Select the tags that you want to add from the Candidate Tag List and click the << Button.



Edit Tag Set

Name : Var_In_a

Controller Status: ● Not Include ○ Include

Tag List

Name	Fault ...	Size	B
Var_In_a		2Byte	
Var_In_b		2Byte	
Var_In_e		2Byte	
Var_In_f		2Byte	

CandidateTag List

Name	Fault ...	Size	B

You can register up to eight tags in a tag set. (If you include the Controller status in the tag set, you can register up to only seven tags, and two bytes are added to the size.)

Tag data is sent and received in the order of tags displayed in the tag list. To change the order of tag data, select a tag and click the ▼ or ▲ Button.

12 To confirm the change, click the **OK** Button in the **Edit Tag Set** Dialog Box.

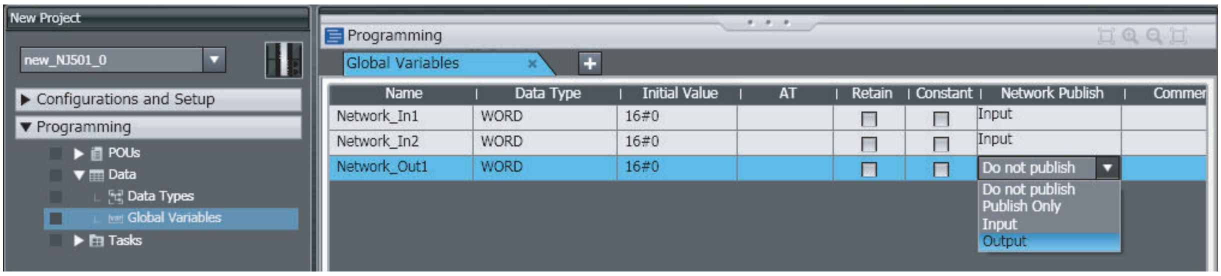
13 Click the **OK** Button in the **Edit Device Parameters** Dialog Box.

Importing Variables with a Network Publish Attribute Created in the Sysmac Studio to the Network Configurator

You can create network variables in the Sysmac Studio and import these variables to the Network Configurator to assign them to tags and tag sets. Use the following procedure.

● Exporting Global Variables on the Sysmac Studio

1 Create a global variable on the global variable table of the Sysmac Studio and select **Input** or **Output** for the Network Publish attribute of the variable.



Name	Data Type	Initial Value	AT	Retain	Constant	Network Publish	Commer
Network_In1	WORD	16#0		☐	☐	Input	
Network_In2	WORD	16#0		☐	☐	Input	
Network_Out1	WORD	16#0		☐	☐	Do not publish	

2 Select **Export Global Variables - Network Configurator...** from the **Tools** Menu.
Any global variables with **Input** or **Output** set for the Network Publish attribute are imported from the csv file through the import procedure described below (Importing to the Network Configurator).

● Importing to the Network Configurator

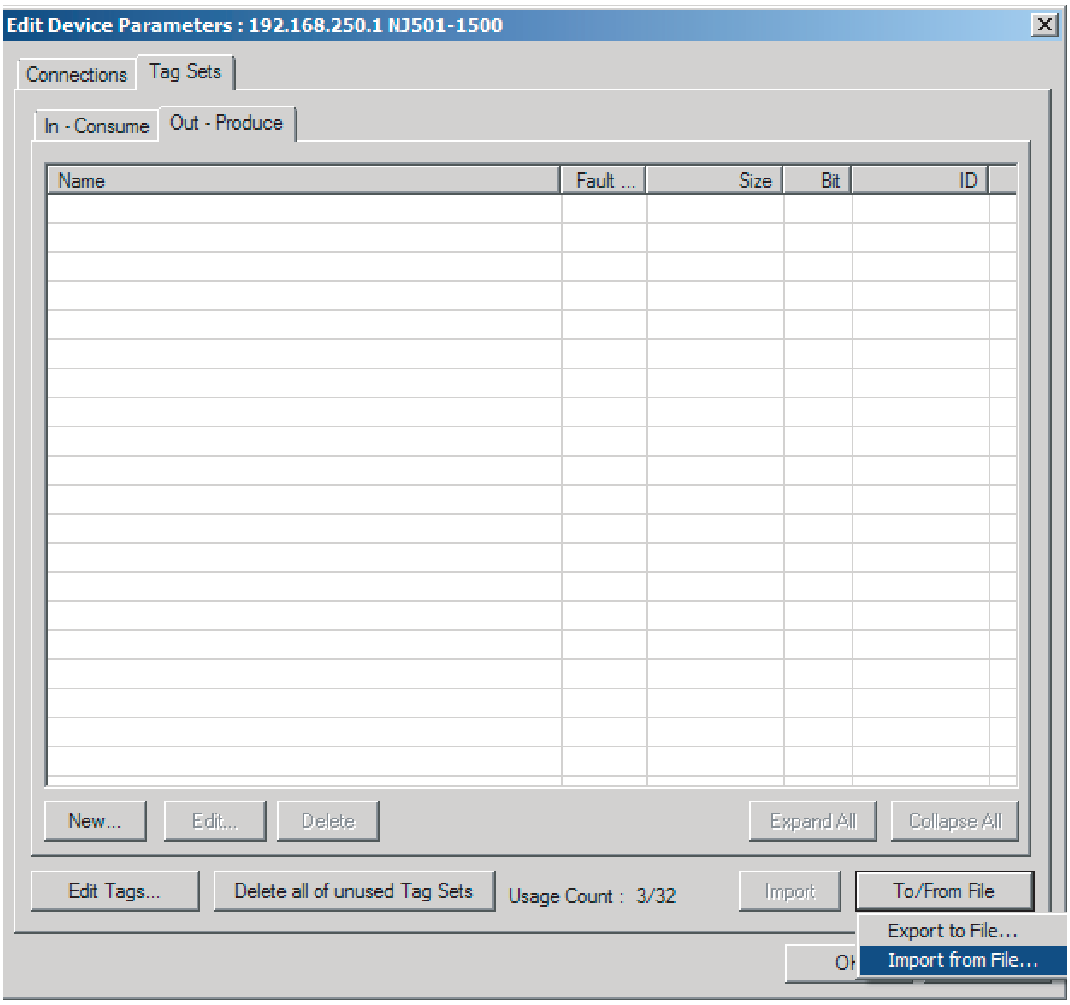
Precautions for Correct Use

Variables with a Network Publish attribute that have variable names that are the same as the I/O memory address notation, such as, "0000" and "H0000" are not exported to CSV files.

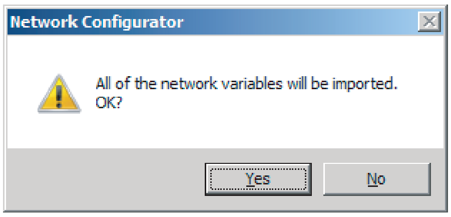
- Variable names that contain only single-byte numerals (Example: 001)
- Variable names with the following single-byte letters (uppercase or lowercase) followed by single-byte numerals
  - H (Example: H30)
  - W (Example: w30)
  - D (Example: D100)
  - E0_ to E18_ (Example: EA_100)

1 From the devices registered on the Network Configurator, select and double-click the icon of the device for which you want to import the variable with a Network Publish attribute. Then, the **Edit Device Parameters** Dialog Box is displayed.
Or, right-click the icon to display the pop-up menu, and select **Device** - **Parameter** - **Edit**.

2 Click the **Tag Sets** Tab at the top of the **Edit Device Parameters** Dialog Box. Select **Import from File** from the **To/From File** Button.

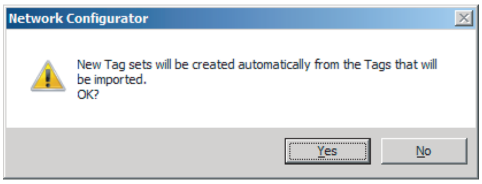


To import all variables with a Network Publish attribute, click the **Yes** Button. To import only some of these variables, click the **No** Button.



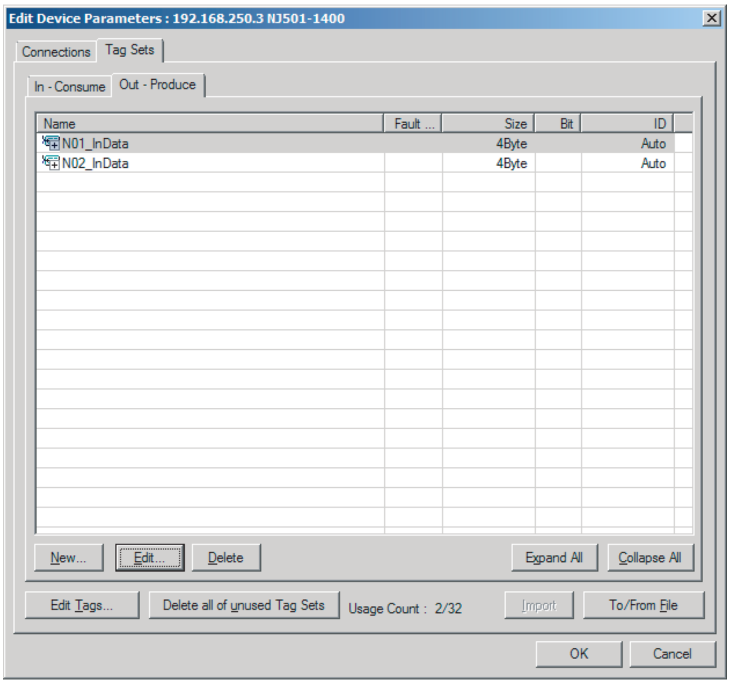
All of the network variables will be imported.
OK?

After you import the variables to the tags, click the **Yes** Button to automatically create tag sets, or click the **No** Button to set up tag sets manually.



New Tag sets will be created automatically from the Tags that will be imported.
OK?

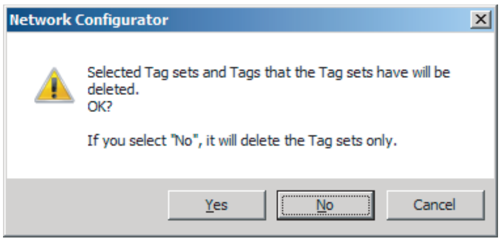
If you select the **Yes** Button in the previous step, the variables will be imported as shown below on the **Tag Sets** Tab Page. Each variable will be imported into a separate tag set and the device parameters will be automatically edited. (The variable name will be used for the tag set name.)



Name	Fault ...	Size	Bit	ID
N01_InData		4Byte		Auto
N02_InData		4Byte		Auto

Usage Count : 2/32

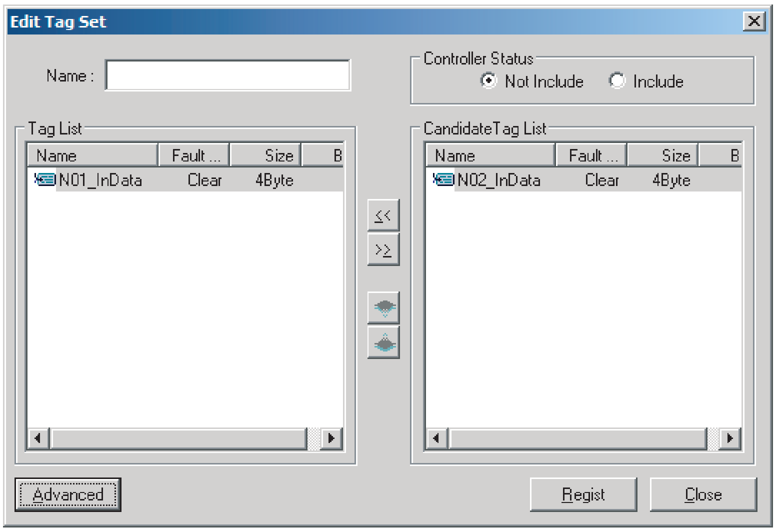
To place more than one input variable (input tag) imported from the Sysmac Studio into one tag set, you must delete the input tags that were registered.
Select the tag set containing the variables you want to put into a tag set, then click the **Delete** Button. A message box is displayed to confirm that you want to delete the selected tag set and the tags contained in that tag set. You only want to delete the tag set, so click the **No** Button.



Selected Tag sets and Tags that the Tag sets have will be deleted.
OK?

If you select "No", it will delete the Tag sets only.

Click the **New** Button to create a new tag set. To place more than one tag in an existing tag set, double-click the tag set, or select it and click the **Edit** Button.
The **Edit Tag Set** Dialog Box is displayed. Imported tags that are not registered in another tag set are displayed in the **Candidate Tag List** on the right side of the **Edit Tag Set** Dialog Box.
Click the Button to add tags individually.



Controller Status: ● Not Include ○ Include

Tag List

Name	Fault ...	Size	B
N01_InData	Clear	4Byte	

CandidateTag List

Name	Fault ...	Size	B
N02_InData	Clear	4Byte	

3. You can change tag set names in this dialog box. To confirm a change, click the **Regist** Button in the **Edit Tag Set** Dialog Box.

4. Perform steps 1 to 3 for all the devices to which tag data links are made to import variables and to create tag sets.

9-2-5 Connection Settings

After you create 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 and tag sets with which connections are opened
- The connection type (multicast or unicast)
- The length of the packet intervals (RPI)
- Connection name (optional)

Make the connections settings on the originator only. The connections settings are not necessary on the target device.

Precautions for Correct Use

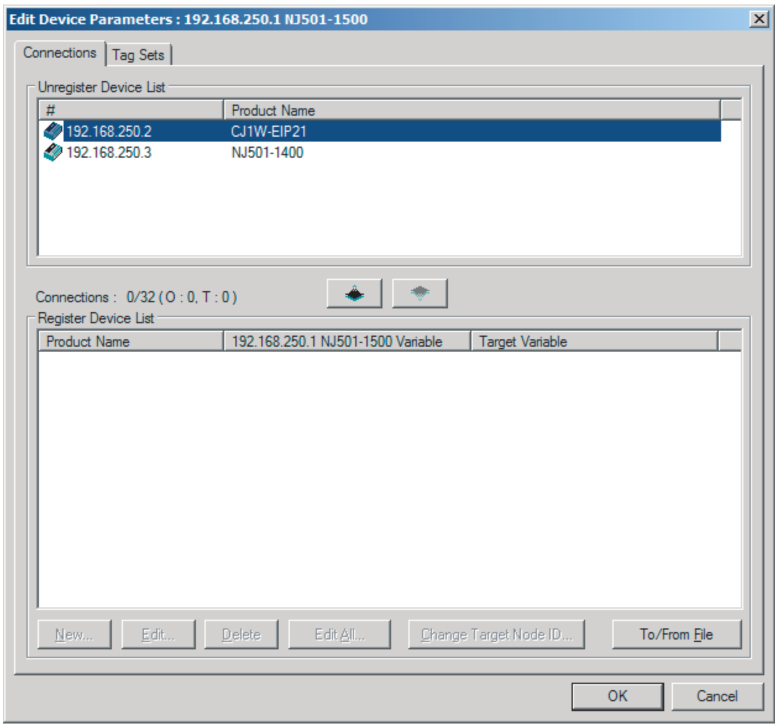
Make the connections settings after you create tag sets for all of the devices involved in tag data links.

Connection Settings (Connections Tab Page)

● Registering Devices in the Register Device List

1. Double-click the icon of the device for which to make originator settings in the Network Configuration Pane of the Network Configurator. The **Edit Device Parameters** Dialog Box is displayed. Or, right-click the icon to display the pop-up menu, and select **Parameter** – **Edit.**

2. Click the **Connections** Tab in the **Edit Device Parameters** Dialog Box.
All of the devices registered in the network (except the local node) are displayed.



Edit Device Parameters : 192.168.250.1 NJ501-1500

Unregister Device List

#	Product Name
192.168.250.2	CJ1W-EIP21
192.168.250.3	NJ501-1400

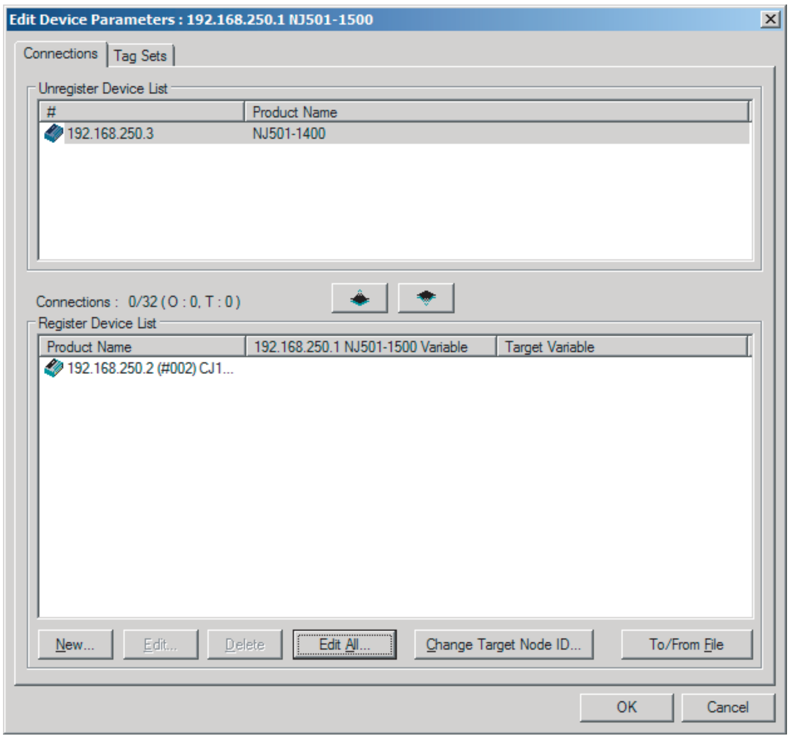
Connections : 0/32 (O : 0, T : 0)

Register Device List

Product Name	192.168.250.1 NJ501-1500 Variable	Target Variable

3 In the **Unregister Device List**, click the target device that requires connection settings so its color changes to gray, and click the ▼ Button.

The selected target device is displayed in the **Register Device List**, as shown below.



Edit Device Parameters : 192.168.250.1 NJ501-1500

Unregister Device List

#	Product Name
192.168.250.3	NJ501-1400

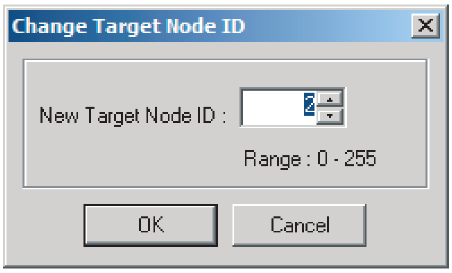
Connections : 0/32 (O : 0, T : 0)

Register Device List

Product Name	192.168.250.1 NJ501-1500 Variable	Target Variable
192.168.250.2 (#002) CJ1...		

4 Target node IDs are assigned to the devices that are registered in the **Register Device List**. The target node ID serves as the bit array position for the following variables in the originator Controller: Target Node Controller Mode, Target Node Controller Error Information, Target

Node Error Information, Registered Target Node Information, and Normal Target Node Information. 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 target node ID is #002. If a target node ID is duplicated and you want to change the target node ID, click the **Change Target Node ID** Button and change the target ID.



Change Target Node ID

New Target Node ID : 2

Range : 0 - 255

Editing Settings for Individual Connections

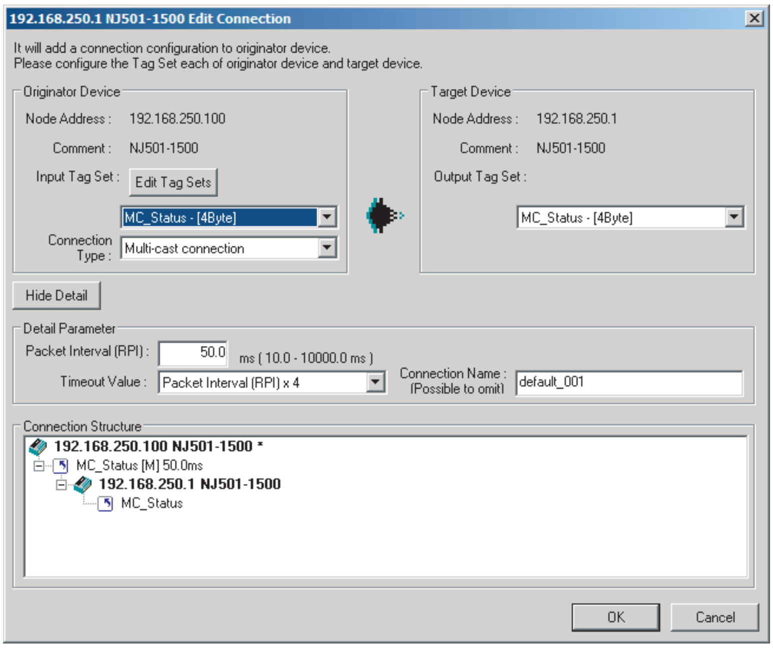
You can edit each connection separately.

Refer to *Editing Settings for All Connections* on page 9-36 for information on how to edit all the connections in a table format.

1 Click the **Connections** Tab and then the click the **New** Button.

The following **Edit Connection** Dialog Box is displayed according to the type of device that is selected.

- (A) Using EtherNet/IP Ports as Targets (for Input Only)



192.168.250.1 NJ501-1500 Edit Connection

It will add a connection configuration to originator device.
Please configure the Tag Set each of originator device and target device.

Originator Device

Node Address : 192.168.250.100

Comment : NJ501-1500

Input Tag Set : MC_Status - [4Byte]

Connection Type : Multi-cast connection

Target Device

Node Address : 192.168.250.1

Comment : NJ501-1500

Output Tag Set : MC_Status - [4Byte]

Detail Parameter

Packet Interval (RPI) : 50.0 ms (10.0 - 10000.0 ms)

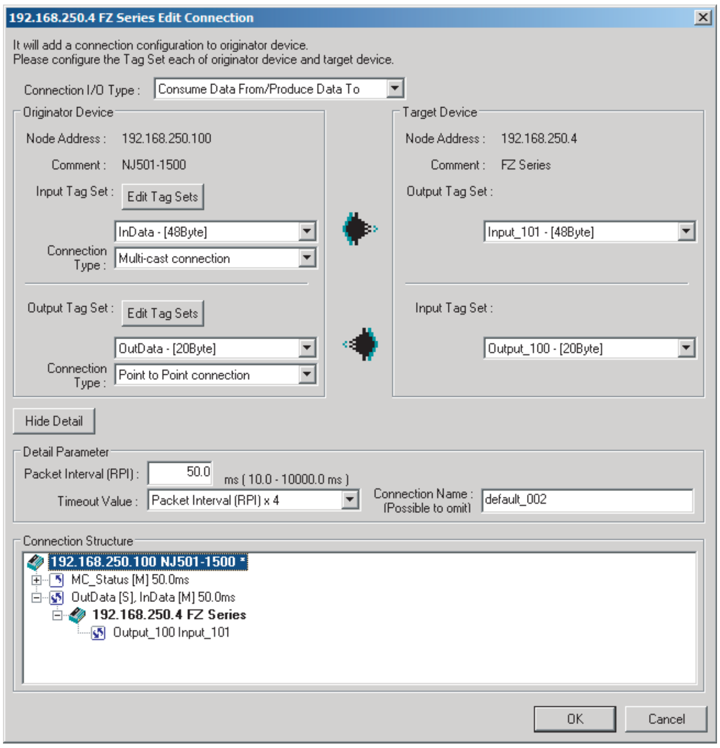
Timeout Value : Packet Interval (RPI) x 4

Connection Name : (Possible to omit) default_001

Connection Structure

192.168.250.100 NJ501-1500 *
MC_Status [M] 50.0ms
192.168.250.1 NJ501-1500
MC_Status

- (B) Using Other EtherNet/IP Devices as Targets (for Settings Other Than Input Only)


192.168.250.4 FZ Series Edit Connection

It will add a connection configuration to originator device.
Please configure the Tag Set each of originator device and target device.

Connection I/O Type : Consume Data From/Produce Data To

Originator Device
Node Address : 192.168.250.100
Comment : NJ501-1500
Input Tag Set : InData - [48Byte]
Connection Type : Multi-cast connection
Output Tag Set : OutData - [20Byte]
Connection Type : Point to Point connection

Target Device
Node Address : 192.168.250.4
Comment : FZ Series
Output Tag Set : Input_101 - [48Byte]
Input Tag Set : Output_100 - [20Byte]

Detail Parameter
Packet Interval (RPI) : 50.0 ms (10.0 - 10000.0 ms)
Timeout Value : Packet Interval (RPI) x 4
Connection Name : (Possible to omit) default_002

Connection Structure
192.168.250.100 NJ501-1500 *
MC_Status [M] 50.0ms
OutData [S], InData [M] 50.0ms
192.168.250.4 FZ Series
Output_100 Input_101

The settings are as follows:

Setting	Description
Connection I/O Type	Select **Input Only (Tag type)** to use tag data links with an NX-EIP201, CS1W-EIP21, CJ1W-EIP21, CJ2B-EIP21, CJ2M-EIP21, CJ1W-EIP21(CJ2), CJ1W-EIP21(NJ), NX701, NX102-□□□□, NX1P2, NJ501-□□□□, NJ301-□□□□, or NJ101 CPU Unit. When you create tag data links for 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 a Tag type setting.
Connection Type	Select whether the data is sent in multicast or unicast (point-to-point) form. The default setting is multicast. • Multi-cast connection: Select when the same data is shared by multiple nodes. This setting is usually used. • Point-to-point connection: Select when the same data is not shared by multiple nodes. In a unicast transmission, other nodes are not burdened with an unnecessary load. Refer to *9-1-4 Overview of Operation* on page 9-7 for details on using multi-cast and unicast connections, and counting the number of connections.
The **Connection Structure** Area and the following items are not displayed if the **Hide Detail** Button is clicked.	
Packet Interval (RPI)[*1]	Set the data update cycle (i.e., the packet interval) of each connection between the originator and target. The default setting is 50 ms (i.e., data is updated once every 50 ms). Set the RPI between 1.0 and 10,000 ms in 1.0-ms increments.

Setting	Description
Timeout Value	Set the time elapsed until a connection timeout is detected. 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).
Connection Name	Set a name for the connection. (32 single-byte characters max.)

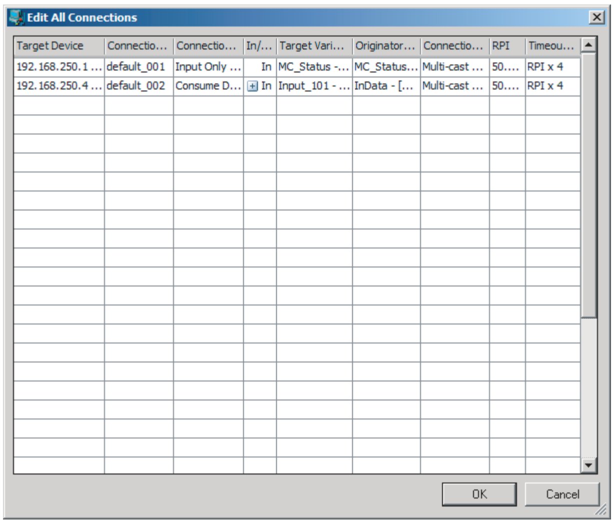
*1. The approximate I/O response time of the tag data link is determined by the relationship between the packet interval and the number of connections. Refer to *12-3 Tag Data Link I/O Response Time* on page 12-23 for details.

2 After you make all of the settings, click the **OK** Button.

● Editing Settings for All Connections

You can edit the connection settings between the originator and all of the target devices selected in the Register Device List together in a table.

1 Click the **Connections** Tab, and then click the **Edit All** Button.
The following **Edit All Connections** Dialog Box is displayed.



Edit All Connections

Target Device	Connectio…	Connectio…	In/…	Target Vari…	Originator…	Connectio…	RPI	Timeou…
192.168.250.1 …	default_001	Input Only …	In	MC_Status -…	MC_Status…	Multi-cast …	50.…	RPI x 4
192.168.250.4 …	default_002	Consume D…	⊞ In	Input_101 - …	InData - […	Multi-cast …	50.…	RPI x 4

The settings are as follows:

Setting	Description
Target Device	Select the target device.
Connection Name	Any name can be given to the connection. (32 single-byte characters max.) If this field is left blank, a default name is assigned. The connection name is used as a comment.
Connection I/O Type	Select **Input Only (Tag type)** to use tag data links with an NX-EIP201, CS1W-EIP21, CJ1W-EIP21, CJ2B-EIP21, CJ2M-EIP21, CJ1W-EIP21 (CJ2), CJ1W-EIP21 (NJ), NX701, NX502-□□□□, NX102-□□□□, NX1P2, NJ501-□□□□, NJ301-□□□□, or NJ101 CPU Unit. When you create tag data links for 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 a Tag type setting.

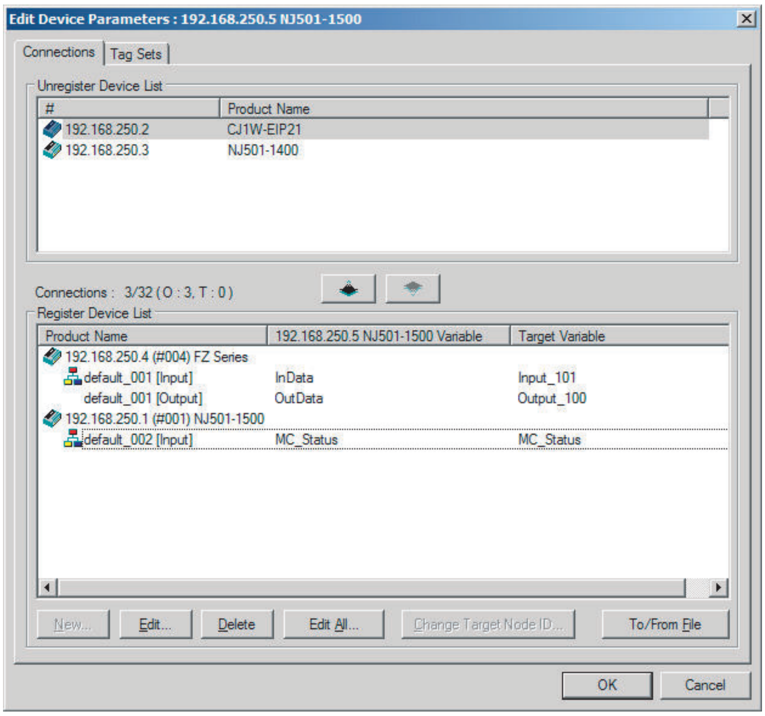
Setting	Description
In/Out	The connection's I/O is automatically displayed based on the selected connection. Input Only: Just In is displayed.
Target Variable	Select the target node's tag set to assign. • In: Select the target's output (produce) tag set. • Out: Select the target's input (consume) tag set.
Originator Variable	Select the originator node's tag set to assign. • In: Select the originator's input (consume) tag set. • Out: Select the originator's output (produce) tag set.
Connection Type	Select whether the data is sent in multi-cast or unicast (point-to-point) form. The default setting is multi-cast. • Multi-cast connection: Select when the same data is shared by multiple nodes. This setting is usually used. • Point-to-point connection: Select when the same data is not shared by multiple nodes. In a unicast transmission, other nodes are not burdened with an unnecessary load. Refer to *9-1-4 Overview of Operation* on page 9-7 for details on using multi-cast and unicast connections, and counting the number of connections.
RPI[*1]	Set the data update cycle (i.e., the packet interval) of each connection between the originator and target. The default setting is 50 ms (i.e., data is updated once every 50 ms). Set the RPI between 1.0 and 10,000 ms in 1.0-ms increments.
Timeout Value	Set the time elapsed until a connection timeout is detected. 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).

[*1] The approximate I/O response time of the tag data link is determined by the relationship between the packet interval and the number of connections. Refer to *12-3 Tag Data Link I/O Response Time* on page 12-23 for details.

2 After you make all of the settings, Click the **OK** Button.

● Confirming the Connection Settings

1 An overview of the connections that were set in the Register Device List is displayed in the Connections Tab Page.



Unregister Device List

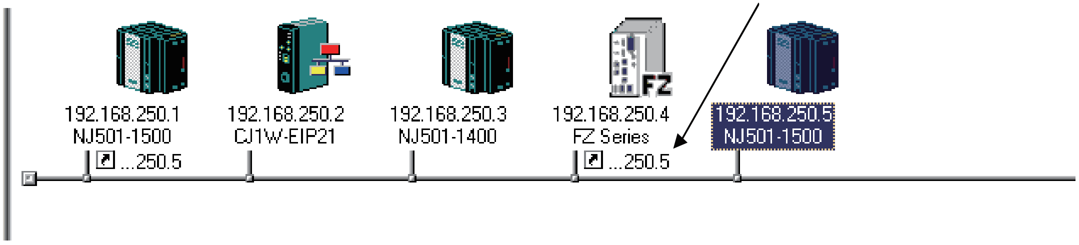
#	Product Name
192.168.250.2	CJ1W-EIP21
192.168.250.3	NJ501-1400

Connections : 3/32 (O : 3, T : 0)

Register Device List

Product Name	192.168.250.5 NJ501-1500 Variable	Target Variable
192.168.250.4 (#004) FZ Series		
default_001 [Input]	InData	Input_101
default_001 [Output]	OutData	Output_100
192.168.250.1 (#001) NJ501-1500		
default_002 [Input]	MC_Status	MC_Status

2 Click the **OK** Button. The following figure is displayed.



Indicates the IP address of the originator where the connection was set.

3 Repeat the connections setting procedure until all of the connections are set.

Precautions for Correct Use

After you have made all of the settings, always click the **OK** Button before you close the **Edit Device Parameters** Dialog Box. If the **Cancel** Button is clicked and the dialog box is closed, all the settings you made here are discarded.

4 If you change the size of a tag set for the originator or a target node after the connection settings, a parameter data mismatch will occur due to the size difference between them.
if you change the connection settings, be sure to check the connections. (Refer to *9-2-16 Checking Connections* on page 9-69 for details.)

Automatically Setting Connections (Network - Auto Connection)

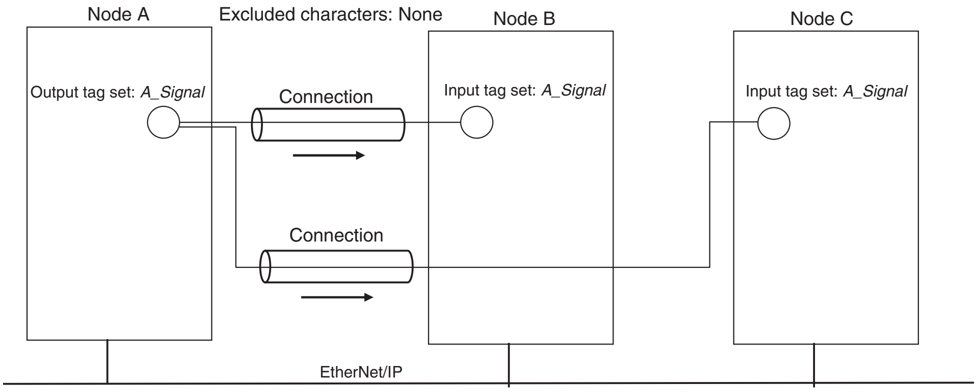
You can use automatic detection of the tag set names that are set for devices to automatically set connections between input and output tag sets with the same name (or the same names excluding specified ellipses).

Connections are automatically set under the following conditions.

Output tag set names for connection setting	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 for connection settings	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 type	The connection I/O type must be Input Only. Multicast or unicast connections can be specified for a connection.
RPI	The default setting is used.
Timeout	The default setting is used.

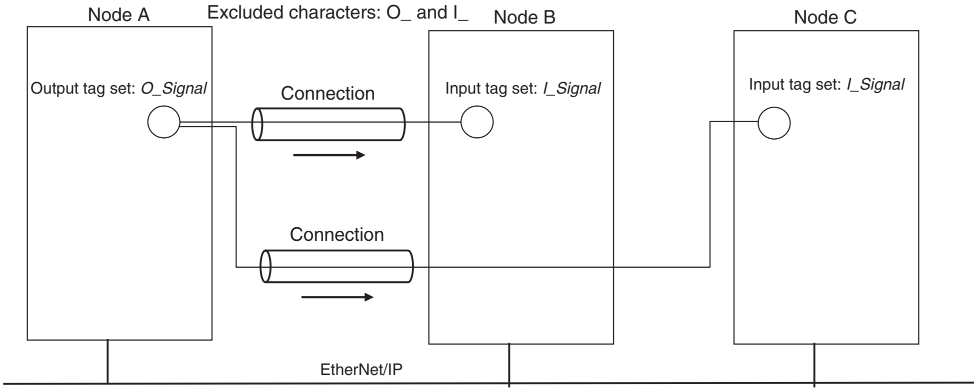
Example 1: Automatic Connections with the Same Tag Set Names

The following connections are automatically set with the same tag set name (*A_Signal*) if there is an output (produce) tag set named *A_Signal* at node A, and input (consume) tag sets named *A_Signal* at nodes B and C.


Node A
Excluded characters: None
Node B
Node C
Output tag set: *A_Signal*
Connection
Input tag set: *A_Signal*
Input tag set: *A_Signal*
Connection
EtherNet/IP

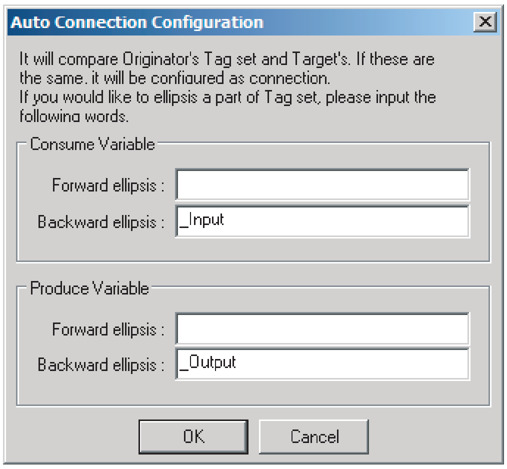
Example 2: Automatic Connections with the Ellipses

The following connections are automatically set with the same tag set name (*Signal*) if there is an output (produce) tag set named *O_Signal* at node A, and input (consume) tag sets named *I_Signal* at nodes B and C, and *O_* and *I_* are set as forward ellipses.


Node A
Excluded characters: O_ and I_
Node B
Node C
Output tag set: *O_Signal*
Connection
Input tag set: *I_Signal*
Input tag set: *I_Signal*
Connection
EtherNet/IP

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 Configuration** from the **Network** Menu.
A dialog box will appear to set forward and backward ellipses for both output and input tag sets as soon as automatic connection setting processing starts.


Auto Connection Configuration

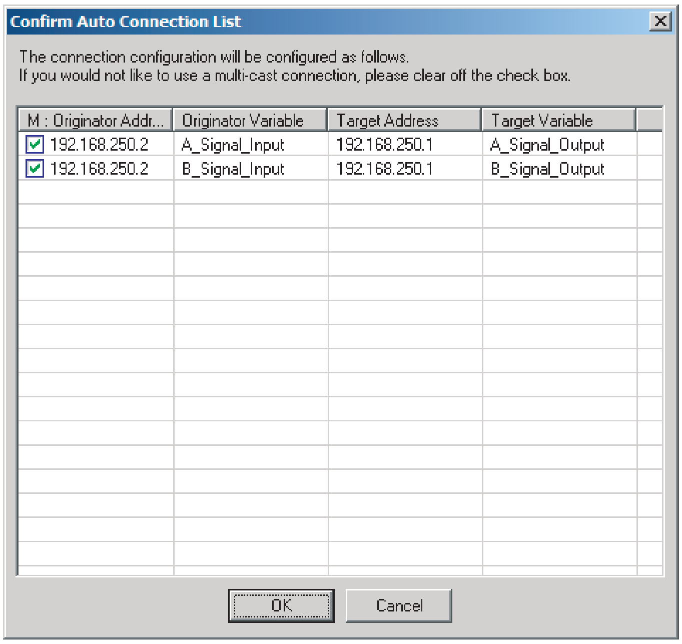
It will compare Originator's Tag set and Target's. If these are the same, it will be configured as connection.
If you would like to ellipsis a part of Tag set, please input the following words.

Consume Variable
Forward ellipsis :
Backward ellipsis : _Input

Produce Variable
Forward ellipsis :
Backward ellipsis : _Output

Input the ellipses and click the **OK** Button. Processing for automatic setting is started.

3 If there are tag sets that meet the conditions for automatic connection setting, they are displayed.



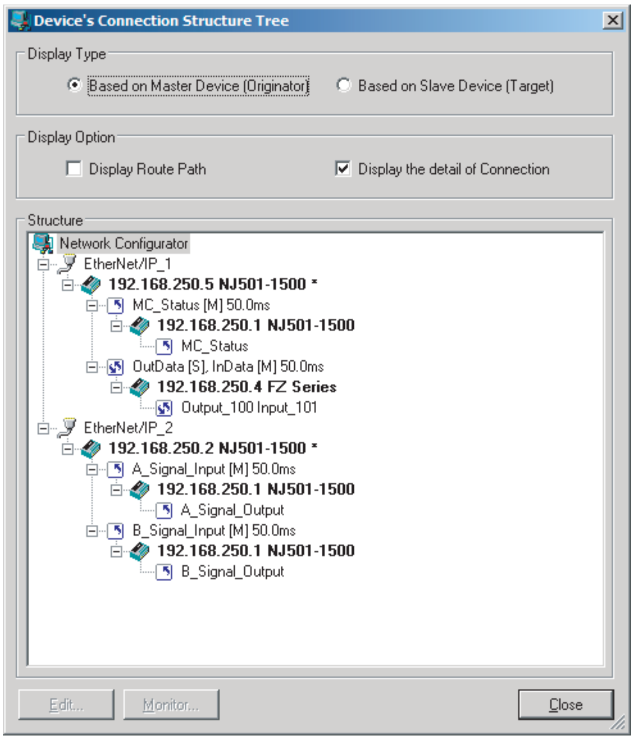
Confirm Auto Connection List

The connection configuration will be configured as follows.
If you would not like to use a multi-cast connection, please clear off the check box.

M : Originator Addr...	Originator Variable	Target Address	Target Variable
☑ 192.168.250.2	A_Signal_Input	192.168.250.1	A_Signal_Output
☑ 192.168.250.2	B_Signal_Input	192.168.250.1	B_Signal_Output

Click the **OK** Button. Processing for automatic setting is started.

4 A device connection structure tree is displayed when processing is completed.



Device's Connection Structure Tree

Display Type
● Based on Master Device (Originator) ○ Based on Slave Device (Target)

Display Option
☐ Display Route Path ☑ Display the detail of Connection

Structure

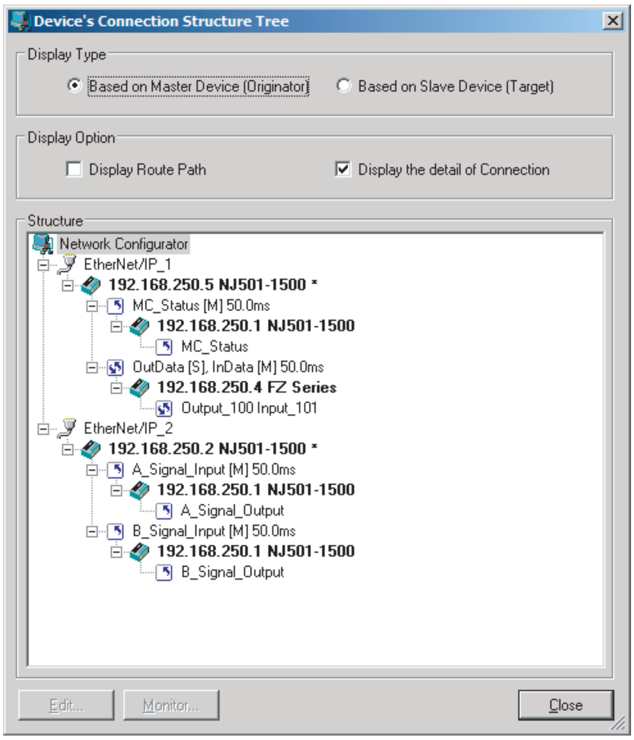
```
Network Configurator
  EtherNet/IP_1
    192.168.250.5 NJ501-1500 *
      MC_Status [M] 50.0ms
        192.168.250.1 NJ501-1500
          MC_Status
      OutData [S], InData [M] 50.0ms
        192.168.250.4 FZ Series
          Output_100 Input_101
  EtherNet/IP_2
    192.168.250.2 NJ501-1500 *
      A_Signal_Input [M] 50.0ms
        192.168.250.1 NJ501-1500
          A_Signal_Output
      B_Signal_Input [M] 50.0ms
        192.168.250.1 NJ501-1500
          B_Signal_Output
```

5 Use the device connection structure tree to change the RPI and timeout settings if necessary.

Device Connection Structure Tree

Connection settings can be displayed on the network configuration.

Select **View Device's Connection Structure Tree** from the **Network** Menu.



Display Type

● Based on Master Device (Originator) ○ Based on Slave Device (Target)

Display Option

☐ Display Route Path ☑ Display the detail of Connection

Structure

```
Network Configurator
⊟ EtherNet/IP_1
    ⊟ 192.168.250.5 NJ501-1500 *
        ⊟ MC_Status [M] 50.0ms
            ⊟ 192.168.250.1 NJ501-1500
                MC_Status
        ⊟ OutData [S], InData [M] 50.0ms
            ⊟ 192.168.250.4 FZ Series
                Output_100 Input_101
⊟ EtherNet/IP_2
    ⊟ 192.168.250.2 NJ501-1500 *
        ⊟ A_Signal_Input [M] 50.0ms
            ⊟ 192.168.250.1 NJ501-1500
                A_Signal_Output
        ⊟ B_Signal_Input [M] 50.0ms
            ⊟ 192.168.250.1 NJ501-1500
                B_Signal_Output
```

- You can check the **Display the detail of Connection** Check Box to switch between device-level and connection-level views of tag data link communications.
- An asterisk is displayed after the device name of the originator set for the connection.
- The **Edit Device Parameters** Dialog Box is displayed if you select a connection and click the **Edit** Button. You can edit the connections in this dialog box.

9-2-6 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.

Additional Information

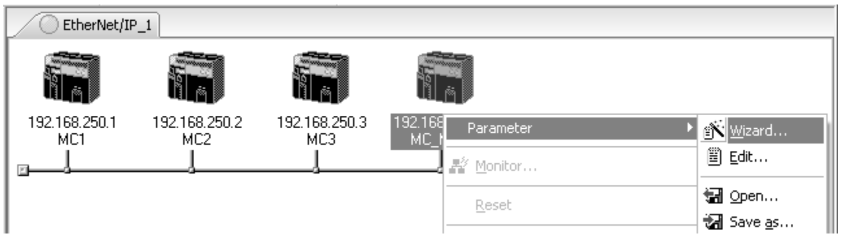
The Wizard can be used only with the following OMRON EtherNet/IP devices.

Device name	Remarks
NX-EIP201	EtherNet/IP port in NX-series EtherNet/IP Unit
CJ1W-EIP21 (NJ)	CJ1W-EIP21 mounted to NJ-series Controller
CJ1W-EIP21	CJ1W-EIP21 mounted to CJ1 CPU Unit
CJ1W-EIP21 (CJ2)	CJ1W-EIP21 mounted to CJ2 CPU Unit
CJ2B-EIP21	Built-in EtherNet/IP port in CJ2H CPU Unit
CJ2M-EIP21	Built-in EtherNet/IP port in CJ2M CPU Unit
CS1W-EIP21	CS1W-EIP21 mounted to CS1 CPU Unit
NX701	Built-in EtherNet/IP port on NX-series CPU Unit
NX502-□□□□	
NX102-□□□□	
NX1P2	
NJ501-□□□□	Built-in EtherNet/IP port on NJ-series CPU Unit
NJ301-□□□□	
NJ101	

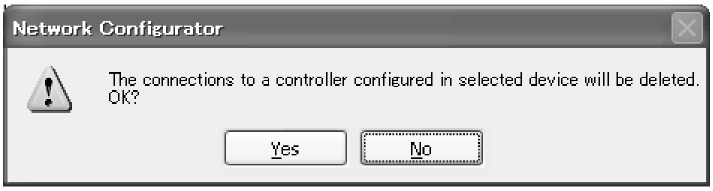
Use the following procedure to create connections (i.e., tag data links) with the Wizard.

1 Set tags and tag sets for all the devices before starting the Wizard. Refer to *9-2-4 Creating Tags and Tag Sets* on page 9-19 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 menu.



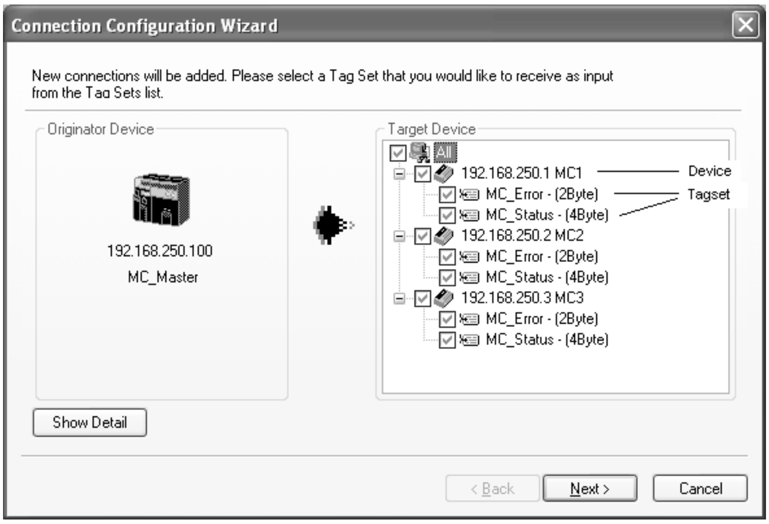
The following message box will be displayed before the Wizard starts.



The connections to a controller configured in selected device will be deleted. OK?

Click the **Yes** Button to delete the connections that are 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.)



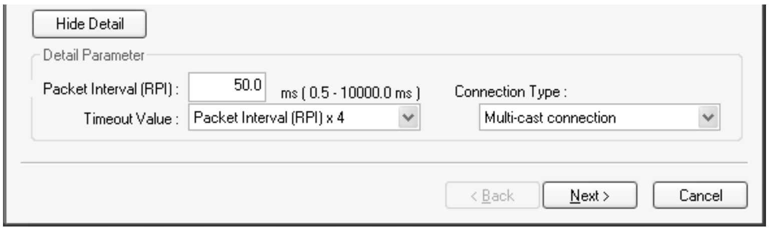
New connections will be added. Please select a Tag Set that you would like to receive as input from the Tag Sets list.

4 A list of tag sets is displayed on the right side of the Wizard with target devices that support receiving input data.
Select the tag sets that you want to receive at the originator device.
The following table 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 used in connections that are already set are not displayed.

The following display will appear when you click the **Show Detail** Button.

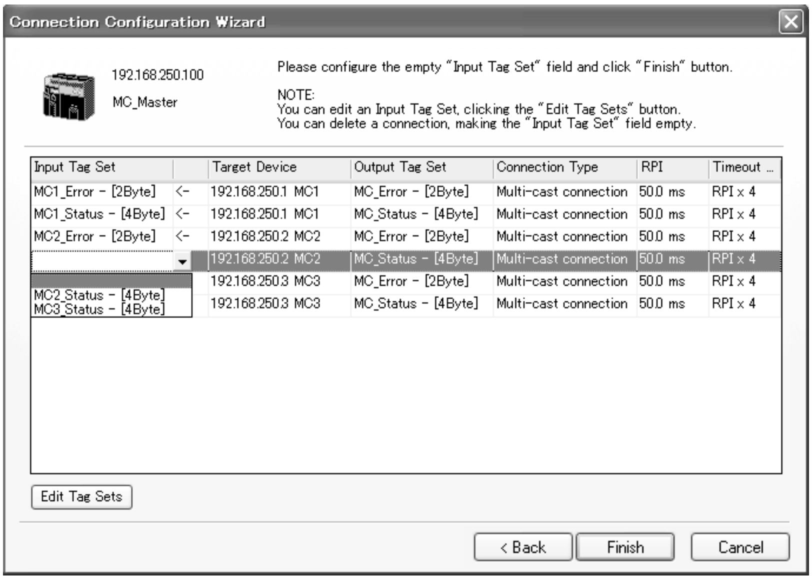


Packet Interval (RPI) : 50.0 ms (0.5 - 10000.0 ms)
Timeout Value : Packet Interval (RPI) x 4
Connection Type : Multi-cast connection

The preset 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 the input tag set of the originator device that receives the output tag set of the target device from the list box.



Please configure the empty "Input Tag Set" field and click "Finish" button.

NOTE:
You can edit an Input Tag Set, clicking the "Edit Tag Sets" button.
You can delete a connection, making the "Input Tag Set" field empty.

Input Tag Set		Target Device	Output Tag Set	Connection Type	RPI	Timeout ...
MC1_Error - [2Byte]	<-	192.168.250.1 MC1	MC_Error - [2Byte]	Multi-cast connection	50.0 ms	RPI x 4
MC1_Status - [4Byte]	<-	192.168.250.1 MC1	MC_Status - [4Byte]	Multi-cast connection	50.0 ms	RPI x 4
MC2_Error - [2Byte]	<-	192.168.250.2 MC2	MC_Error - [2Byte]	Multi-cast connection	50.0 ms	RPI x 4
		192.168.250.2 MC2	MC_Status - [4Byte]	Multi-cast connection	50.0 ms	RPI x 4
		192.168.250.3 MC3	MC_Error - [2Byte]	Multi-cast connection	50.0 ms	RPI x 4
		192.168.250.3 MC3	MC_Status - [4Byte]	Multi-cast connection	50.0 ms	RPI x 4

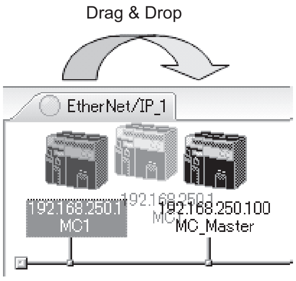
- The blank area in the Input Tag Set Column is for the connection that you are creating.
- For the connections that are already set, values are already given in the Input Tag Set Column.
- To prevent duplicate settings, input tag sets that are used are not displayed in the list box for input tag sets.
- 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 the **Edit Tag** Button.

6 Once the input tag set settings are completed, click the **Finish** Button. You can check the set connection by selecting **Network** - **View Devices Connection Structure Tree** from the menu.

- 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.

9-2-7 Creating Connections by Dragging and Dropping Devices

You can create a connection to the originator by dragging a target device and dropping it at the originator device.
Example) Drag the target device at 192.168.250.1 and drop it at the originator device at 192.168.250.100.



Additional Information

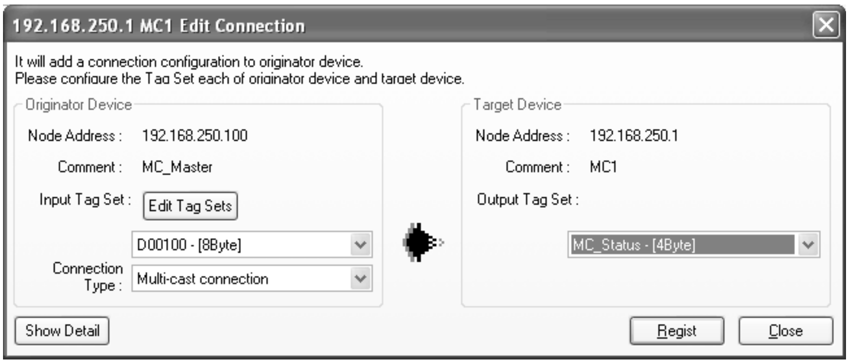
The EtherNet/IP originator device (i.e., a device in which connections can be set) must be one of the following OMRON EtherNet/IP devices.

Device name	Remarks
NX-EIP201	EtherNet/IP port on NX-series EtherNet/IP Unit
CJ1W-EIP21 (NJ)	CJ1W-EIP21 mounted to NJ-series Controller
CJ1W-EIP21	CJ1W-EIP21 mounted to CJ1 CPU Unit
CJ1W-EIP21 (CJ2)	CJ1W-EIP21 mounted to CJ2 CPU Unit
CJ2B-EIP21	Built-in EtherNet/IP port in CJ2H CPU Unit
CJ2M-EIP21	Built-in EtherNet/IP port in CJ2M CPU Unit
CS1W-EIP21	CS1W-EIP21 mounted to CS1 CPU Unit
NX701	Built-in EtherNet/IP port on NX-series CPU Unit
NX502-□□□□	
NX102-□□□□	
NX1P2	
NJ501-□□□□ NJ301-□□□□ NJ101	Built-in EtherNet/IP port on NJ-series CPU Unit

Use the following procedure to create connections (i.e., tag data links) by dragging and dropping devices.

1 Set the tags and tag sets for the target device that will be dragged.
- Refer to *9-2-4 Creating Tags and Tag Sets* on page 9-19 for information on the settings if the target is one of the OMRON EtherNet/IP devices given above.
- 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.
- Using One of the Above OMRON EtherNet/IP Devices As Target



It will add a connection configuration to originator device.
Please configure the Tag Set each of originator device and target device.

Originator Device

Node Address : 192.168.250.100
Comment : MC_Master
Input Tag Set : D00100 - [8Byte]
Connection Type : Multi-cast connection

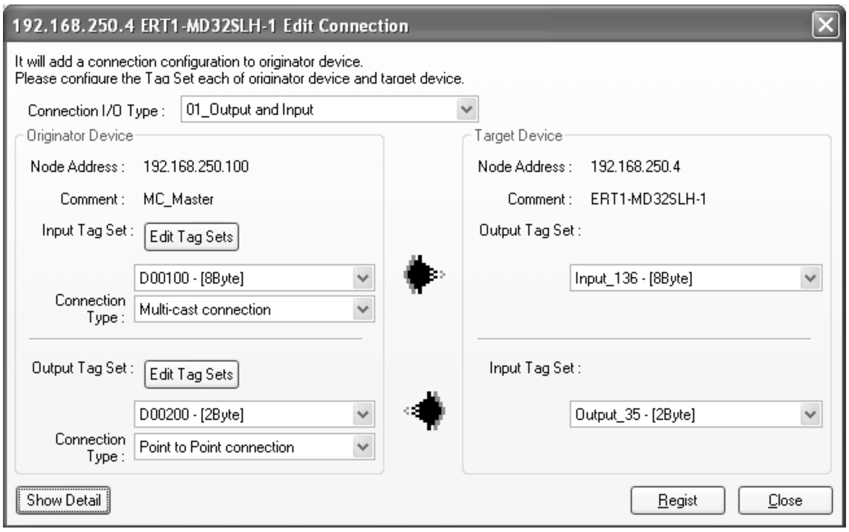
Target Device

Node Address : 192.168.250.1
Comment : MC1
Output Tag Set : MC_Status - [4Byte]

Select an output tag set from the **Target Device** Area on the right side of the **Edit Connection** Dialog Box, and then select an 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 the **Edit Tag** Button.

- Using Other EtherNet/IP Devices as Target



It will add a connection configuration to originator device.
Please configure the Tag Set each of originator device and target device.

Connection I/O Type : 01_Output and Input

Originator Device

Node Address : 192.168.250.100
Comment : MC_Master
Input Tag Set : D00100 - [8Byte]
Connection Type : Multi-cast connection
Output Tag Set : D00200 - [2Byte]
Connection Type : Point to Point connection

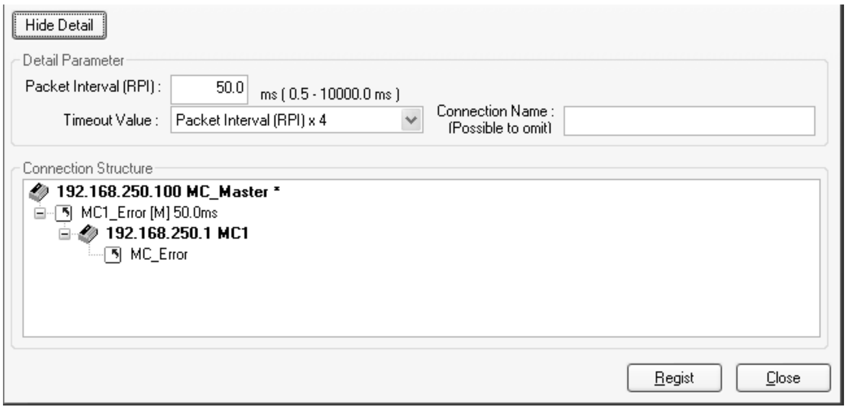
Target Device

Node Address : 192.168.250.4
Comment : ERT1-MD32SLH-1
Output Tag Set : Input_136 - [8Byte]
Input Tag Set : Output_35 - [2Byte]

The **Connection I/O Type** list box in the upper part of the **Edit Connection** Dialog Box lists connection I/O types. Select a 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 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 the **Edit Tag** Button.

The following view will appear when you click the **Show Detail** Button.



Packet Interval (RPI) : 50.0 ms (0.5 - 10000.0 ms)

Timeout Value : Packet Interval (RPI) x 4

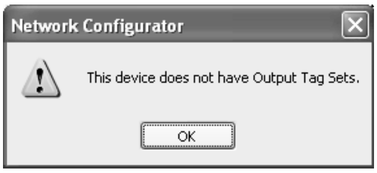
Connection Name : (Possible to omit)

```
192.168.250.100 MC_Master *
  MC1_Error [M] 50.0ms
    192.168.250.1 MC1
      MC_Error
```

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)

Additional Information

The following dialog box will be displayed if a target device that does not have I/O data is dropped.



This device does not have Output Tag Sets.

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 complete the settings, click the **Regist** Button to create the connection. When the connection is completed, the input tag set box and the output tag set box will be blank. You can continue to create another connection by selecting a next connection I/O type and setting a tag set.

9-2-8 Connecting the Network Configurator to the Network

This section describes how to connect the Network Configurator to the network.

Precautions for Correct Use

Connection may not be possible if the following settings are made on an NJ/NX-series Controller on the connection path or on a connection destination NJ/NX-series Controller. If connection fails, check the following settings. For the details on the settings, refer to *CIP Message Server* on page 7-15 and *Packet Filter* on page 7-7.

- The **Do not use** Option is selected for the CIP message server.
- The **Use** Option is selected for Packet Filter.

Additional Information

Although the NX-series EtherNet/IP Unit provides two EtherNet/IP ports, the Network Configurator treats these two ports as two different Units and connects them individually.

Connecting through Ethernet

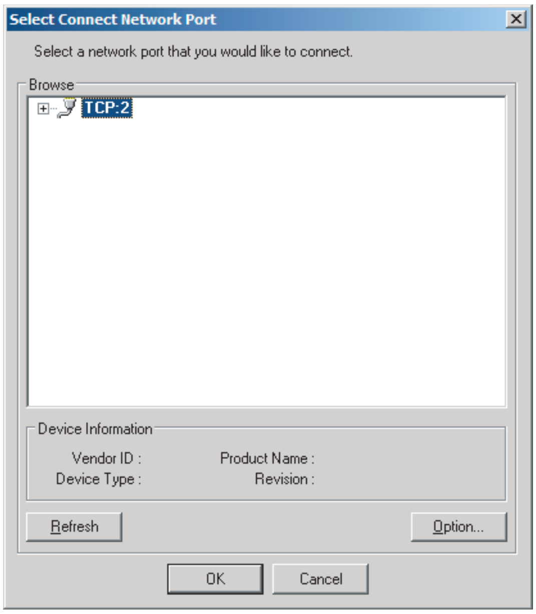
Connect to the EtherNet/IP port on the CPU Unit or NX-series EtherNet/IP Unit via an Ethernet switch.

Precautions for Correct Use

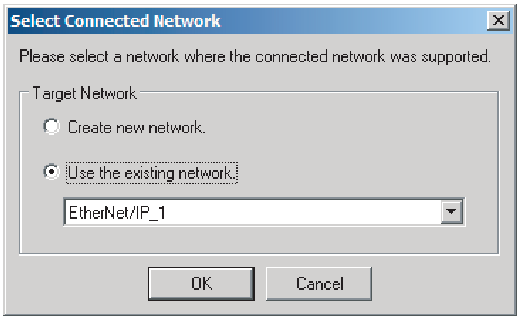
The first time you connect via Ethernet with the computer to use, you must change the Windows firewall settings.
For the procedure, refer to *A-5 Precautions for Using the Network Configurator on Windows XP, Windows Vista, or Windows 7 or Higher* on page A-47.

1. Select **Option** - **Select Interface** - **Ethernet I/F**.

2. Select **Network** - **Connect**.
   If there are multiple Ethernet interfaces on the computer, the **Select Interface** Dialog Box is displayed. Select the interface to connect, and press the **OK** Button.
   The following dialog box is displayed.

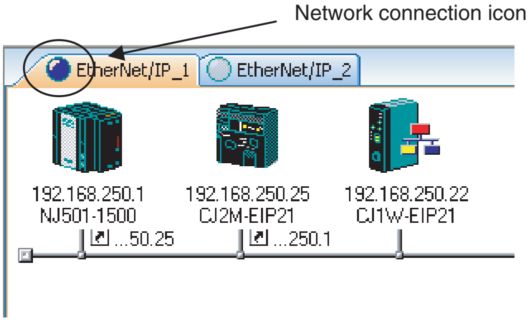


3. Click the **OK** Button.
   Select the network to connect to.

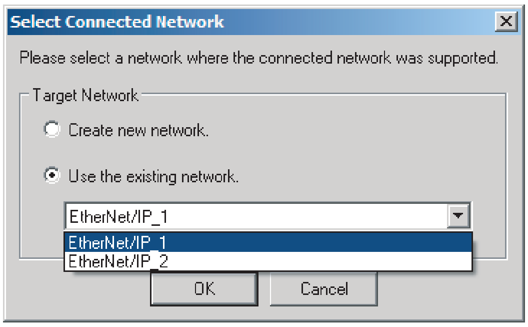

Select Connected Network
Please select a network where the connected network was supported.
Target Network
○ Create new network.
● Use the existing network.
EtherNet/IP_1
OK
Cancel

The Network Configurator will connect to the EtherNet/IP network. If the Network Configurator goes online normally, **On-line** is displayed in the status bar at the bottom of the window.

The network connection icon is displayed in blue on the Network Tab Page in which the Network Configurator is connected.



Select **Network** - **Change Connect Network** to switch the connected network.


Select Connected Network

Please select a network where the connected network was supported.

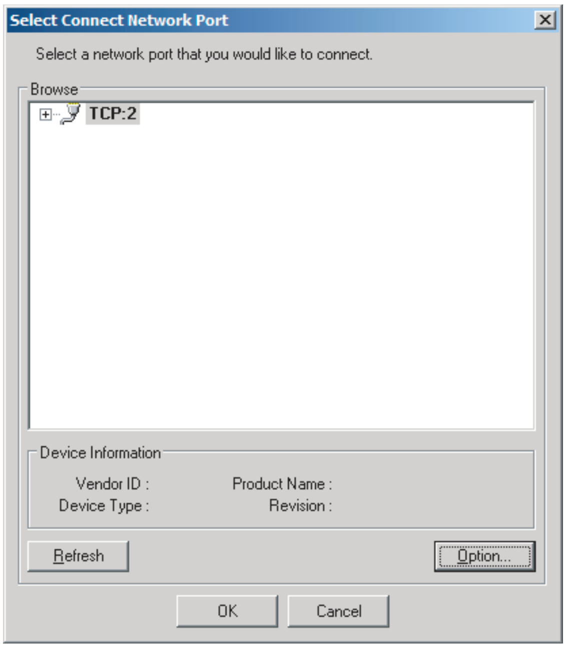
Target Network

○ Create new network.

● Use the existing network.

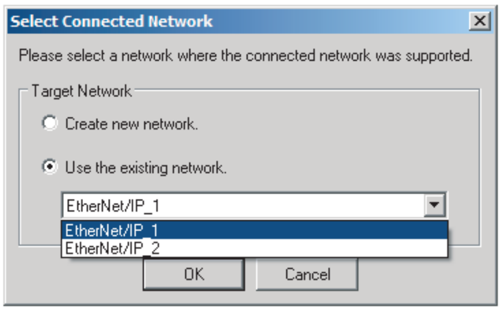
EtherNet/IP_1

4 The following dialog box is displayed.


Select Connect Network Port

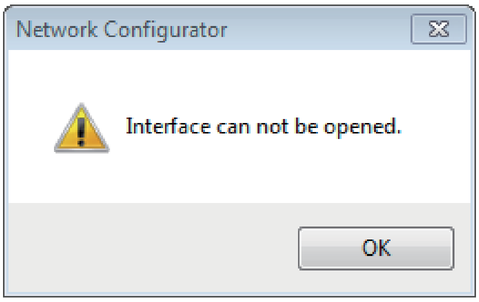
Select a network port that you would like to connect.

5 Click the **OK** Button.
Select the network to connect to.



Additional Information

If the following dialog box appears in the Network Configurator when you go online with an NX-series EtherNet/IP Unit, refer to the following table for possible causes and corrections.



Interface can not be opened.

Assumed cause	Correction
The cable is not connected correctly.	Check if the cable is disconnected or loose.
Connection with the Controller is blocked due to the firewall settings.	If connection with the Controller is blocked due to the firewall settings, disable the blocking. For the firewall settings, refer to *A-5 Precautions for Using the Network Configurator on Windows XP, Windows Vista, or Windows 7 or Higher* on page A-47.
Communications with Network Configurator are blocked due to Packet Filter of the Controller.	Allow communications with Network Configurator. For details on Packet Filter settings, refer to *Packet Filter* on page 7-7.
The server function of CIP message communications is disabled.	Enable the server function of CIP message communications. Refer to *CIP Message Server* on page 7-15 for details on setting CIP message server.

9-2-9 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 are transferred to the EtherNet/IP devices that require the settings.

The following procedure shows how to download the tag data link parameters.
For details on how to connect to the network from the Network Configurator, refer to *9-2-8 Connecting the Network Configurator to the Network* on page 9-48.

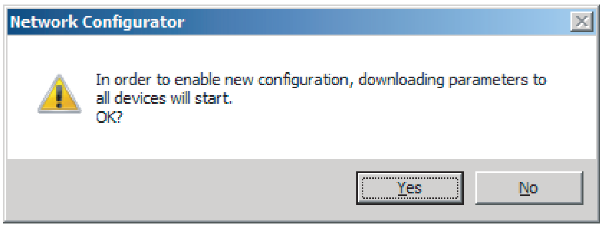
Precautions for Correct Use

- If the node addresses (IP addresses) are not set correctly, you may connect to the wrong Controller and set incorrect device parameters. Download data only after you confirm that you are connected to the correct Controller.
- 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 you transfer the data.
- When network variables are used in tag settings, a connection error will result if the variables are not set in the NX-series EtherNet/IP Unit. Before downloading the tag data link parameters, check to confirm that the network variables are set in the NX-series EtherNet/IP Unit. Check whether the network variable, tag, and connection settings are correct on the **Connection** Tab Page and the **Tag Status** Tab Page as described in *14-6-1 The Network Configurator's Device Monitor Function* on page 14-47.
- If a communications error occurs, the output status depends on the specifications of the device being used. When a communications error occurs for a device that is used along with output devices, check the operating specifications and implement safety countermeasures.
- The EtherNet/IP port is automatically restarted after the parameters are downloaded. This restart is required to enable the tag set and connection information. Before you download the parameters, check to confirm that problems will not occur with the equipment when the port is restarted.
- Make sure that the major CIP revision of the device registered with the Network Configurator is the same as the major CIP revision of the NX-series EtherNet/IP Unit that you use. If the major CIP revisions are not the same, the parameters may not be downloaded. To determine whether downloading is possible, refer to *9-2-3 Registering Devices* on page 9-17.
- Do not disconnect the Ethernet cable or reset or turn OFF the power to the NX-series EtherNet/IP Unit during the parameter download.
- Tag data links (data exchange) between relevant nodes are stopped during a download. Before you download data in RUN mode, make sure that it will not adversely affect the controlled system.
  Also implement interlocks on data processing in ladder programming that uses tag data links when the tag data links are stopped or a tag data link error occurs.

1 Connect the Network Configurator to the network.

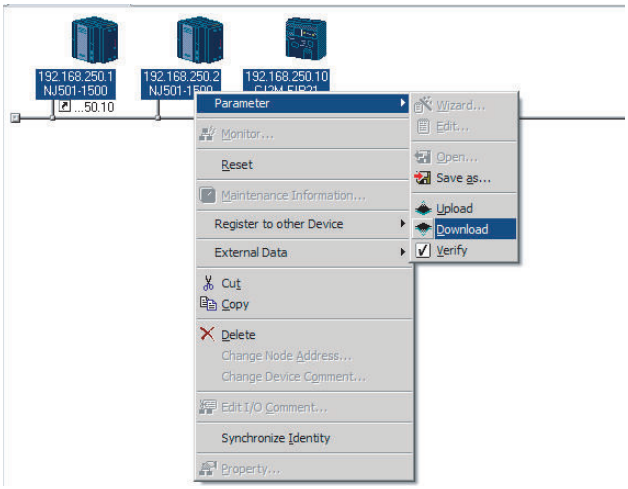
2 There are two ways to download the parameters.

- Downloading to All Devices in the Network
  Select **Network** - **Download**.
  The following dialog box is displayed.

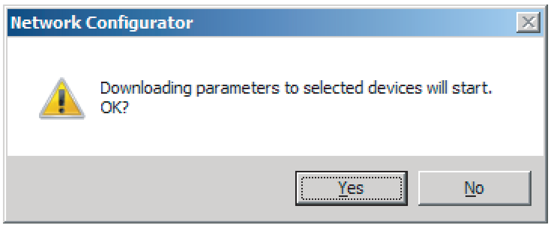


In order to enable new configuration, downloading parameters to all devices will start.
OK?

- Downloading Individually to Particular Devices
  Select the icon of the NX-series EtherNet/IP Unit to which you want to download. To select multiple nodes, press and hold the Shift Key or the Ctrl Key while you select additional icons. (In the following example, 2 nodes are selected: 192.168.250.1 and 192.168.250.2.)
  Right-click the icon to display the popup menu, and select **Parameter** - **Download**.

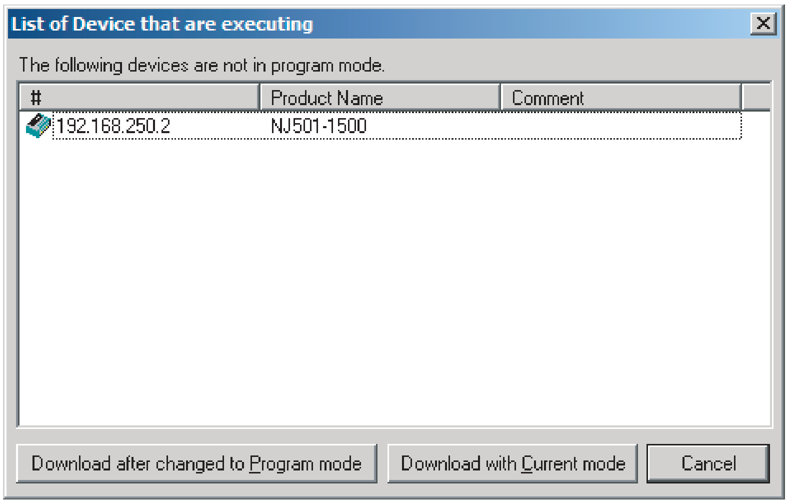


The following dialog box is displayed.



Downloading parameters to selected devices will start.
OK?

3 Click the **Yes** Button to download the tag data link parameters to the EtherNet/ IP Unit.
The following dialog box is displayed if any of the CPU Units is not in PROGRAM mode.

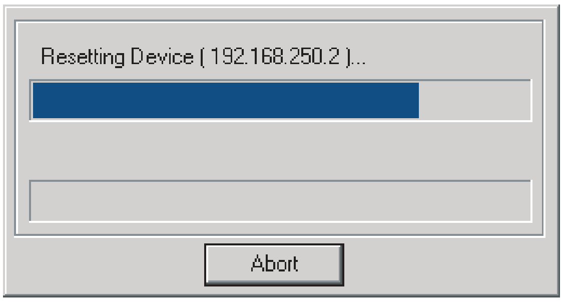

List of Device that are executing

The following devices are not in program mode.

#	Product Name	Comment
192.168.250.2	NJ501-1500	

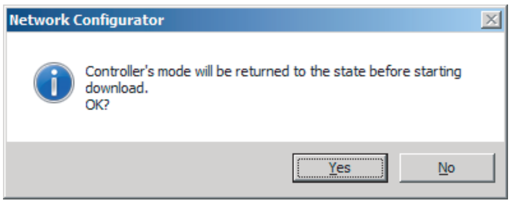
Download after changed to Program mode
Download with Current mode
Cancel

If the **Download after changed to Program mode** Button is clicked, all CPU Units are changed to PROGRAM mode and the parameters are downloaded. Confirm safety for all controlled equipment before you change the CPU Units to PROGRAM mode. You can restore the operating modes after the parameters are downloaded.
You can click the **Download with Current mode** Button to download the parameters even when one or more CPU Units is in RUN mode.
During the download, the following progress indicator is displayed to show the progress of the download.



Resetting Device (192.168.250.2)...

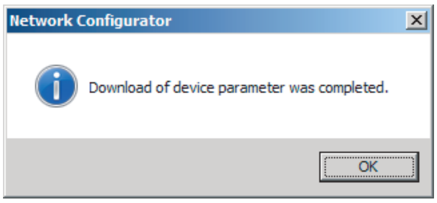
If the operating mode of one or more CPU Units was changed to download the parameters, you can return the CPU Units to the previous operating modes. If the **No** Button is clicked, the CPU Units remain in PROGRAM mode.



Network Configurator

Controller's mode will be returned to the state before starting download.
OK?

4 The following dialog box is displayed to show that the download was completed.



Network Configurator

Download of device parameter was completed.

9-2-10 Uploading Tag Data Link Parameters

You can upload tag data link parameters (such as tag set settings and connection settings) from EtherNet/IP devices in the EtherNet/IP network.

The following procedure shows how to upload the parameters. For details on how to connect to the network from the Network Configurator, refer to *9-2-8 Connecting the Network Configurator to the Network* on page 9-48.

Precautions for Correct Use

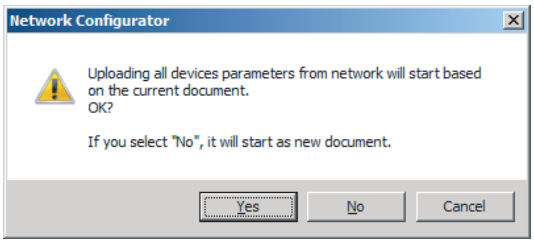
- Make sure that the major CIP revision of the device registered with the Network Configurator is the same as the major CIP revision of the NX-series EtherNet/IP Unit that you use. If the major CIP revisions are not the same, the parameters may not be uploaded. To determine whether uploading is possible, refer to *9-2-3 Registering Devices* on page 9-17.

There are two ways to upload the parameters.

Uploading from All Devices in the Network

1 Connect the Network Configurator online, and then select **Upload** from the **Network** Menu.

2 The following dialog box is displayed.

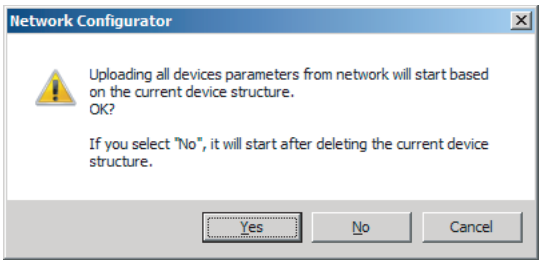

Network Configurator

Uploading all devices parameters from network will start based on the current document.
OK?

If you select "No", it will start as new document.

- Clicking the **Yes** Button:
  The tag data link parameters in the current project are uploaded.
- Clicking the **No** Button:
  You open a new project to upload the tag data link parameters. The current project is closed.
- Clicking the **Cancel** Button:
  The upload operation is canceled. The upload is not performed.

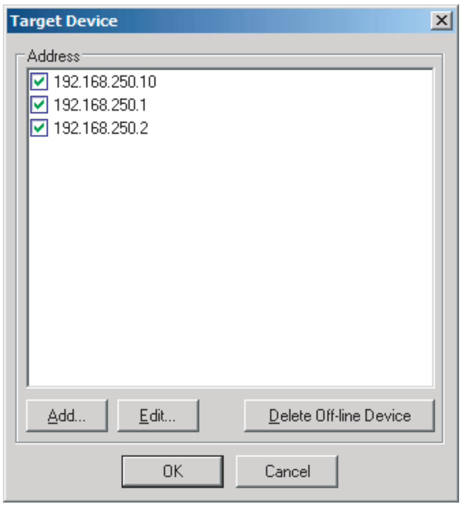
3 If you click the **Yes** Button in step 2, the following dialog box is displayed.


Network Configurator

Uploading all devices parameters from network will start based on the current device structure.
OK?

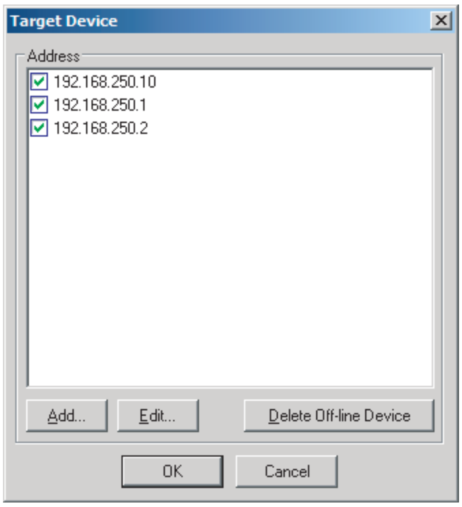
If you select "No", it will start after deleting the current device structure.

- Clicking the **Yes** Button:
  Parameters are uploaded only from the devices registered in the Network Configuration Pane. Parameters are not uploaded from devices that are not registered in the Network Configuration Pane.
- Clicking the **No** Button:
  Performing a Batch Upload over the Network
  Parameters are uploaded from all devices on the network.
  The current Network Configuration Information will be lost.
  The following dialog box will be displayed. Select the devices for which to upload parameters and click the **OK** Button.



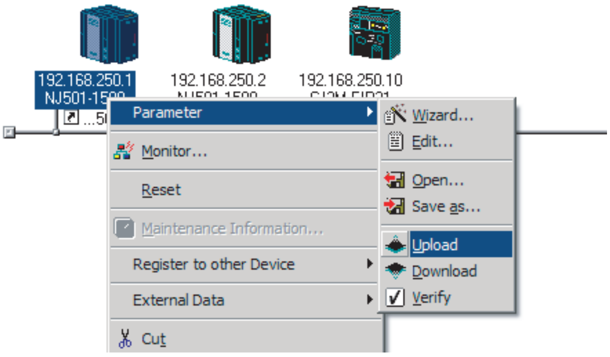
- Clicking the **Cancel** Button:
  The upload operation is canceled. The upload is not performed.

4 If you click the **No** Button in step 2, the following dialog box is displayed.
Select the devices for which to upload parameters and click the **OK** Button.

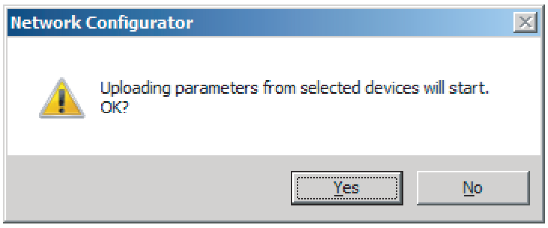


Uploading Individually from Particular Devices

1 Connect the Network Configurator to the network.
Select the icon of the EtherNet/IP Unit from which you want to upload parameters. To select multiple nodes, press and hold the Shift Key or the Ctrl Key while you select additional icons. (In the following example, 2 nodes are selected: 192.168.250.1 and 192.168.250.2.)
Right-click the icon to display the pop-up menu, and select **Parameter** - **Upload**.



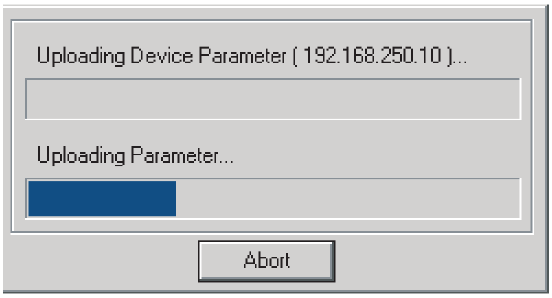
2 The following dialog box is displayed.



Uploading parameters from selected devices will start.
OK?

Click the **Yes** Button or the **No** Button.

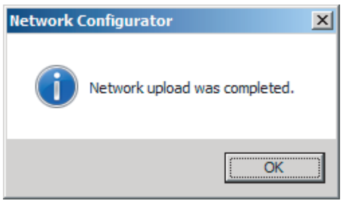
3 During the upload, the following progress indicator is displayed to show the progress of the upload.



Uploading Device Parameter (192.168.250.10)...

Uploading Parameter...

4 The following dialog box is displayed to show that the upload was completed.



Network upload was completed.

9-2-11 Verifying Tag Data Link Parameters

Tag data link parameters (such as tag set settings and connection settings) can be compared with the parameters of the EtherNet/IP ports in the EtherNet/IP network.

The following procedure shows how to compare the parameters. For details on how to connect to the network from the Network Configurator, refer to *9-2-8 Connecting the Network Configurator to the Network* on page 9-48.

Precautions for Correct Use

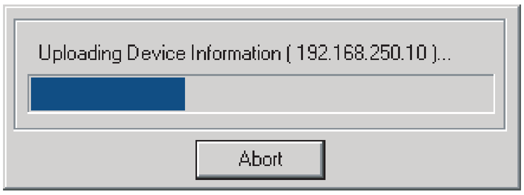
- Make sure that the major CIP revision of the device registered with the Network Configurator is the same as the major CIP revision of the NX-series EtherNet/IP Unit that you use. If the major CIP revisions are not the same, the parameters may not be compared. To determine whether comparison is possible, refer to *9-2-3 Registering Devices* on page 9-17.

Verifying the Network Configuration

You can use the following procedure to compare the list of registered devices in the Network Configuration Pane with the devices connected on the EtherNet/IP network, and check the IP addresses and device types.
This function does not verify device parameters.

1 Connect the Network Configurator to the network.

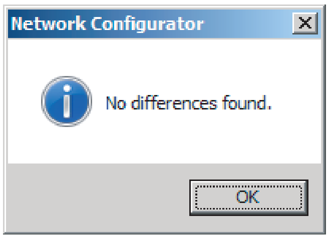
2 Select **Network** - **Verify Structure**.
The following progress indicator is displayed to show the progress as data is read from the network and compared.



Uploading Device Information (192.168.250.10)...

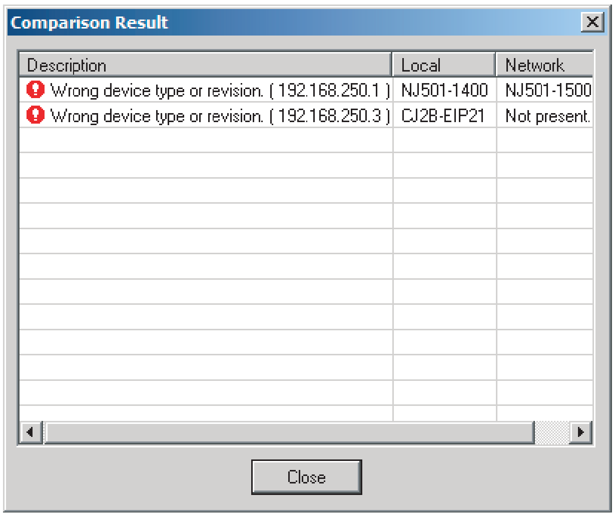
3 The result of the comparison between the network configuration file and data from the network is displayed as shown below.

- Differences Not Found in the Comparison



No differences found.

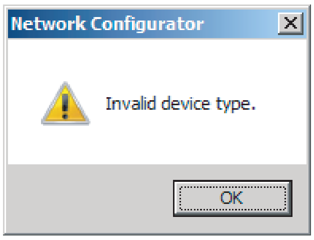
- Differences Found in the Comparison



Comparison Result

Description	Local	Network
Wrong device type or revision. (192.168.250.1)	NJ501-1400	NJ501-1500
Wrong device type or revision. (192.168.250.3)	CJ2B-EIP21	Not present.

- Differences Found in the Device Type



Network Configurator

Invalid device type.

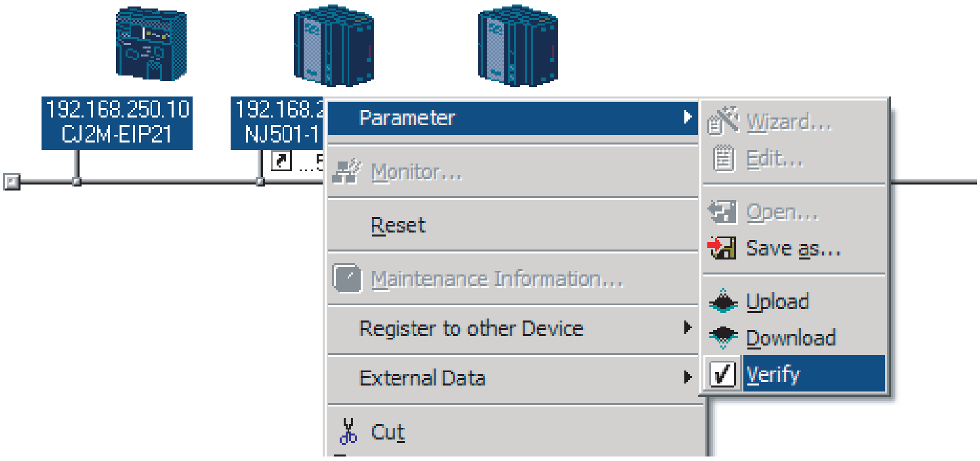
Click the **OK** Button or the **Close** Button.

Verifying the Device Parameters

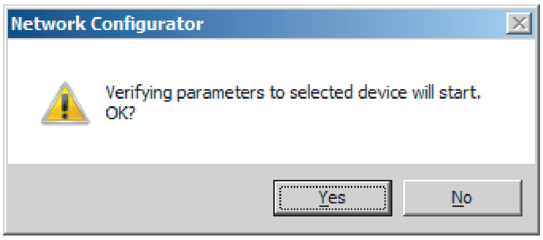
Use the following procedure to compare the device parameters for the devices selected in the Network Configuration Pane with those of the devices connected on the EtherNet/IP network.
The IP addresses, device types, and device parameters are compared.

1 Connect the Network Configurator to the network.

2 Click the icon of the EtherNet/IP port to verify. To select multiple nodes, press and hold the Shift Key or the Ctrl Key while you select additional icons. (In the following example, 2 nodes are selected: 192.168.250.1 and 192.168.250.2.)
Right-click the icon to display the pop-up menu and select **Parameter** – **Verify**.



3 The following dialog box is displayed.

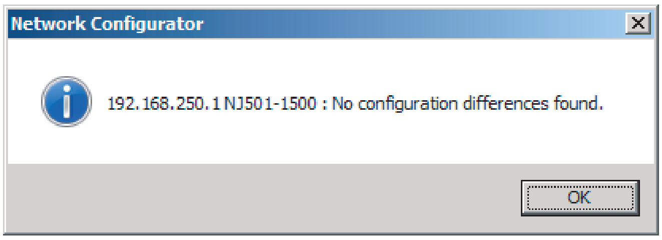


Verifying parameters to selected device will start.
OK?

Click the **Yes** Button or the **No** Button.

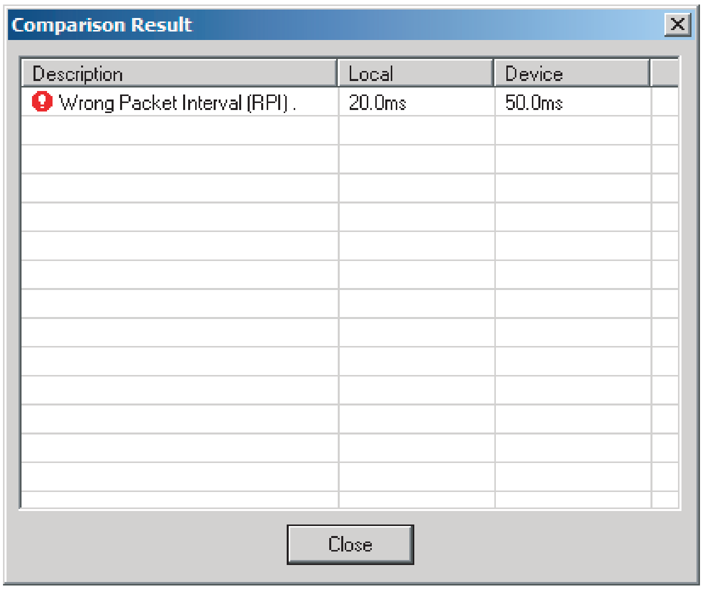
4 The following dialog box is displayed.

- Differences Not Found in the Comparison



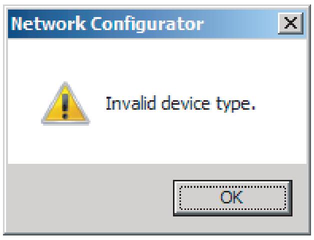
192.168.250.1 NJ501-1500 : No configuration differences found.

- Differences Found in the Comparison



Description	Local	Device
Wrong Packet Interval (RPI) .	20.0ms	50.0ms

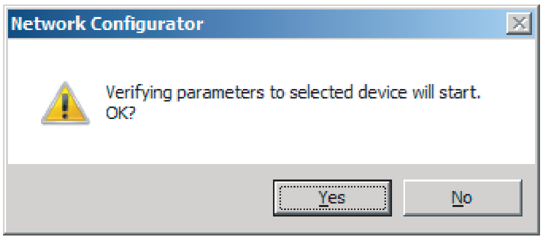
- Differences Found in the Device Type



Invalid device type.

Click the **OK** Button or the **Close** Button.

5 If multiple nodes have been selected and compared, the following message is displayed. Click the **Yes** Button.



Verifying parameters to selected device will start.
OK?

The comparison results are displayed in order of the selected nodes.

9-2-12 Starting and Stopping Tag Data Links

This section describes the procedure for starting/stopping tag data links. For details on how to connect Network Configurator to a network, refer to *9-2-8 Connecting the Network Configurator to the Network* on page 9-48.

Automatically Starting Tag Data Links

Tag data links are automatically started immediately after the data link parameters are downloaded from the Network Configurator.

(They are automatically started after the CPU Unit's power is turned ON or the Unit is restarted.)

Additional Information

With a CPU Unit that operates as the originator device, a *Tag Data Link Connection Timeout* error will occur if a connection is not established with the target device within one minute after the tag data links are started.
Even after this error occurs, reconnection processing is continued periodically until automatic recovery is performed.
If the application environment allows you to ignore this error, such as when a target device is started later than the originator device, you can change the event level to the observation level.

Starting and Stopping Tag Data Links for the Entire Network

You can start and stop tag data links for the entire network by instructions from the user program or operations from the Network Configurator.

Precautions for Correct Use

Use the same method (i.e., either the user program or the Network Configurator) to both start and stop tag data links.
For example, if you execute an instruction to stop tag data links, you cannot restart them from the Network Configurator.

● Executing Instructions in the User Program

You can start tag data links for the entire network by executing the TDLinkStartConnection (Start Tag Data Link Target Connection) instruction from the user program. You can stop tag data links for the entire network by executing the TDLinkStopConnection (Stop Tag Data Link Target Connection) instruction.
Refer to *Section 13 Instructions Specific to NX-series EtherNet/IP Units* on page 13-1 for detailed instruction specifications.

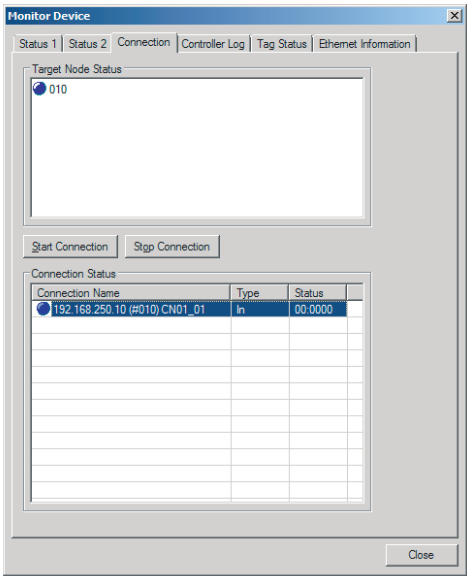
● Using the Network Configurator

You can select **I/O Connection** - **Start** or **Stop** from the **Network** Menu to start and stop tag data links for individual devices.

Starting and Stopping Tag Data Links for Individual Devices

● Using the Network Configurator

You can start and stop tag data links on a device basis (at the originator) by selecting **Monitor** from the **Device** Menu and performing the following operation in the **Connection** Tab Page in the **Monitor Device** Dialog Box.
You can start and stop tag data links for each of the EtherNet/IP ports 1 and 2 connected to the Network Configurator.



● 010

Connection Name	Type	Status
● 192.168.250.10 (#010) CN01_01	In	00:0000

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.

9-2-13 Clearing the Device Parameters

You can clear the tag data link settings (or return them to their factory settings) that are saved in the registered EtherNet/IP device.

The following shows how to clear tag data link parameters. For details on how to connect to the network from the Network Configurator, refer to *9-2-8 Connecting the Network Configurator to the Network* on page 9-48.

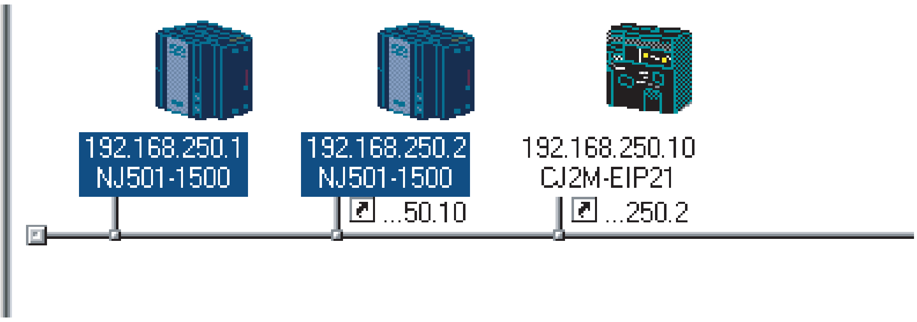
Precautions for Correct Use

- Use the Network Configurator version 3.58 or higher to perform the following procedure to clear the tag data link settings.
- If you perform the following procedure from the Network Configurator version 3.57 or lower, the tag data link settings are not cleared. Refer to Additional Information in this section for the procedure to clear the tag data link settings from the Network Configurator version 3.57 or lower.

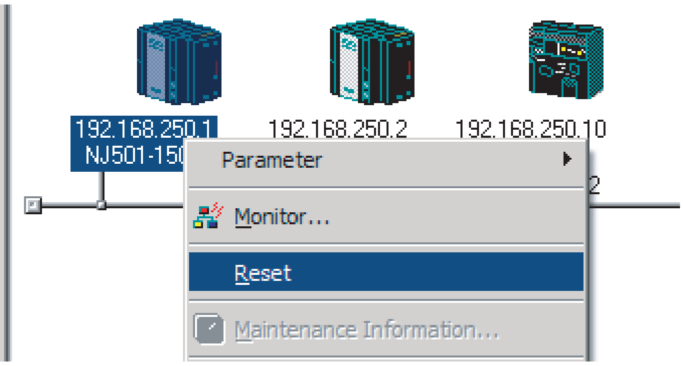
1 Connect the Network Configurator to the network.

2 Select the icon of the device from which you want to clear the device parameters.

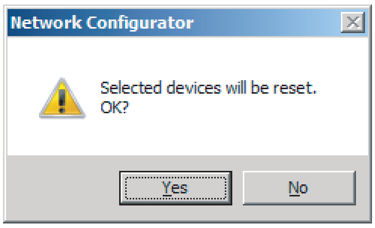
In the following example, two nodes are selected: 192.168.250.1 and 192.168.250.2. To select multiple nodes, press and hold the **Shift** Key while you select additional icons.



3 Select **Device** - **Reset**.
You can also right-click the icon and select **Reset** from the pop up menu.

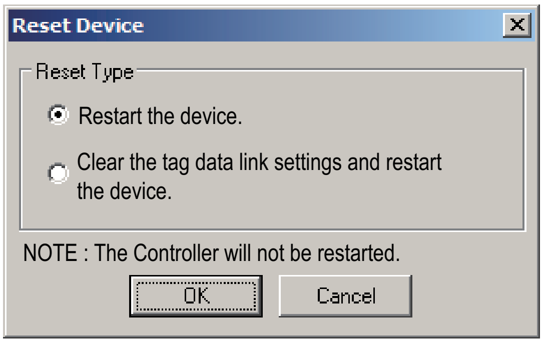


4 The following dialog box is displayed.


Network Configurator

Selected devices will be reset.
OK?

- If you click the **Yes** Button:
  The following dialog box is displayed.


Reset Device

Reset Type

● Restart the device.

○ Clear the tag data link settings and restart the device.

NOTE : The Controller will not be restarted.

Select the **Initialize tag data link configuration, and then emulate cycling power** Option, and then click the **OK** Button.

Precautions for Correct Use

The Controller is not restarted. Only the EtherNet/IP port is reset.

- If you click the **No** Button:
  The tag data link settings will not be cleared and the built-in EtherNet/IP port will not be reset.

Additional Information

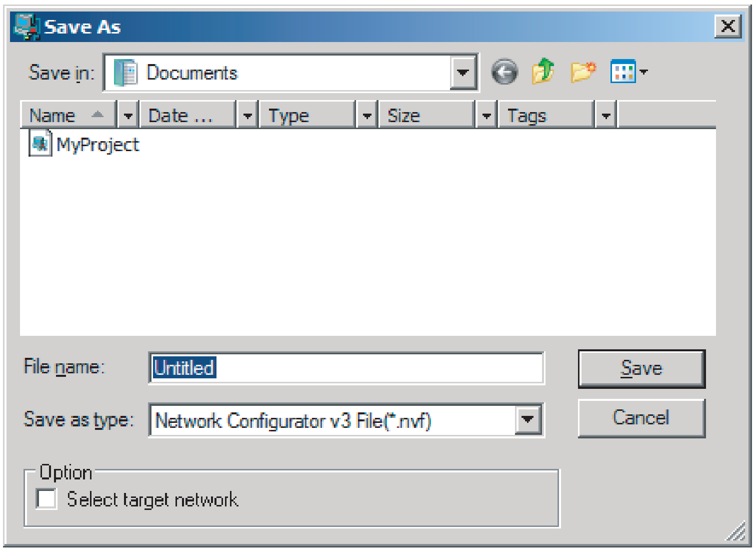
You can also execute the Reset service of the Identity Object for the NX-series EtherNet/IP Unit to clear the tag data link settings. The procedure to execute the service from the Network Configurator is given below.

1. Connect the Network Configurator to the network.
2. Select **Tool** - **Setup Parameters** in the main window.
   Then the dialog box for the general parameter settings are displayed.
3. Specify the target device and message to send.
   - Target Node Address : Enter the IP address of the target device.
   - Service : Select **Reset**.
   - Class : Enter *01*.
   - Instance : Enter *01*.
   - Attribute : Enter *00*.
   - Data : Enter *02*[*1].
4. Click the **Send** Button.

9-2-14 Saving the Network Configuration File

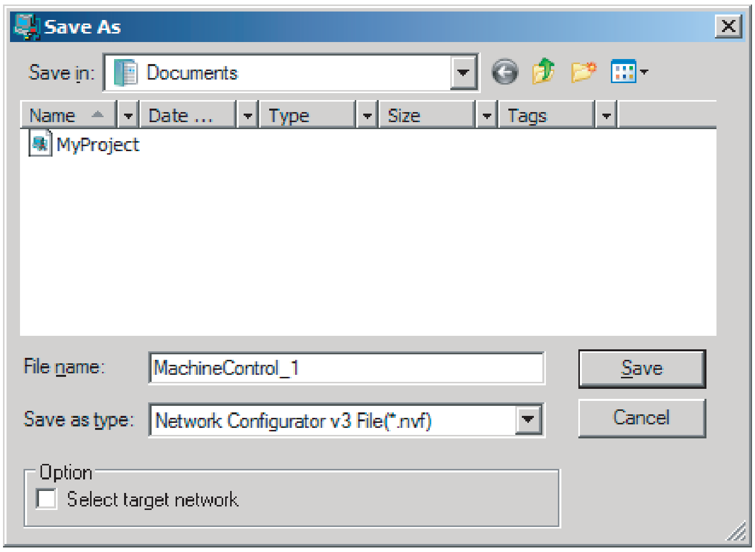
You can save device parameters set in the Network Configurator or device parameters uploaded from the network in a network configuration file.

1 Select **File** - **Save As**.
The following dialog box is displayed.



Untitled.nvf is displayed as the default file name.

2 Input the file name, and then click the **Save** Button.



File name: MachineControl_1

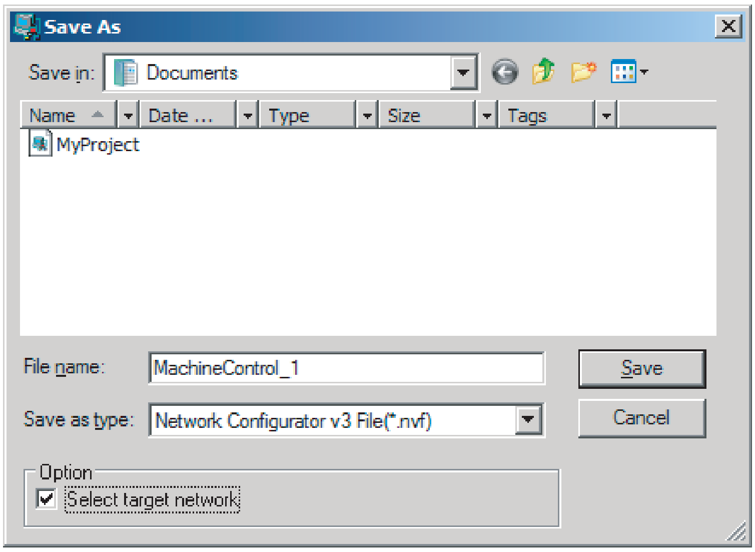
Save as type: Network Configurator v3 File(*.nvf)

☐ Select target network

This completes the network configuration file save operation.

3 When the network configuration is changed later, you can overwrite the existing network configuration file if you select **File** - **Save**, or click the 💾 Button.

4 You can select the **Select target network** Check Box in the **Option** Area to select and save only the required network configuration files from the existing multiple files.

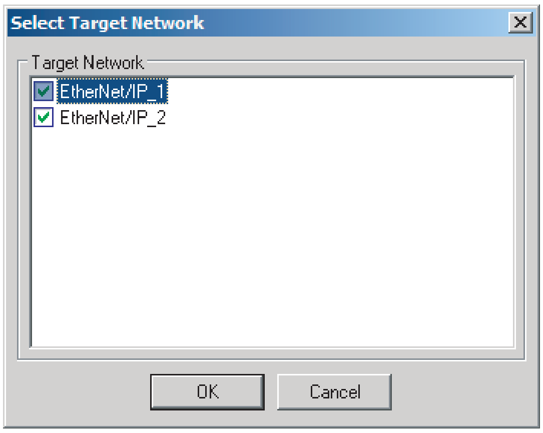


File name: MachineControl_1

Save as type: Network Configurator v3 File(*.nvf)

☑ Select target network

Select the check boxes of the networks to save and click the **OK** Button.



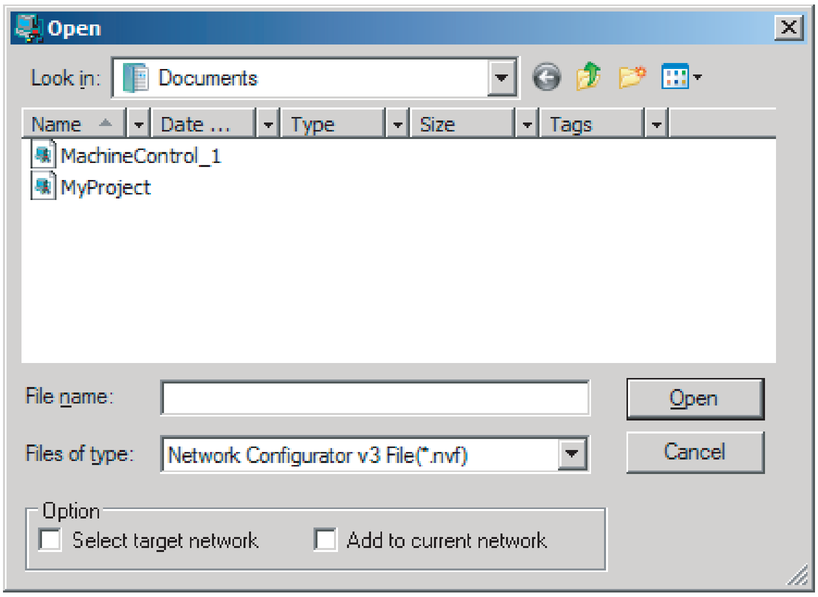
☑ EtherNet/IP_1
☑ EtherNet/IP_2

9-2-15 Reading a Network Configuration File

You can read out a previously saved network configuration file into the Network Configurator.

1 Select **File** - **Open**, or click the 📂 Button.

The following dialog box is displayed.



Look in: Documents

MachineControl_1
MyProject

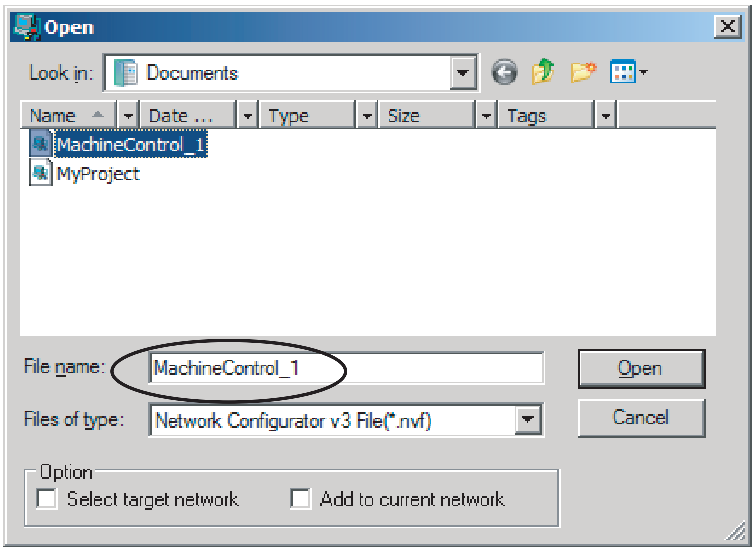
File name:

Files of type: Network Configurator v3 File(*.nvf)

☐ Select target network ☐ Add to current network

If the network configuration file that you want to read out is not displayed, change to another folder.

2 If you select the network configuration file that you want to read out, that file name is displayed in the File name Field.



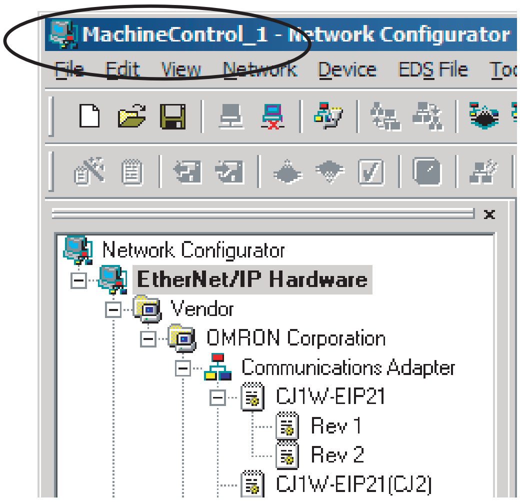
File name: MachineControl_1

Files of type: Network Configurator v3 File(*.nvf)

☐ Select target network ☐ Add to current network

3 Click the **Open** Button to read out the network configuration file.

4 The Network Configurator's Title Bar will display the name of the file that was read out.



5 Select options in the **Option** Area as necessary.

The options are listed below.

Setting	Description
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 that is currently open to the current configuration file.

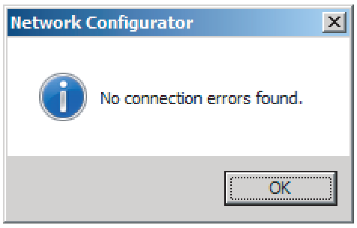
Additional Information

The save format will depend on the version of the Network Configurator. You can import configuration files (*.ncf) created with the Network Configurator for EtherNet/IP (version 2 or lower) if you select **External Data** - **Import** from the **File** Menu.

9-2-16 Checking Connections

You can check the consistency of connection parameters for network configuration files with device parameters that were set with the Network Configurator or device parameters uploaded from the network.

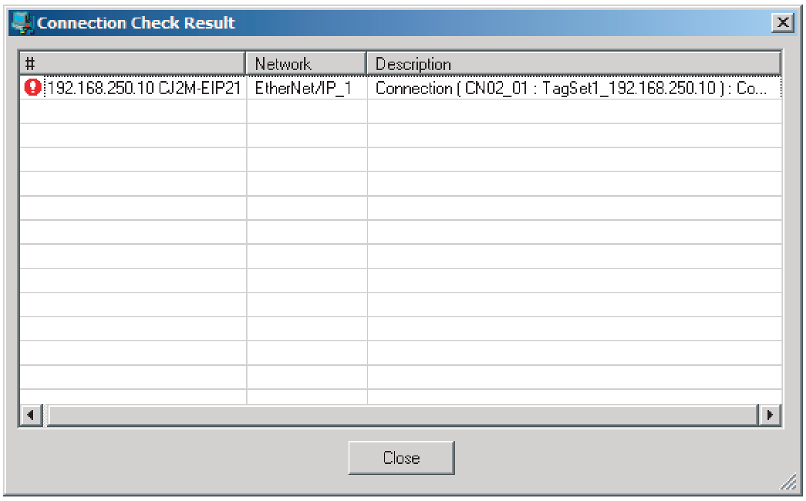
1 Select **Check Connection** from the **Network** Menu.
The following dialog box is displayed if parameters are normal.



Network Configurator

No connection errors found.

The following dialog box is displayed if there are parameter errors. Check the displayed details and review the settings.

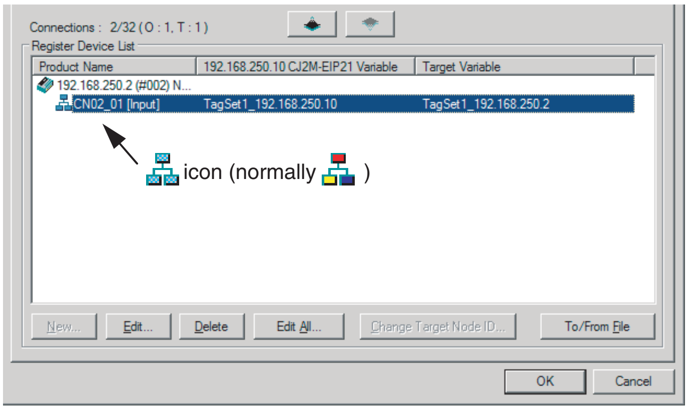


Connection Check Result

#	Network	Description
192.168.250.10 CJ2M-EIP21	EtherNet/IP_1	Connection (CN02_01 : TagSet1_192.168.250.10) : Co...

If an inconsistency is found, open the originator’s **Edit Device Parameter** Dialog Box and click the **Connection** Tab. The inconsistent connection in the **Register Device List** is 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.



Connections : 2/32 (O : 1, T : 1)

Register Device List

Product Name	192.168.250.10 CJ2M-EIP21 Variable	Target Variable
192.168.250.2 (#002) N...		
CN02_01 [Input]	TagSet1_192.168.250.10	TagSet1_192.168.250.2

9-2-17 Changing Devices

You can change devices that are registered in a network configuration with the Network Configurator. Select **Change Device** from the **Device** Menu to display a list of the possible devices to change. You can change a device only when there is complete or upward compatibility with the device.

Device Changes

Model before change	CIP Rev	Model after change										
		NX-EIP201	CS1W-EIP21	CS1W-EIP21 (NE)	CS1W-EIP21S	CJ1W-EIP21	CJ1W-EIP21 (CJ2)	CJ1W-EIP21S	CJ1W-EIP21 (NJ)	CJ1W-EIP21S (CJ2)	CJ2B-EIP21	CJ2M
		Rev 2	Rev 3	Rev 3	Rev 4	Rev 3	Rev 3	Rev 4	Rev 3	Rev 4	Rev 3	Rev 2
NX-EIP201	**Rev 2**	----	No	No	No	No	△2/6/7	No	△2/4/7	△2/6/7	△2/6/7	△2/4/7
CS1W-EIP21	**Rev 3**	No	---	Yes	Yes	Yes	Yes	Yes	△5	Yes	Yes	△3
CS1W-EIP21 (NE)	**Rev 3**	No	△1	---	Yes	△1	Yes	Yes	△5	Yes	Yes	△3
CS1W-EIP21S	**Rev 4**	No	Yes	Yes	---	Yes	Yes	Yes	△5	Yes	Yes	△3
CJ1W-EIP21	**Rev 3**	No	Yes	Yes	Yes	----	Yes	Yes	△5	Yes	Yes	△3
CJ1W-EIP21 (CJ2)	**Rev 3**	△5	△1	△0	△1	△1	---	△1	△5	Yes	Yes	△3
CJ1W-EIP21S	**Rev 4**	No	Yes	Yes	Yes	Yes	Yes	---	△5	Yes	Yes	△3
CJ1W-EIP21 (NJ)	**Rev 3**	Yes	△1/2	△0/2	△1/2	△1/2	△2	△1/2	---	△2	△2	△2/6
CJ1W-EIP21S (CJ2)	**Rev 4**	△5	△1	△0	△1	△1	Yes	△1	△5	---	Yes	△3
CJ2B-EIP21	**Rev 3**	△5	△1	△0	△1	△1	Yes	△1	△5	Yes	----	△3
CJ2M	**Rev 2**	△5	△1	△0	△1	△1	Yes	△1	△5	Yes	Yes	----

Model before change	CIP Rev	Model after change										
		NX-EIP201	CS1W-EIP21	CS1W-EIP21 (NE)	CS1W-EIP21S	CJ1W-EIP21	CJ1W-EIP21 (CJ2)	CJ1W-EIP21S	CJ1W-EIP21 (NJ)	CJ1W-EIP21S (CJ2)	CJ2B-EIP21	CJ2M
		Rev 2	Rev 3	Rev 3	Rev 4	Rev 3	Rev 3	Rev 4	Rev 3	Rev 4	Rev 3	Rev 2
NJ501 **NJ301**	**Rev 1**	No	△1/2	△0/2	△1/2	△1/2	△2	△1/2	Yes	△2	△2	△2/6
	Rev 2	Yes	△1/2	△0/2	△1/2	△1/2	△2	△1/2	Yes	△2	△2	△2/6
NJ101	**Rev 2**	Yes	△1/2	△0/2	△1/2	△1/2	△2	△1/2	Yes	△2	△2	△2/6
NX701	**Rev 2**	Yes	No	No	No	No	△2	No	Yes	△2	△2	△2/6
NX502	**Rev 2**	Yes	No	No	No	No	△2/7	No	△2/7	△2/7	△2/7	△2/6/7
NX102	**Rev 2**	Yes	No	No	No	No	△2	No	Yes	△2	△2	△2/6
NX1P2	**Rev 2**	Yes	No	No	No	No	△2	No	Yes	△2	△2	△2/6

Model before change	CIP Rev	Model after change						
		NJ501 NJ301		NJ101	NX701	NX502	NX102	NX1P2
		Rev 1 *1	Rev 2 *2	Rev 2 *2	Rev 2	Rev 2	Rev 2	Rev 2
NX-EIP201	**Rev 2**	No	△4/7	△4/7	△6/7	△4	△4/7	△4/7
CS1W-EIP21	**Rev 3**	△4/5	△4/5	△4/5	No	No	No	No
CS1W-EIP21 (NE)	**Rev 3**	△4/5	△4/5	△4/5	No	No	No	No
CS1W-EIP21S	**Rev 4**	△4/5	△4/5	△4/5	No	No	No	No
CJ1W-EIP21	**Rev 3**	△4/5	△4/5	△4/5	No	No	No	No
CJ1W-EIP21 (CJ2)	**Rev 3**	△4/5	△4/5	△4/5	△5	△4/5	△4/5	△4/5
CJ1W-EIP21S	**Rev 4**	△4/5	△4/5	△4/5	No	No	No	No
CJ1W-EIP21 (NJ)	**Rev 3**	△4	△4	△4	Yes	△4	△4	△4
CJ1W-EIP21S (CJ2)	**Rev 4**	△4/5	△4/5	△4/5	△5	△4/5	△4/5	△4/5
CJ2B-EIP21	**Rev 3**	△4/5	△4/5	△4/5	△5	△4/5	△4/5	△4/5
CJ2M	**Rev 2**	△4/5	△4/5	△4/5	△5	△5	△4/5	△4/5
NJ501 **NJ301**	**Rev 1**	----	Yes	△4	No	No	No	No
	Rev 2	Yes	---	△4	Yes	Yes	Yes	△4
NJ101	**Rev 2**	Yes	Yes	---	Yes	Yes	Yes	△4
NX701	**Rev 2**	No	△4	△4	---	△4	△4	△4
NX502	**Rev 2**	No	△4/7	△4/7	△7	---	△4/7	△4/7
NX102	**Rev 2**	No	Yes	Yes	Yes	Yes	----	△4
NX1P2	**Rev 2**	No	Yes	Yes	Yes	Yes	Yes	----

*1. CPU Unit with a unit version 1.00 to 1.02

*2. CPU Unit with a unit version 1.03 or later

Yes	Can be changed.
No:	Cannot be changed.
△0	Cannot be changed if a Japanese variable is specified in the tag.
△1	Cannot be changed if a network variable is specified as a tag.
△2	Cannot be changed if the maximum size of a tag name or tag set name (size after conversion into UTF-8) exceeds 48 bytes.

△3 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.

△4 Cannot be changed in any of the following cases:

- The number of I/O connections, number of tags, number of tag sets, or size of one tag set exceeds the permissible settings for the device after the change.
- RPI exceeds the permissible settings or is set in 0.5-ms increments (such as 10.5ms)

△5 Cannot be changed if a tag set size is an odd number of bytes.

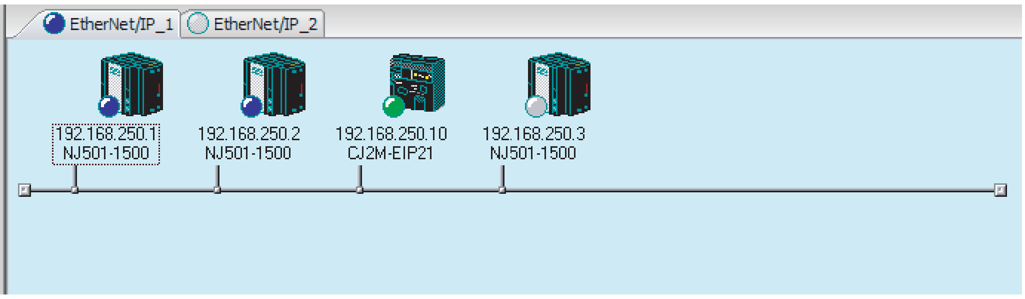
△6 Cannot be changed if tags, tag sets, or refreshing sizes exceed the permissible settings.

△7 Cannot be changed if the maximum number of tags per tag set exceeds the permissible setting.

9-2-18 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
● (white)	Offline
● (gray)	Default (including no Controller Configurations and Setup)
● (green)	Idle (including when the Controller is in PROGRAM mode)
● (blue)	Normal communications state (including when the Controller is in RUN mode)
● (yellow)	Warning status (including when there is a partial fault or non-fatal error in the Controller)
● (red)	Alarm status (including when there is a major fault or fatal error in the Controller)

9-3 Ladder Programming for Tag Data Links

9-3-1 Ladder Programming for Tag Data Links

The following conditions 1 to 3 should be fulfilled if you use tag data link data for a ladder programming. The additional conditions 4 and 5 should be also fulfilled if you input the Controller information of the target node.

The device variables listed below assume that the communications port 1 of an NX-series EtherNet/IP Unit with unit number 2 is used. *N2* at the beginning of the device variable represents unit number 2. Refer to *Section 6 Device Variables Related to the NX-series EtherNet/IP Unit* on page 6-1 for the variable names of device variables when the communications port 2 is used.

● Conditions for Enabling Tag Data Links for the EtherNet/IP Port

The following conditions 1 and 2 should be both fulfilled.

No.	Condition
1	The following error status bits in the *N2_ETN_ErrSta* (Communications Port Error) variable are FALSE. • Major fault: Bit 7 • Partial fault: Bit 6 • Minor fault: Bit 5
2	The *N2_ETN_Port1Status.EtnOnlineSta* (Port1 Online) variable is TRUE.

● Condition for Tag Data Links with Connection Established to the Target Device

The following condition 3 should be fulfilled.

No.	Condition
3	In the *N2_EIP_Comm1Status.EstbTargetSta[255]* (CIP Communications1 Normal Target Node Information) variable, the bit corresponding to the target node address is TRUE.

● Condition of the Controller Operating Mode (Operating or Stopped) (Only for OMRON Controllers)

The following condition 4 should be fulfilled.

No.	Condition
4	In the *N2_EIP_Comm1Status.TargetPLCModeSta[255]* (CIP Communications1 Target PLC Operating Mode) variable, the bit corresponding to the target node address is TRUE.

● Condition of the Controller Error Status (Fatal or Non-fatal Error) of the Target Node (Only for OMRON Controllers)

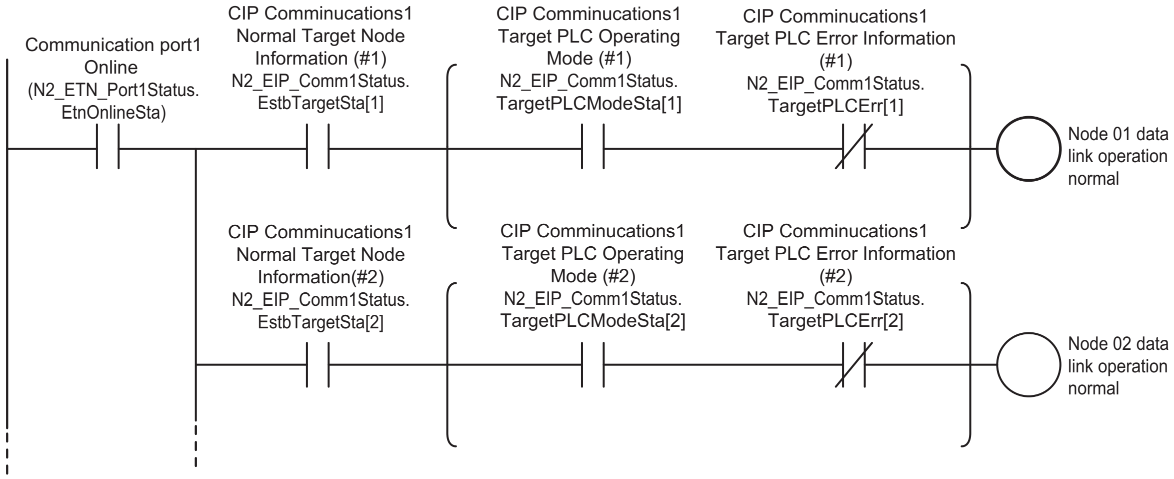
The following condition 5 should be fulfilled.

No.	Condition
5	In the *N2_EIP_Comm1Status.TargetPLCErr[255]* (CIP Communications1 Target PLC Error Information) variable, the bit corresponding to the target node address is FALSE. When you want to use the Target Node Controller Error Flag, the Controller status must be included in the tag sets for both the originator and target. Include the Controller status by using the Network Configurator to select the Include Option in the Edit Tag Set Dialog Box.

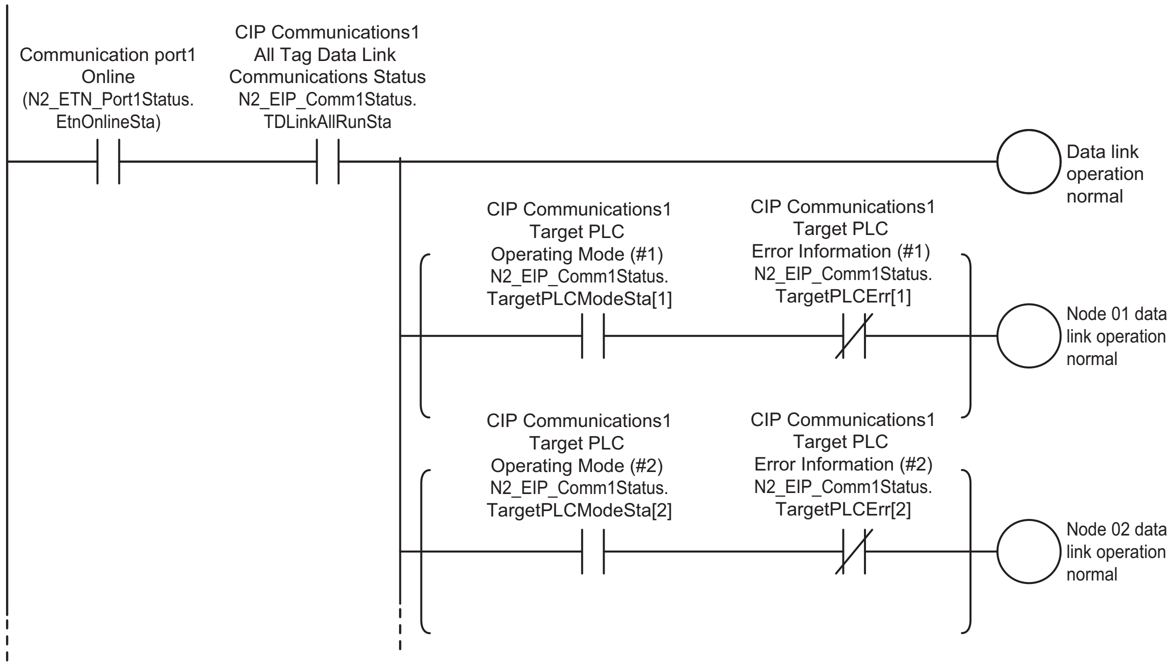
● Programming Example for Normal Operation Detection

The following program can be used to confirm that normal communications are being performed for each target node. If the Controller status is included in the tag data, the status of the Controller can also be detected.

- Normal Operation Detection Programming Example 1

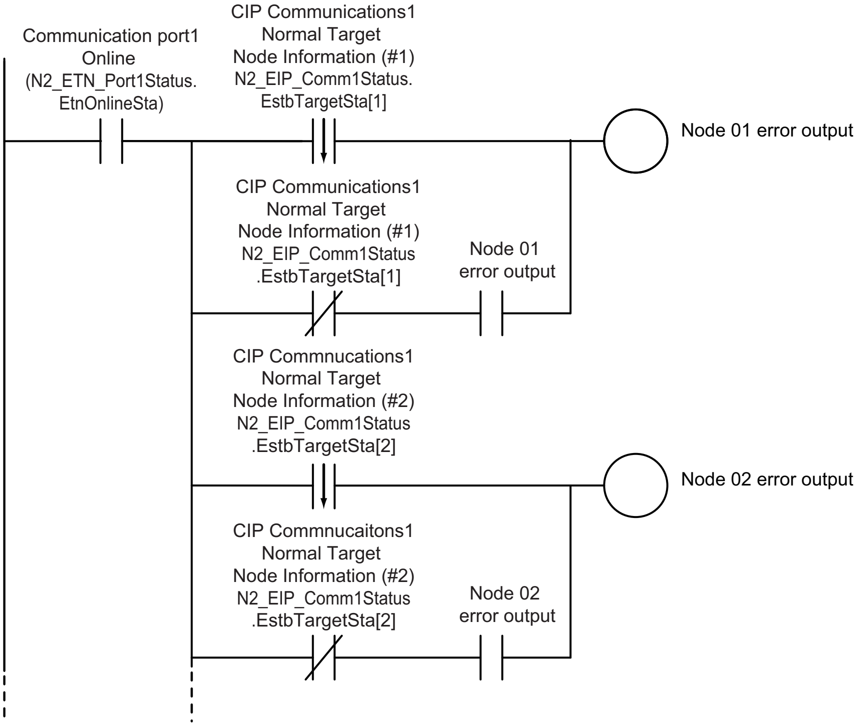

Communication port1 Online (N2_ETN_Port1Status. EtnOnlineSta)
CIP Comminucations1 Normal Target Node Information (#1) N2_EIP_Comm1Status. EstbTargetSta[1]
CIP Comminucations1 Target PLC Operating Mode (#1) N2_EIP_Comm1Status. TargetPLCModeSta[1]
CIP Comminucations1 Target PLC Error Information (#1) N2_EIP_Comm1Status. TargetPLCErr[1]
Node 01 data link operation normal
CIP Comminucations1 Normal Target Node Information(#2) N2_EIP_Comm1Status. EstbTargetSta[2]
CIP Comminucations1 Target PLC Operating Mode (#2) N2_EIP_Comm1Status. TargetPLCModeSta[2]
CIP Comminucations1 Target PLC Error Information (#2) N2_EIP_Comm1Status. TargetPLCErr[2]
Node 02 data link operation normal

- Normal Operation Detection Programming Example 2


Communication port1 Online (N2_ETN_Port1Status. EtnOnlineSta)
CIP Communications1 All Tag Data Link Communications Status N2_EIP_Comm1Status. TDLinkAllRunSta
Data link operation normal
CIP Communications1 Target PLC Operating Mode (#1) N2_EIP_Comm1Status. TargetPLCModeSta[1]
CIP Communications1 Target PLC Error Information (#1) N2_EIP_Comm1Status. TargetPLCErr[1]
Node 01 data link operation normal
CIP Communications1 Target PLC Operating Mode (#2) N2_EIP_Comm1Status. TargetPLCModeSta[2]
CIP Communications1 Target PLC Error Information (#2) N2_EIP_Comm1Status. TargetPLCErr[2]
Node 02 data link operation normal

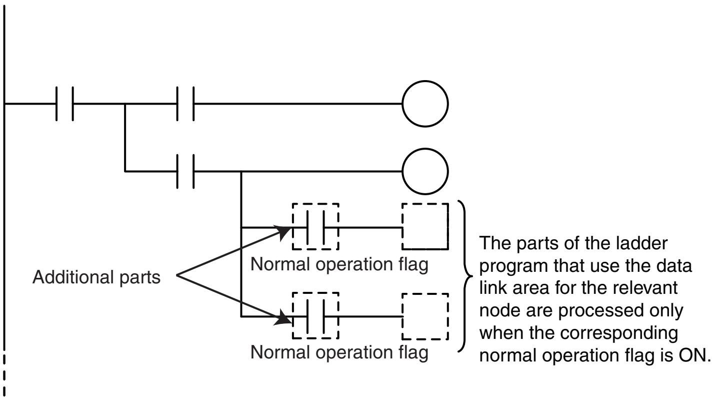
● Programming Example for Error Detection

The following program can be used to check for tag data link errors for each target node. This programming is used to detect errors which may occur after the data links for all the nodes are started normally.

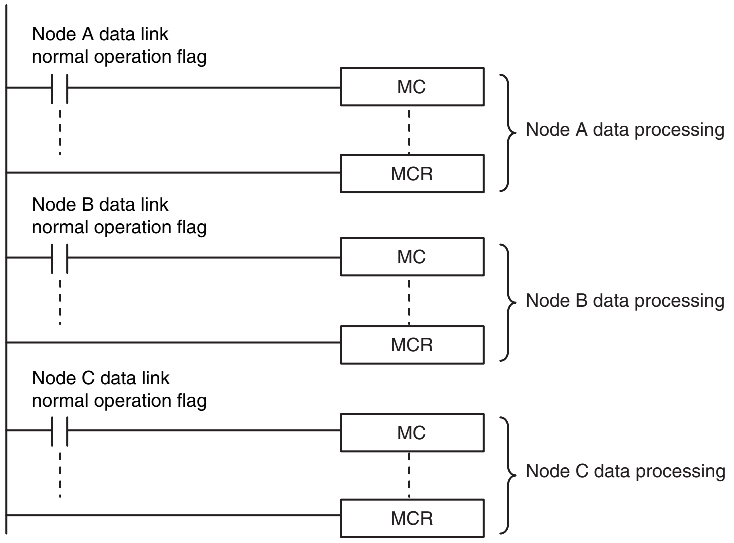


● Data Processing Programming Example

- The following shows an example where data processing is performed only when data links are operating normally.


Additional parts
Normal operation flag
Normal operation flag
The parts of the ladder program that use the data link area for the relevant node are processed only when the corresponding normal operation flag is ON.

- The following shows an example where data processing is performed only when data links are operating normally with MC and MCR instructions, or with JMP instructions.



Precautions for Correct Use

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 user program so that no input processing is performed when any of the following bits of the *ETN_ErrSta* (Communications Port Error) variable is TRUE.

- Major fault: Bit 7
- Partial fault: Bit 6
- Minor fault: Bit 5

9-3-2 Status Flags Related to Tag Data Links

The status of the tag data links is reflected in the following device variables.

Variable	Description
• EIP_Comm1Status.TargetPLCModeSta[255] (CIP Communications1 Target PLC Operating Mode) • EIP_Comm2Status.TargetPLCModeSta[255] (CIP Communications2 Target PLC Operating Mode) (Corresponds to the Controller Operating Flag in the Controller status.)	This variable shows the operating status of the target node Controller that is connected with the EtherNet/IP port as the originator. The information in this area is valid only when the corresponding Normal Target Node Information is TRUE. If the value is FALSE, the Target Node Controller Operating Information indicates the previous operating status. Array[x] is TRUE: The target Controller with a node address of x is in operating status. Array[x] is FALSE: Other than the above.

Variable	Description
• EIP_Comm1Status.TargetNodeErr[255] (CIP Communications1 Target Node Error Information) • EIP_Comm2Status.TargetNodeErr[255] (CIP Communications2 Target Node Error Information) (Corresponds to the Controller Error Flag in the Controller status.)	This variable indicates that the connection for Registered Target Node Information is not established or that an error has occurred in the target the Controller. The array elements are valid only when the Registered Target Node Information is TRUE. Array[x] is TRUE: The Registered Target Node Information for a node address of x is TRUE, and the Normal Target Node Information is FALSE or the Target PLC Error Information is TRUE. Array[x] is FALSE: When the Registered Target Node Information for a node address of x is FALSE, or when the Registered Target Node Information is TRUE, the Normal Target Node Information is TRUE, and the Target PLC Error Information is FALSE.
• EIP_Comm1Status.EstbTargetSta[255] (CIP Communications1 Normal Target Node Information) • EIP_Comm2Status.EstbTargetSta[255] (CIP Communications2 Normal Target Node Information) (This status is not included in the Controller status.)	This variable gives a list of nodes that have normally established EtherNet/IP connections. Array[x] is TRUE: The connection to the node with a node address of x is established normally. Array[x] is FALSE: A connection is not established yet, or an error has occurred.

9-4 Tag Data Links with Other Models

The performance of tag data links depends on the CPU Unit model and EtherNet/IP Unit model as shown below.

When you use tag data links between the NX-series EtherNet/IP Unit and another CPU Unit or an EtherNet/IP Unit, configure the tag data link settings based on the Unit which has the lower level of communications performance.

● Differences in Tag Data Link Performance Specifications

Item		**NX-series EtherNet/IP Unit**	**NX-series CPU Unit**				**NJ-series CPU Unit**		**CJ2M-CPU3☐**		**CS1W-EIP21** **CJ1W-EIP21** **CJ2H-CPU6☐-EIP**
		NX-EIP201	**NX701**	**NX502**	**NX102**	**NX1P2**			**Unit version**		
							Ver. 1.00 to 1.02	**1.03 or later**	**2.0**	**2.1 or later**	
Tag	Total size of all tags	184,832 words (total of 369,664 words with two ports)	184,832 words (total of 369,664 words with two ports)	46,208 words (total of 92,416 words with two ports)	9,600 words (total of 19,200 words with two ports)	9,600 words			640 words		184,832 words
	Maximum size of tag	722 words (721 words when the tag set includes the Controller status)	722 words (721 words when the tag set includes the Controller status)		300 words (299 words when the tag set includes the Controller status)				20 words (19 words when the tag set includes the Controller status)	640 words (639 words when the tag set includes the Controller status)	722 words (721 words when the tag set includes the Controller status)
	Number of registrable tags	1024 (total of 2048 with two ports)	256 (total of 512 with two ports)			256[*1]			32		256

Item		NX-series EtherNet/IP Unit	NX-series CPU Unit				NJ-series CPU Unit		CJ2M-CPU3☐		CS1W-EIP21 CJ1W-EIP21 CJ2H-CPU6☐-EIP
									Unit version		
		NX-EIP201	NX701	NX502	NX102	NX1P2	Ver. 1.00 to 1.02	1.03 or later	2.0	2.1 or later	
Tag set	Maximum size of 1 tag set	722 words (721 words when the tag set includes the Controller status)	722 words (721 words when the tag set includes the Controller status)		300 words (299 words when the tag set includes the Controller status)				20 words (19 words when the tag set includes the Controller status)	640 words (639 words when the tag set includes the Controller status)	722 words (721 words when the tag set includes the Controller status)
	Number of tags per tag set	64 (63 tags when the tag set includes the Controller status) Note: Input and output variables cannot be combined in one tag set.	8 (7 tags when the tag set includes the Controller status) Note: Input and output variables cannot be combined in one tag set.	64 (63 tags when the tag set includes the Controller status) Note: Input and output variables cannot be combined in one tag set.	8 (7 tags when the tag set includes the Controller status) Note: Input and output variables cannot be combined in one tag set.						
	Number of registrable tag sets	256 (total of 512 with two ports)	256 (total of 512 with two ports)	64 (total of 128 with two ports)	32 (total of 40 with two ports)[2]	32			32		256
Connection	Number of connections	256 (total of 512 with two ports)	256 (total of 512 with two ports)	64 (total of 128 with two ports)	32 (total of 64 with two ports)	32			32		256
	Maximum data size per connection	722 words[3] (Data concurrency is maintained at each connection.)	722 words[3] (Data concurrency is maintained at each connection.)		300 words (Refer to *9-1-7 Concurrency of Tag Data Link Data* on page 9-12 for the conditions for maintaining data concurrency on a connection basis.)				20 words (Data concurrency is maintained at each connection.)	640 words	252 or 722 words[3] (Data concurrency is maintained at each connection.)

Item	NX-series EtherNet/IP Unit	NX-series CPU Unit				NJ-series CPU Unit		CJ2M-CPU3☐		CS1W-EIP21 CJ1W-EIP21 CJ2H-CPU6☐-EIP
								Unit version		
	NX-EIP201	NX701	NX502	NX102	NX1P2	Ver. 1.00 to 1.02	1.03 or later	2.0	2.1 or later	
Packet intervals (RPIs)	1.0 to 10,000 ms in 1.0-ms increments	0.5 to 10,000 ms in 0.5-ms increments	1 to 10,000 ms in 1-ms increments		2 to 10,000 ms in 1-ms increments	10 to 10,000 ms in 1-ms increments	1 to 10,000 ms in 1-ms increments	1 to 10,000 ms in 0.5-ms increments		0.5 to 10,000 ms in 0.5-ms increments
Communications bandwidth used (pps)[*4]	40,000 pps[*5][*6]	40,000 pps[*5]	20,000 pps[*5]	12,000 pps[*5]	3,000 pps	1,000 pps	3,000 pps	3,000 pps		6,000 pps

*1. The maximum number of tags is given for the following conditions.
- All tag sets contain eight tags.
- The maximum number of tag sets (32) is registered.

*2. When tag sets that exceed total of 40 are set, a Number of Tag Sets for Tag Data Links Exceeded (840E0000 hex) event occurs.

*3. To use data of 505 bytes or more, large forward open (an optional CIP specification) should be supported. The SYSMAC CS/CJ-series Units support large forward open, and if you use nodes from other companies, confirm that the devices also support it.

*4. Here, pps means “packets per second” and indicates the number of packets that can be processed in one second.

*5. If the two EtherNet/IP ports are used simultaneously, the maximum communications data size means the maximum data size of the total of the two ports.

*6. When the Unit is performing tag data link communications where the allowable communications bandwidth per Unit is close to or greater than 30,000 pps, the following functions may not be used properly. In that case, use the built-in EtherNet/IP port on the CPU Unit or an EtherNet/IP port of a different NX-series EtherNet/IP Unit.
- Connecting the Sysmac Studio online from the EtherNet/IP port of the NX-series EtherNet/IP Unit
- Connecting the Network Configurator online from the EtherNet/IP port of the NX-series EtherNet/IP Unit
- Connecting the NA-series Programmable Terminal online from the EtherNet/IP port of the NX-series EtherNet/IP Unit
- Port forward via the NX-series EtherNet/IP Unit
- CIP message communications
- SNMP function

These functions of the NX-series EtherNet/IP Unit can be used via X Bus from the built-in EtherNet/IP port on the CPU Unit or an EtherNet/IP port of a different NX-series EtherNet/IP Unit.

*7. An NX-EIP201 can only be used with the NX502 CPU Unit. However, check the effect on task execution time because it increases I/O refreshing time.

● Specifying Tags

When you assign a tag to a device, you can specify the device with its network variable or I/O memory address. Some CPU Units, however, may not support both of these methods. Communications with such CPU Units are possible though, regardless of whether the I/O memory address or network variable is specified for the tag assignment.

The supported tag specification methods for each CPU Unit are listed in the table below.

Yes: Supported, No: Not supported

CPU Unit		Network Configurator hardware list name	Specifying with network variable	Specifying with I/O memory address
	EtherNet/IP Unit			
NX-series CPU Unit	----	NX701	Yes	No
		NX502	Yes	Yes [1]
		NX102	Yes	Yes [1][2]
		NX1P2□□□□	Yes	Yes [1][2]
	NX-EIP201	NX-EIP201	Yes	Yes [1][2]
NJ-series CPU Unit	---	NJ501-□□□□ NJ301-□□□□ NJ101	Yes	Yes[1]
	CJ1W-EIP21	CJ1W-EIP21 (NJ)	Yes	Yes[1]
CJ2H-CPU6□-EIP	---	CJ2B-EIP21	Yes	Yes
	CJ1W-EIP21	CJ1W-EIP21 (CJ2)	Yes	Yes
CJ2H-CPU6□	CJ1W-EIP21	CJ1W-EIP21 (CJ2)	No	Yes
CJ2M-CPU3□	---	CJ2M-EIP21	Yes	Yes
	CJ1W-EIP21	CJ1W-EIP21 (CJ2)	Yes	Yes
CJ2M-CPU1□	CJ1W-EIP21	CJ1W-EIP21 (CJ2)	No	Yes
CJ1 CPU Unit	CJ1W-EIP21	CJ1W-EIP21	No	Yes
CS1 CPU Unit	CS1W-EIP21	CS1W-EIP21	No	Yes

[1] To specify an I/O memory address for tag assignment, do not specify the address directly. Instead, create a variable with an AT specification of the I/O memory address on the Sysmac Studio, and then specify the variable for the tag.

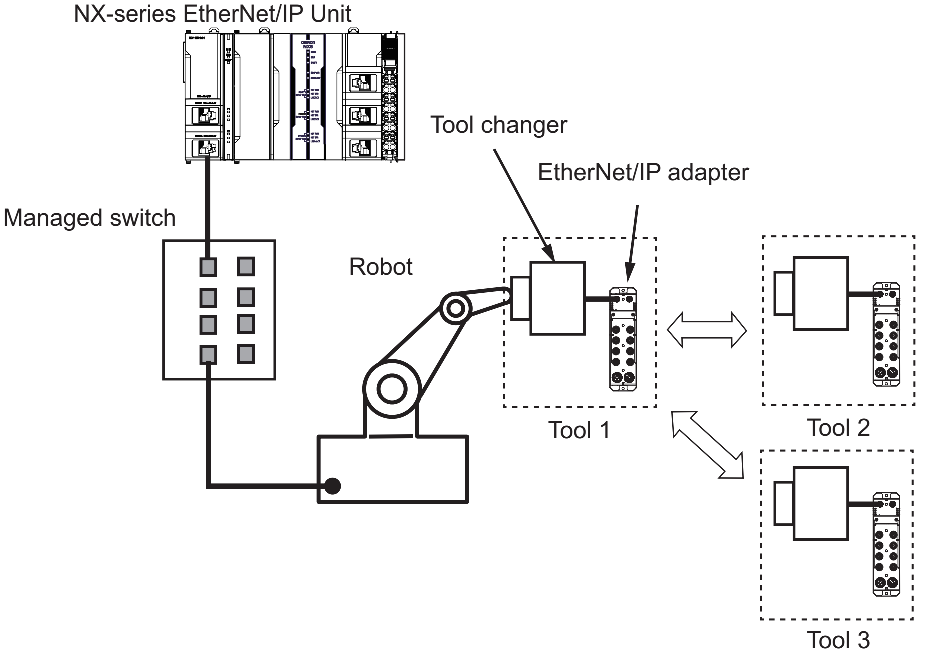
[2] For NX102 and NX1P2 CPU Units, you need to set memory used for CJ-series Unit to use the I/O memory address. For details on memory settings used for CJ-series Unit, refer to the *NJ/NX-series CPU Unit Software User's Manual (Cat. No. W501)*.

9-5 QuickConnect

The NX-series EtherNet/IP Unit supports the QuickConnect function of the EtherNet/IP standard. This allows for fast start and connection to the EtherNet/IP network.
The QuickConnect function is mainly used for the following purposes.

- Fast switching of tools at the tip of the robot
- Changing the production line equipment

The following gives an example of fast switching of the tools at the tip of the robot. Use the QuickConnect function to quickly switch between tools.



9-5-1 Method of Use

Use the QuickConnect function as follows.

- When the communications port of the NX-series EtherNet/IP Unit is online, turn ON the power supply of the device that is an adapter, and execute the TDLinkStartConnection (Start Tag Data Link Target Connection) instruction to start the tag data link after a certain period of time.
- Also, execute the TDLinkStopConnection (Stop Tag Data Link Target Connection) instruction to stop the tag data link before turning OFF the power supply of the device that is an adapter.

Refer to *Section 13 Instructions Specific to NX-series EtherNet/IP Units* on page 13-1 for detailed instruction specifications.

If the NX-series EtherNet/IP Unit is disconnected from the network without stopping the tag data link with the target node, a *Tag Data Link Error* occurs.
A *Tag Data Link Error* also occurs if the correct IP address is not set for the switched target node after starting the tag data link with the target node. A *Verification Error* occurs if the correct connection settings are not configured on the switched target node.

9-5-2 Managed Switches

To use the QuickConnect function, the managed switches that support the QuickConnect function are required. Follow the instructions in the operation manual of the managed switches for details on the settings on the managed switch side.

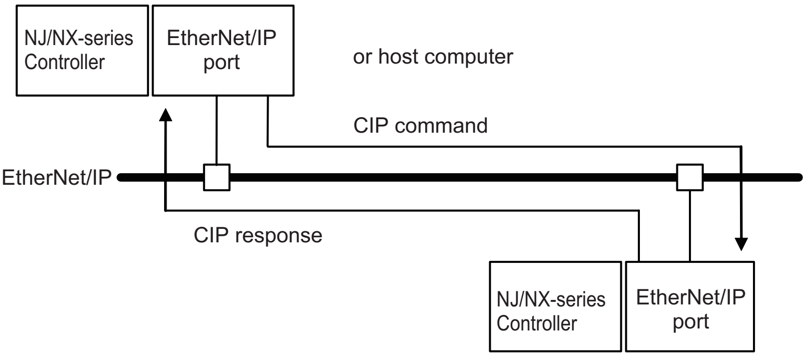
10

CIP Message Communications

10-1 Overview of the CIP Message Communications Service

10-1-1 Overview of the CIP Message Communications Service

CIP commands can be sent to devices on the EtherNet/IP network whenever they are required.
You execute CIP_SEND instructions in a program in the NJ/NX-series CPU Unit to send CIP commands, such as those to read and write data and to receive the responses.
You can use CIP messages from the client to read and write memory in the Controller with the server without adding any special programming to the user program of the Controller with the server.



10-1-2 Message Communications Service Specifications

Item		Specification
Message type		Either of the following can be selected. CIP UCMM connectionless messages CIP class 3 connection messages
Execution method		CIPSend (Send Explicit Message Class 3) instruction or CIPUCMMSend (Send Explicit Message UCMM) instruction
Data contents		Sending required CIP commands and receiving responses
Communications parameters		Message type, timeout value, and route path specification
Maximum length per connection	Non-connection type (UCMM)	502 bytes
	Connection type (class 3)	• Using Forward_Open 502 bytes • Using Large_Forward_Open 8,192 bytes

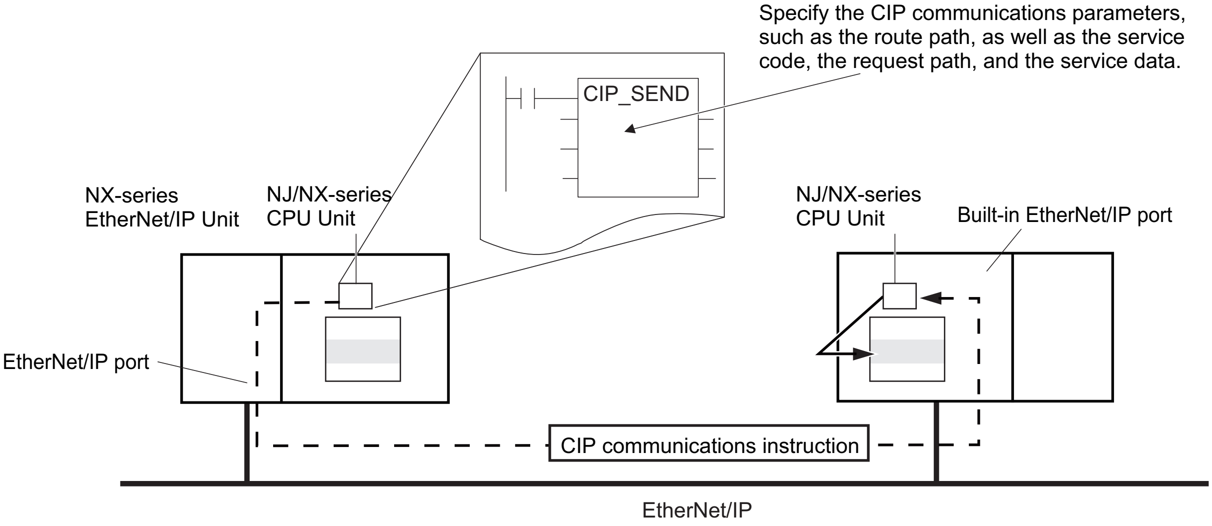
10-2 Client Function of CIP Message Communications

10-2-1 Overview

The NX-series EtherNet/IP Units can send a CIP message to an external device to request a service by specifying an internal object of the device which supports the server function of CIP message communications.

This is called the client function of CIP message communications.

The NX-series EtherNet/IP Units execute CIP communications instructions in the user program and send CIP messages.


Specify the CIP communications parameters, such as the route path, as well as the service code, the request path, and the service data.
CIP_SEND
NX-series EtherNet/IP Unit
NJ/NX-series CPU Unit
NJ/NX-series CPU Unit
Built-in EtherNet/IP port
EtherNet/IP port
CIP communications instruction
EtherNet/IP

10-2-2 CIP Communications Instructions

The following CIP communications instructions are available.

For details on CIP communications instructions, refer to the *NJ/NX-series Instructions Reference Manual (Cat. No. W502)*.

Instructions	Name	Description	Communications method
CIPUCMMSend	Send Explicit Message UCMM	Sends a specified CIP command to the specified remote Controller on the CIP network. Refer to *10-2-8 Response Codes* on page 10-19 and *10-5 CIP Object Services* on page 10-28 for information on the service codes and response codes that are used with the NJ/NX-series CPU Units.	CIP UCMM connectionless message

Instructions	Name	Description	Communications method
CIPOpen	Open CIP Class 3 Connection (Large_Forward_Open)	Opens a CIP class 3 connection (Large_Forward_Open) with the specified remote node.	CIP class 3 connection message
CIPOpenWithDataSize	Open CIP Class 3 Connection with Specified Data Size	Opens a CIP class 3 connection with the specified remote node that allows class 3 explicit messages of the specified data length or shorter to be sent and received.	
CIPSend	Send Explicit Message Class 3	Sends a specified class 3 CIP command to the specified remote Controller on the CIP network. Refer to *10-2-8 Response Codes* on page 10-19 and *10-5 CIP Object Services* on page 10-28 for information on the service codes and response codes that are used with the NJ/NX-series CPU Units.	
CIPClose	Close CIP Class 3 Connection	Closes the CIP class 3 connection that is specified by the handle.	

10-2-3 Using CIP Communications Instructions

CIP message communications include the following processes.

If CIP class 3 connections are used, the open and close processes are required before and after the data is sent and received.

Process	Description	Instruction
Open process (only for CIP class 3 connections)[*1]	Execute this process before you use a CIP message. Open processing is continued until a CIP class 3 connection is established.	CIPOpen CIPOpenWithDataSize
Sending CIP commands	You can set the required CIP command.	CIPUCMMSend CIPSend
Close process (only for CIP class 3 connections)	This process closes the connection.	CIPClose

[*1] The maximum number of connection handles that you can obtain simultaneously through the opening process is 32. Even if a connection is disconnected for a timeout, the handle is not released. Execute the CIPClose instruction to close the connection.

Precautions for Correct Use

You can execute up to 32 CIP communications instructions at the same time regardless of the instruction types.

Use exclusive control in the user program so that the number of CIP communications instructions executed at the same time does not exceed the above number.

10-2-4 Route Path

The route path indicates the path from the source Controller of CIP communications instructions to the destination Controller on the network.

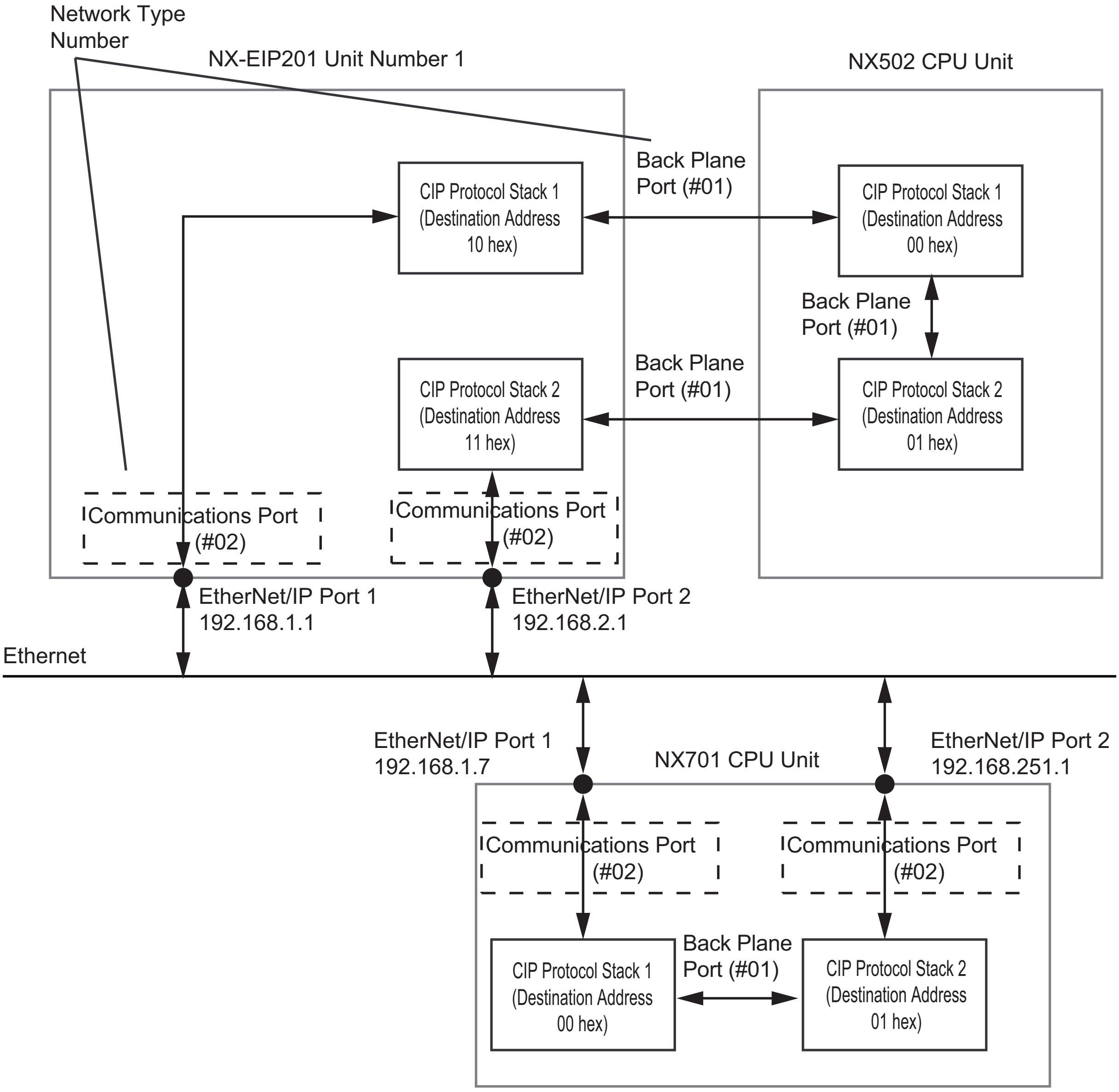
Routing for CIP communications instructions is performed based on the route path. Set the route path in the *RoutePath* input variable of the CIP communications instructions.

Route Path Notation

The route path describes the route from the source Controller to the destination Controller using the network type number and destination address as follows.

Network type number\#Destination address\Network type number\#Destination address
Do not add # to the network type number, and add # to the beginning of the destination address.

The meaning of network type number and destination address is described below.


Network Type Number
NX-EIP201 Unit Number 1
NX502 CPU Unit
Back Plane Port (#01)
CIP Protocol Stack 1 (Destination Address 10 hex)
CIP Protocol Stack 1 (Destination Address 00 hex)
Back Plane Port (#01)
Back Plane Port (#01)
CIP Protocol Stack 2 (Destination Address 11 hex)
CIP Protocol Stack 2 (Destination Address 01 hex)
Communications Port (#02)
Communications Port (#02)
EtherNet/IP Port 1 192.168.1.1
EtherNet/IP Port 2 192.168.2.1
Ethernet
EtherNet/IP Port 1 192.168.1.7
NX701 CPU Unit
EtherNet/IP Port 2 192.168.251.1
Communications Port (#02)
Communications Port (#02)
Back Plane Port (#01)
CIP Protocol Stack 1 (Destination Address 00 hex)
CIP Protocol Stack 2 (Destination Address 01 hex)

● Network Type Number

A network type number is a number that is assigned to each port on the path to the destination Controller. There are two types of port: backplane port and communications port.

A backplane port is a port between CIP Protocol Stacks[*1] in the CPU Unit or the NX-series EtherNet/IP Unit. The NX502 CPU Unit and NX-series EtherNet/IP Unit each have two built-in CIP Protocol Stacks. CIP Protocol Stack1 is connected to the EtherNet/IP port 1 and CIP Protocol Stack2 is connected to the EtherNet/IP port 2.
A communications port is an EtherNet/IP port on the NX-series EtherNet/IP Unit.
The network type numbers that are assigned to the backplane port and communications port are as follows.

Port	Network type number (hexadecimal)
Backplane port	#01
Communications port	#02

*1. A CIP Protocol Stack is a collection of communications protocols related to CIP message communications that are gathered to perform the CIP message communications. The CIP Protocol Stack has the function to send, receive, and transfer the communications data from one port to another port.

● Destination Address

The destination address indicates the address of the Controller at the destination of the port or the CIP Protocol Stack in the Controller. The destination address of the Controller is represented by the IP address of the EtherNet/IP port on that Controller. The destination address of the CIP Protocol Stack is determined as follows.

Destination Unit	Unit number	CIP Protocol Stack	Destination address (hexadecimal)
CPU Unit	---	CIP Protocol Stack1	#00
		CIP Protocol Stack2	#01
NX-series EtherNet/IP Unit	1	CIP Protocol Stack1	#10
		CIP Protocol Stack2	#11
	2	CIP Protocol Stack1	#20
		CIP Protocol Stack2	#21
	3	CIP Protocol Stack1	#30
		CIP Protocol Stack2	#31
	4	CIP Protocol Stack1	#40
		CIP Protocol Stack2	#41

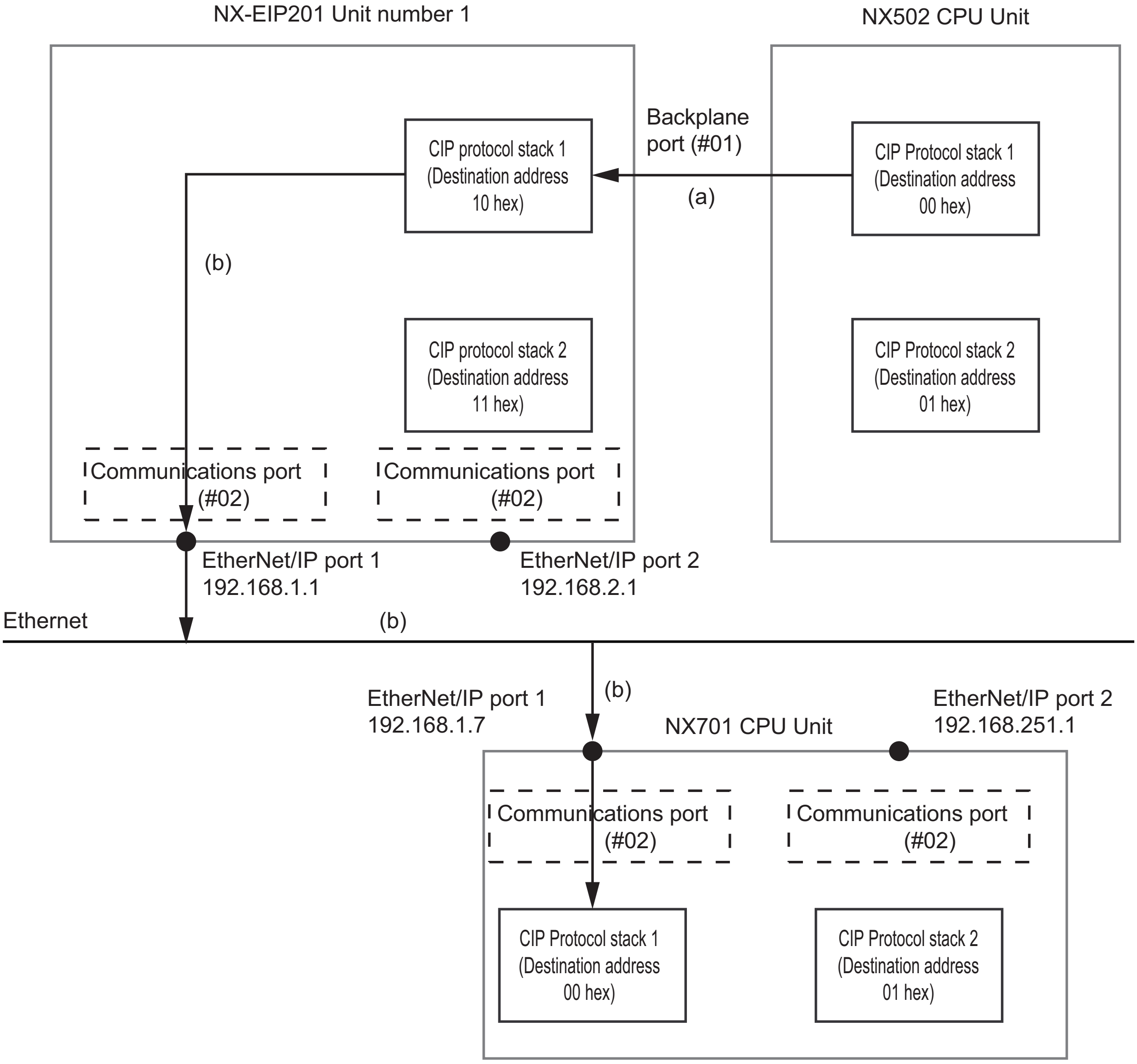
Route Path Notation Examples

The following gives examples of route path.

- Communicating from the EtherNet/IP port 1 on an NX-series EtherNet/IP Unit to the EtherNet/IP port 1 on an NX701 CPU Unit
- Communicating from the EtherNet/IP port 2 on an NX-series EtherNet/IP Unit to CIP Protocol Stack2 via the EtherNet/IP port 1 on an NX701 CPU Unit
- Communicating from the EtherNet/IP port 1 on an NX701 CPU Unit to the EtherNet/IP port 1 on an NX-series EtherNet/IP Unit
- Communicating from the EtherNet/IP port 2 on an NX701 CPU Unit to CIP Protocol Stack1 via the EtherNet/IP port 2 on an NX-series EtherNet/IP Unit
- Communicating from the EtherNet/IP port 1 on an NX-series EtherNet/IP Unit with unit number 2 to the EtherNet/IP port 1 on an NX701 CPU Unit

- Communicating from the EtherNet/IP port 2 on an NX701 CPU Unit to CIP Protocol Stack1 via the EtherNet/IP port 2 on an NX-series EtherNet/IP Unit with unit number 2

Communicating from the EtherNet/IP Port 1 on an NX-series EtherNet/IP Unit to the EtherNet/IP Port 1 on an NX701 CPU Unit

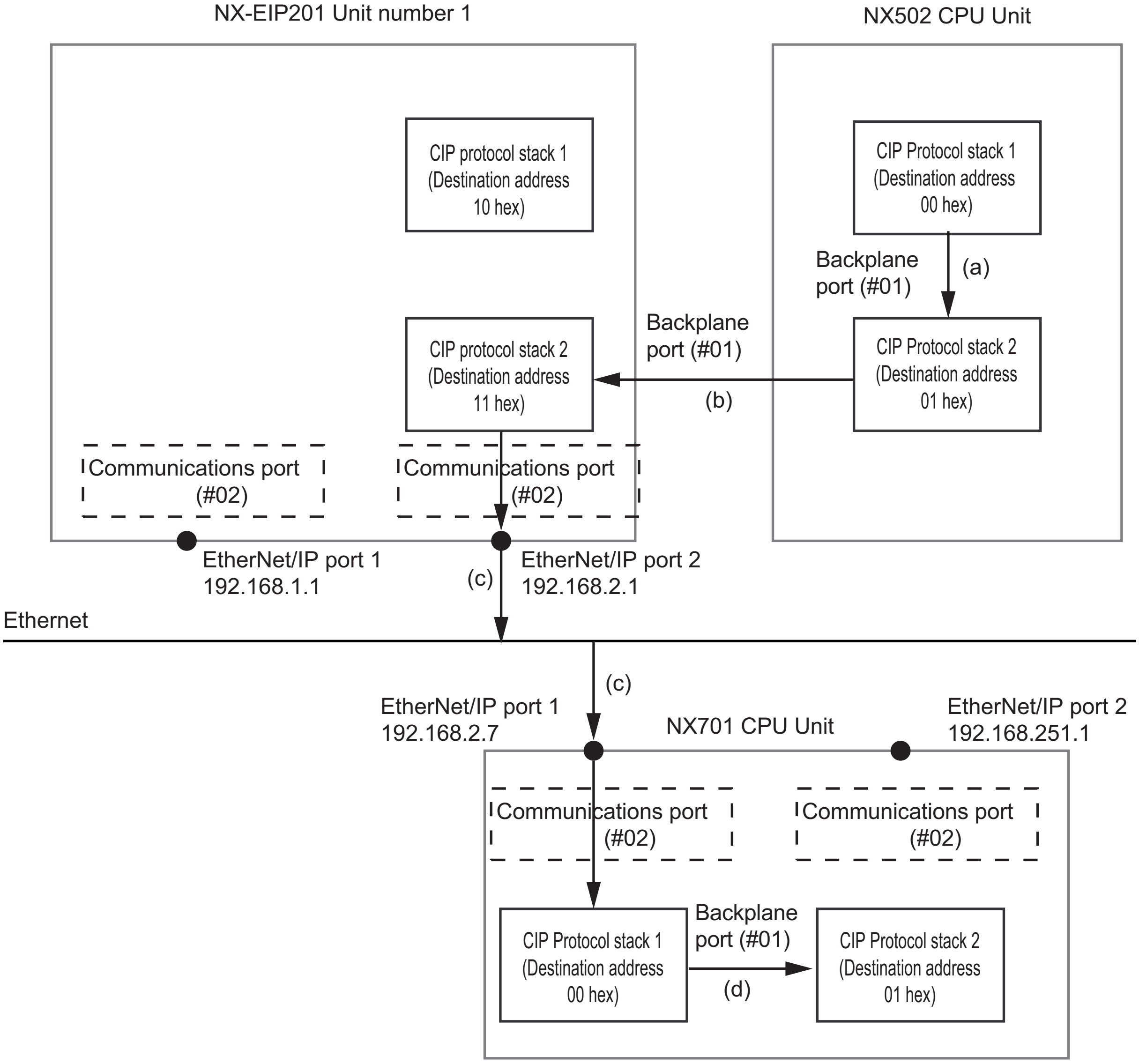

NX-EIP201 Unit number 1
NX502 CPU Unit
Backplane port (#01)
CIP protocol stack 1 (Destination address 10 hex)
(a)
CIP Protocol stack 1 (Destination address 00 hex)
(b)
CIP protocol stack 2 (Destination address 11 hex)
CIP Protocol stack 2 (Destination address 01 hex)
Communications port (#02)
Communications port (#02)
EtherNet/IP port 1 192.168.1.1
EtherNet/IP port 2 192.168.2.1
Ethernet
(b)
EtherNet/IP port 1 192.168.1.7
(b)
NX701 CPU Unit
EtherNet/IP port 2 192.168.251.1
Communications port (#02)
Communications port (#02)
CIP Protocol stack 1 (Destination address 00 hex)
CIP Protocol stack 2 (Destination address 01 hex)

The network type numbers and the destination addresses for routes (a) and (b) in the above figure are as shown in the table below.

Route	Network type number	Destination address
(a)	#01	#10
(b)	#02	192.168.1.7

Therefore, the route path is as follows.
01\#10\02\192.168.1.7

Communicating from the EtherNet/IP Port 2 on an NX-series EtherNet/IP Unit to CIP Protocol Stack2 via the EtherNet/IP Port 1 on an NX701 CPU Unit

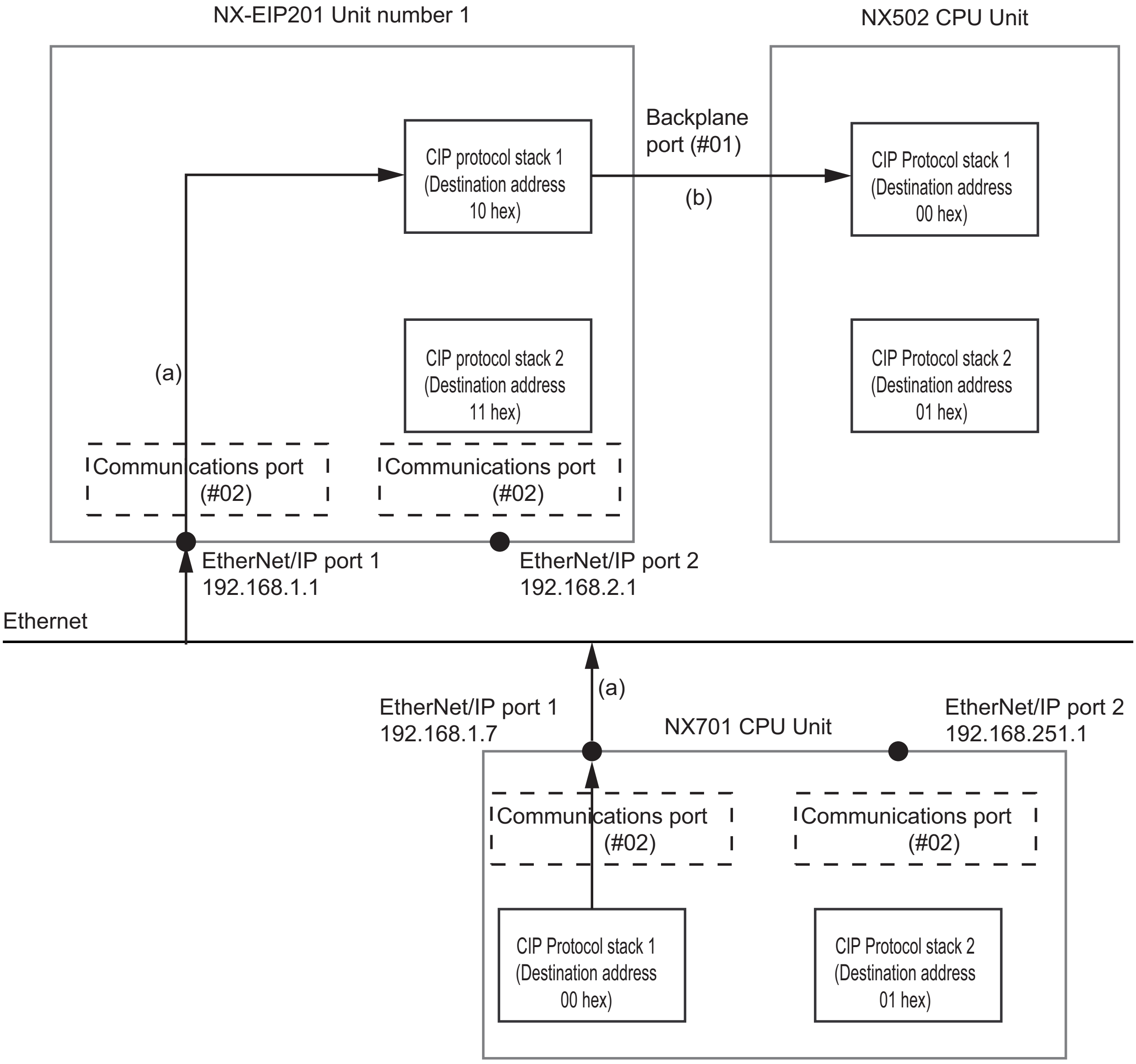

NX-EIP201 Unit number 1
NX502 CPU Unit
CIP protocol stack 1 (Destination address 10 hex)
CIP Protocol stack 1 (Destination address 00 hex)
Backplane port (#01)
(a)
Backplane port (#01)
CIP protocol stack 2 (Destination address 11 hex)
CIP Protocol stack 2 (Destination address 01 hex)
(b)
Communications port (#02)
Communications port (#02)
EtherNet/IP port 1
192.168.1.1
(c)
EtherNet/IP port 2
192.168.2.1
Ethernet
(c)
EtherNet/IP port 1
192.168.2.7
NX701 CPU Unit
EtherNet/IP port 2
192.168.251.1
Communications port (#02)
Communications port (#02)
CIP Protocol stack 1 (Destination address 00 hex)
Backplane port (#01)
(d)
CIP Protocol stack 2 (Destination address 01 hex)

The network type numbers and the destination addresses for routes (a) to (d) in the above figure are as shown in the table below.

Route	Network type number	Destination address
(a)	#01	#01
(b)	#01	#11
(c)	#02	192.168.2.7
(d)	#01	#01

Therefore, the route path is as follows.
01\#01\01\#11\02\192.168.2.7\01#01

Communicating from the EtherNet/IP Port 1 on an NX701 CPU Unit to the EtherNet/IP Port 1 on an NX-series EtherNet/IP Unit

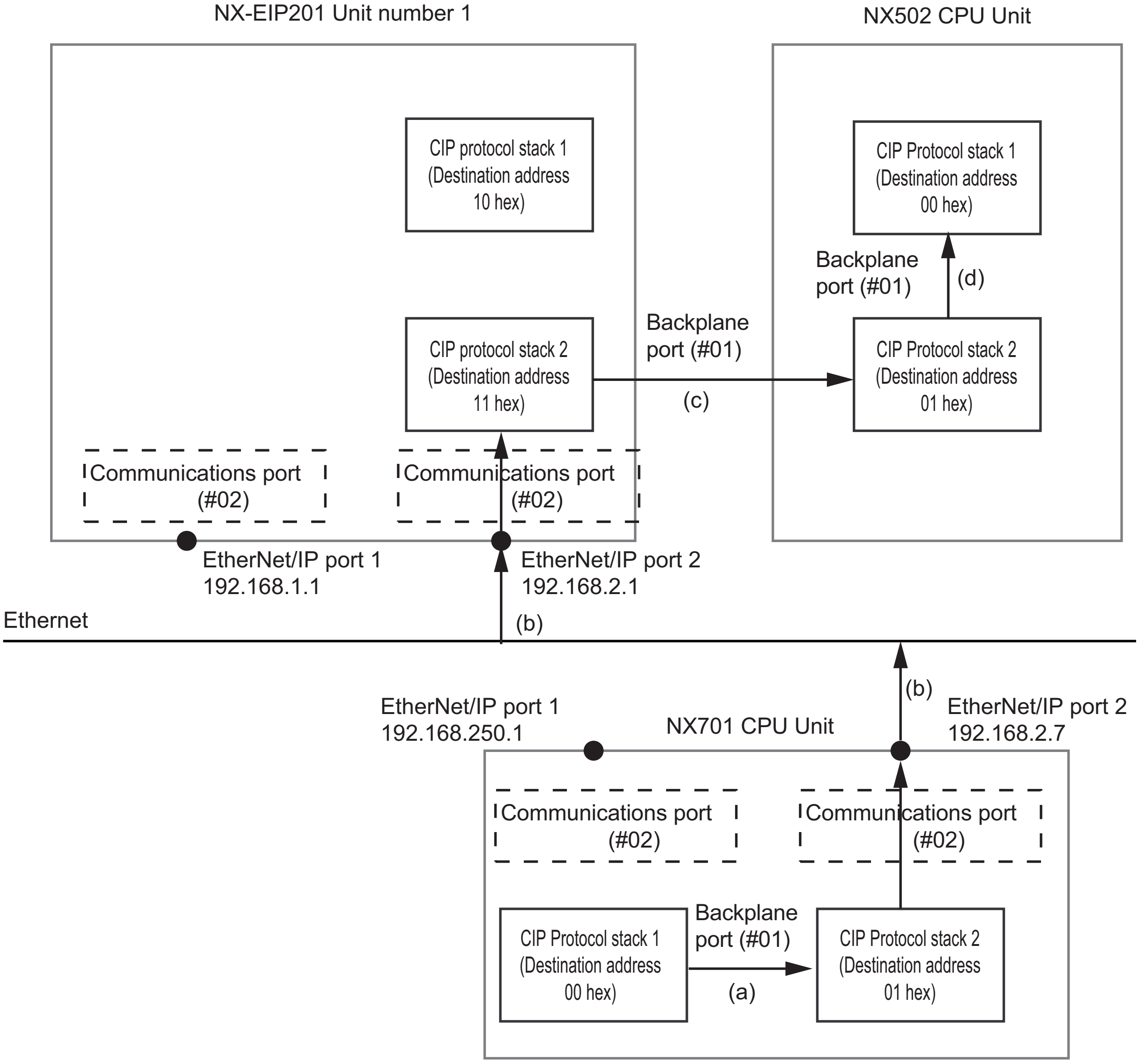

NX-EIP201 Unit number 1
NX502 CPU Unit
CIP protocol stack 1 (Destination address 10 hex)
Backplane port (#01)
(b)
CIP Protocol stack 1 (Destination address 00 hex)
(a)
CIP protocol stack 2 (Destination address 11 hex)
CIP Protocol stack 2 (Destination address 01 hex)
Communications port (#02)
Communications port (#02)
EtherNet/IP port 1 192.168.1.1
EtherNet/IP port 2 192.168.2.1
Ethernet
(a)
EtherNet/IP port 1 192.168.1.7
NX701 CPU Unit
EtherNet/IP port 2 192.168.251.1
Communications port (#02)
Communications port (#02)
CIP Protocol stack 1 (Destination address 00 hex)
CIP Protocol stack 2 (Destination address 01 hex)

The network type numbers and the destination addresses for routes (a) and (b) in the above figure are as shown in the table below.

Route	Network type number	Destination address
(a)	#02	192.168.1.1
(b)	#01	#00

Therefore, the route path is as follows.
02\192.168.1.1\01#00

Communicating from the EtherNet/IP Port 2 on an NX701 CPU Unit to CIP Protocol Stack1 via the EtherNet/IP Port 2 on an NX-series EtherNet/IP Unit

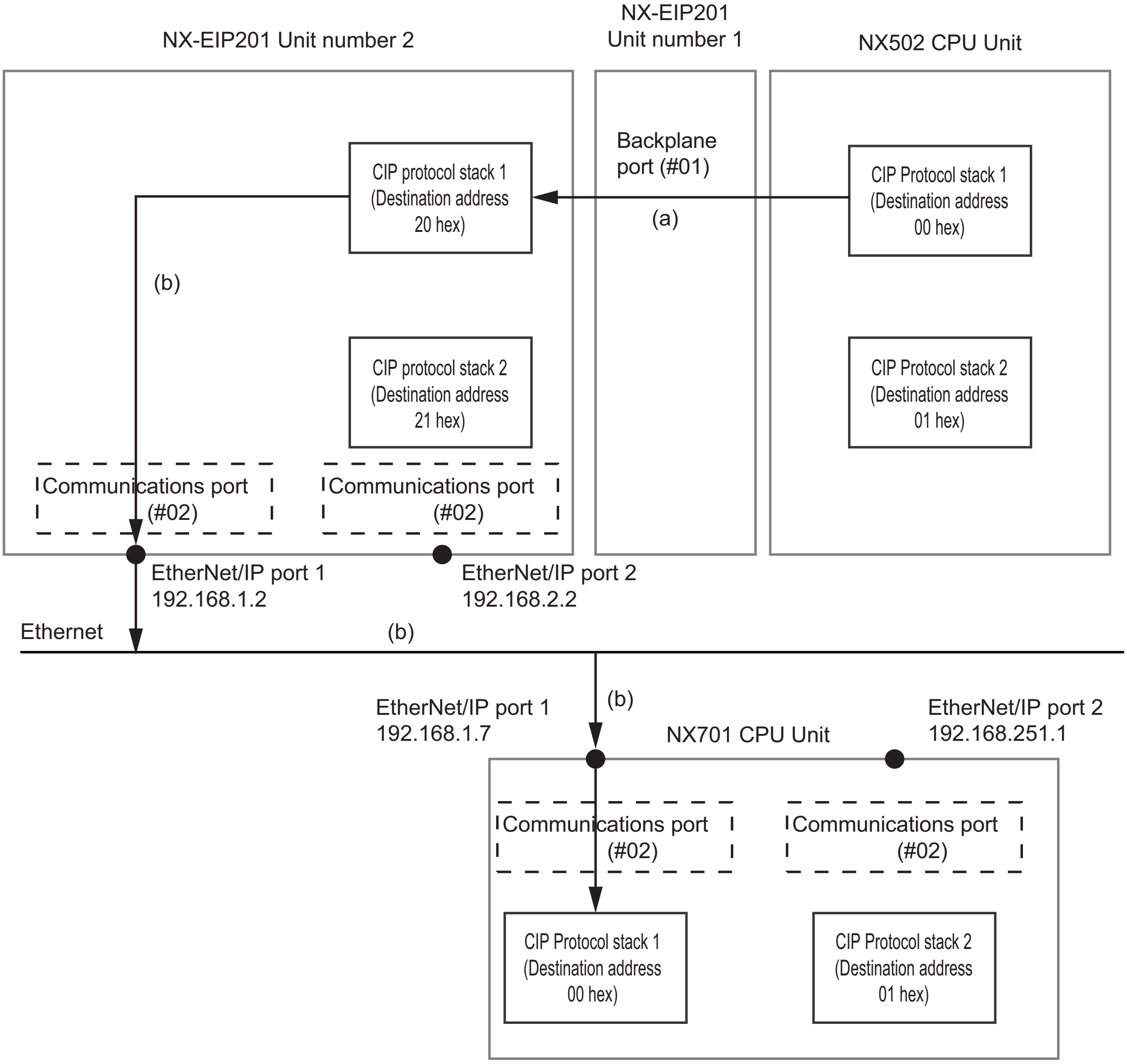

NX-EIP201 Unit number 1
NX502 CPU Unit
CIP protocol stack 1 (Destination address 10 hex)
CIP protocol stack 2 (Destination address 11 hex)
CIP Protocol stack 1 (Destination address 00 hex)
CIP Protocol stack 2 (Destination address 01 hex)
Backplane port (#01)
(d)
Backplane port (#01)
(c)
Communications port (#02)
Communications port (#02)
EtherNet/IP port 1 192.168.1.1
EtherNet/IP port 2 192.168.2.1
Ethernet
(b)
(b)
EtherNet/IP port 1 192.168.250.1
NX701 CPU Unit
EtherNet/IP port 2 192.168.2.7
Communications port (#02)
Communications port (#02)
CIP Protocol stack 1 (Destination address 00 hex)
Backplane port (#01)
(a)
CIP Protocol stack 2 (Destination address 01 hex)

The network type numbers and the destination addresses for routes (a) to (d) in the above figure are as shown in the table below.

Route	Network type number	Destination address
(a)	#01	#01
(b)	#02	192.168.2.1
(c)	#01	#01
(d)	#01	#00

Therefore, the route path is as follows.
01\#01\02\192.168.2.1\01\#01\01\#00

Communicating from the EtherNet/IP Port 1 on an NX-series EtherNet/IP Unit with Unit Number 2 to the EtherNet/IP Port 1 on an NX701 CPU Unit

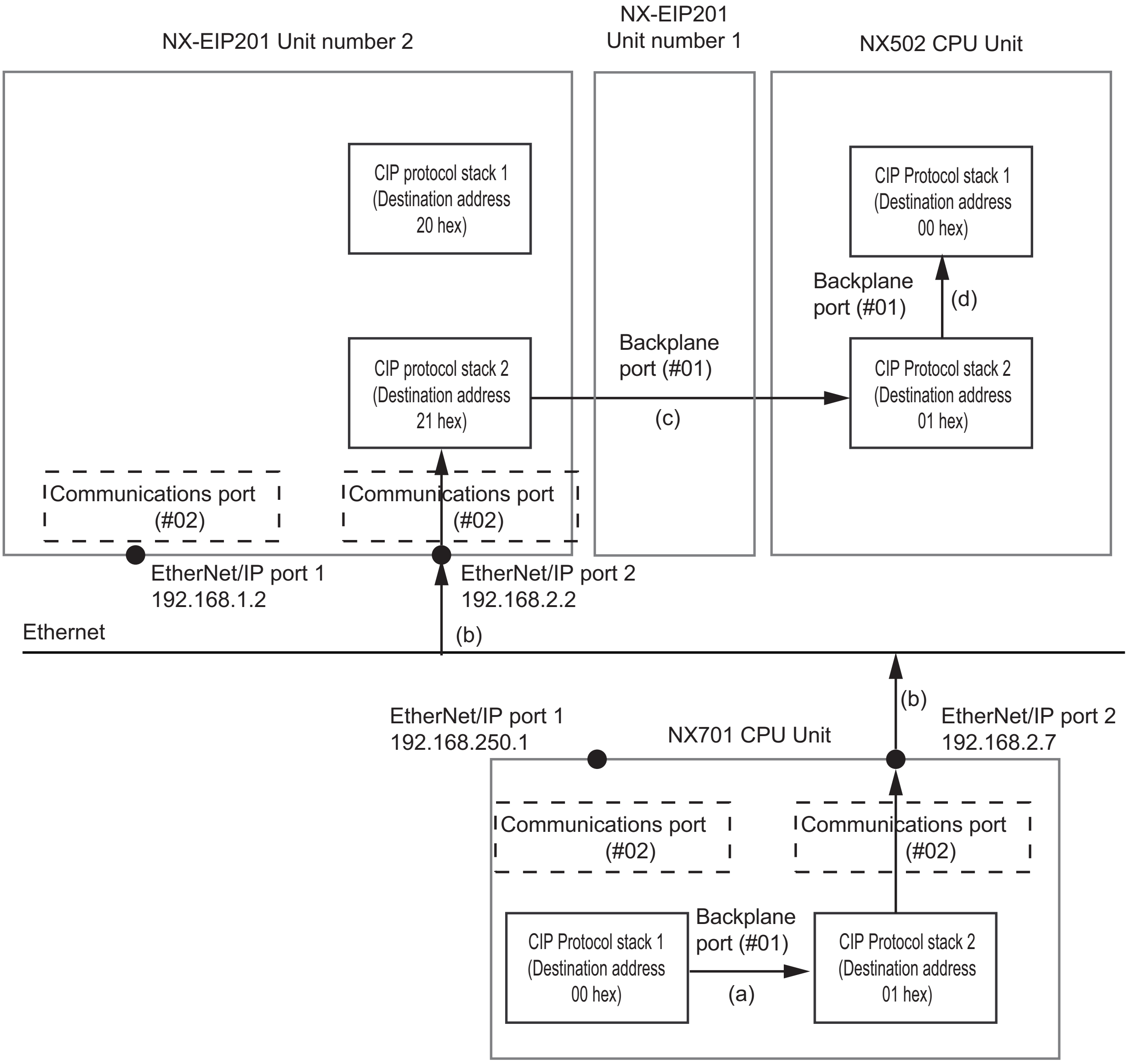


The network type numbers and the destination addresses for routes (a) and (b) in the above figure are as shown in the table below.

Route	Network type number	Destination address
(a)	#01	#20
(b)	#02	192.168.1.7

Therefore, the route path is as follows.
01\#20\02\192.168.1.7

Communicating from the EtherNet/IP Port 2 on an NX701 CPU Unit to CIP Protocol Stack1 via the EtherNet/IP Port 2 on an NX-series EtherNet/IP Unit with Unit Number 2


NX-EIP201 Unit number 2
NX-EIP201 Unit number 1
NX502 CPU Unit
CIP protocol stack 1 (Destination address 20 hex)
CIP Protocol stack 1 (Destination address 00 hex)
Backplane port (#01)
(d)
Backplane port (#01)
CIP protocol stack 2 (Destination address 21 hex)
CIP Protocol stack 2 (Destination address 01 hex)
(c)
Communications port (#02)
Communications port (#02)
EtherNet/IP port 1 192.168.1.2
EtherNet/IP port 2 192.168.2.2
Ethernet
(b)
(b)
EtherNet/IP port 1 192.168.250.1
NX701 CPU Unit
EtherNet/IP port 2 192.168.2.7
Communications port (#02)
Communications port (#02)
Backplane port (#01)
CIP Protocol stack 1 (Destination address 00 hex)
(a)
CIP Protocol stack 2 (Destination address 01 hex)

The network type numbers and the destination addresses for routes (a) to (d) in the above figure are as shown in the table below.

Route	Network type number	Destination address
(a)	#01	#01
(b)	#02	192.168.2.2
(c)	#01	#01
(d)	#01	#00

Therefore, the route path is as follows.

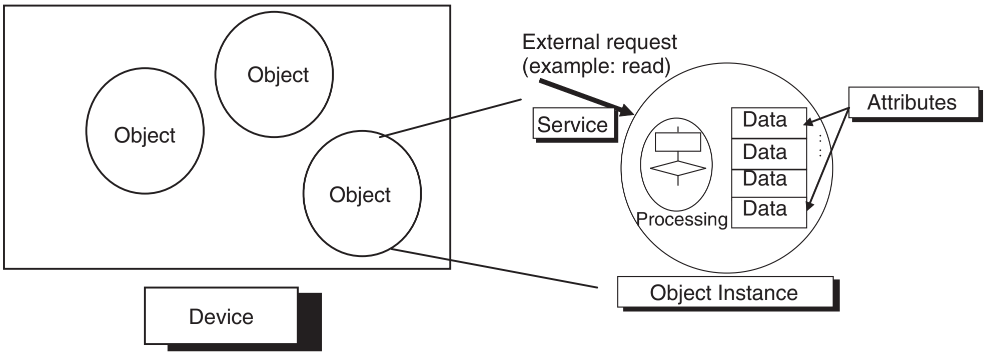
01\#01\02\192.168.2.2\01\#01\01\#00

10-2-5 Request Path (IOI)

A request path indicates an object of a device on the network.
A CIP communications instruction uses the request path to access an object of a device.

Overview of Request Path

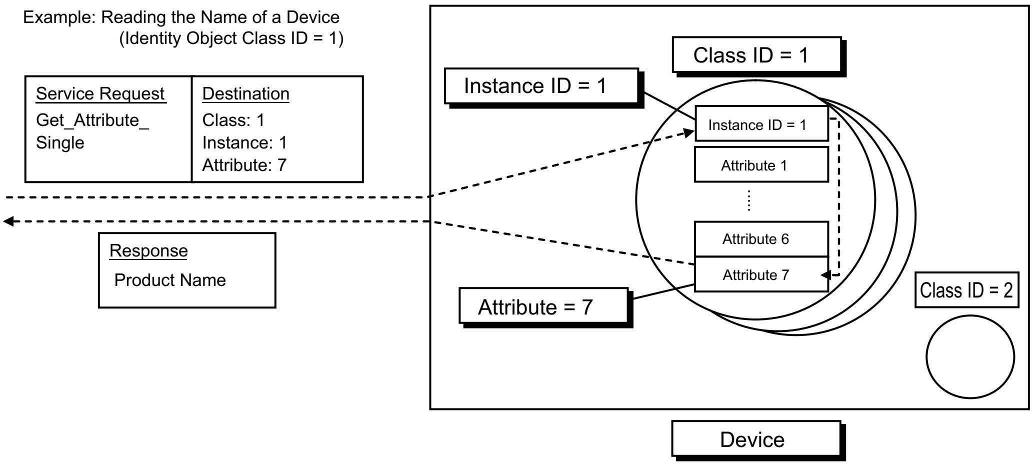
In the CIP world, each device is modeled as a collection of objects. An Object abstractly represents the specific configuration elements of a device.



In the CIP Common Specification, Object, Class, Instance, Attribute, and Service are defined as follows: (Source: CIP Common Specification)

Term	Definition
Object	An abstract representation of a particular component within a device.
Class	A set of objects that all represent the same kind of system component.
Instance	A specific and real (physical) occurrence of an object.
Attribute	A description of an externally visible characteristic or feature of an object.
Service	A request from an external object (e.g., to read data).

You use the Class ID Instance ID and Attribute ID to access an object.
You specify these three IDs to designate an object in a device.
When you make a request from an external device for a service, you must specify the Class ID Instance ID and Attribute ID. (The Instance ID and Attribute ID are not required for some services.)



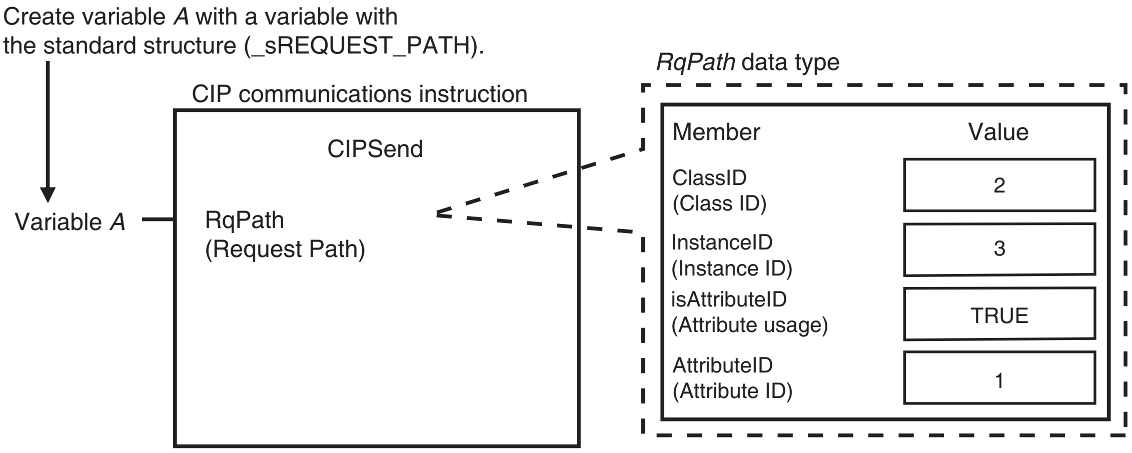
These are called *IOI* (Internal Object Identifier) because they identify the Class ID, Instance ID, and Attribute ID within the device.
Refer to *10-5 CIP Object Services* on page 10-28 for the class ID, instance ID, attribute ID, and service code for each object.

Providing the Structure Variables to Input Request Paths

For a CIP communications instruction, you prepare a variable to store the request path. In this variable, you specify the object to access with the user program.
A structure in which the Class ID, Instance ID, and Attribute ID are specified is provided for the data type of a variable for a request path.
There are two types of structures: standard structure (_sREQUEST_PATH) and extension structure (_sREQUEST_PATH_EX). When you use an extension structure, it is possible to specify the size according to the size of values of the Class ID, Instance ID, and Attribute ID of the object that you access. When you use a standard structure, the size is always set to 16 bits.

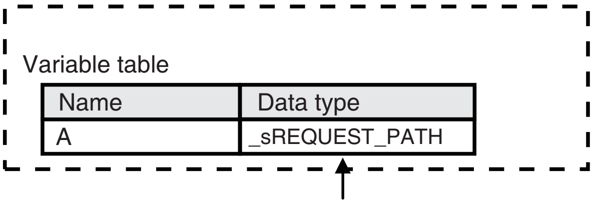
● When a Standard Structure Variable Is Used

Example: Using a standard structure variable to input values into *RqPath* (Request Path) for the CIPSend instruction


Create variable *A* with a variable with
the standard structure (_sREQUEST_PATH).
CIP communications instruction
CIPSend
Variable *A*
RqPath
(Request Path)
RqPath data type

Member	Value
ClassID (Class ID)	2
InstanceID (Instance ID)	3
isAttributeID (Attribute usage)	TRUE
AttributeID (Attribute ID)	1

1 Create a standard structure variable.
To use a standard structure variable to input values into *RqPath* (Request Path) for a CIP communications instruction, first you need to create a standard structure user-defined variable.
When you create a variable in a variable table, select the pre-registered standard structure (_sREQUEST_PATH) for a CIP communications instruction.

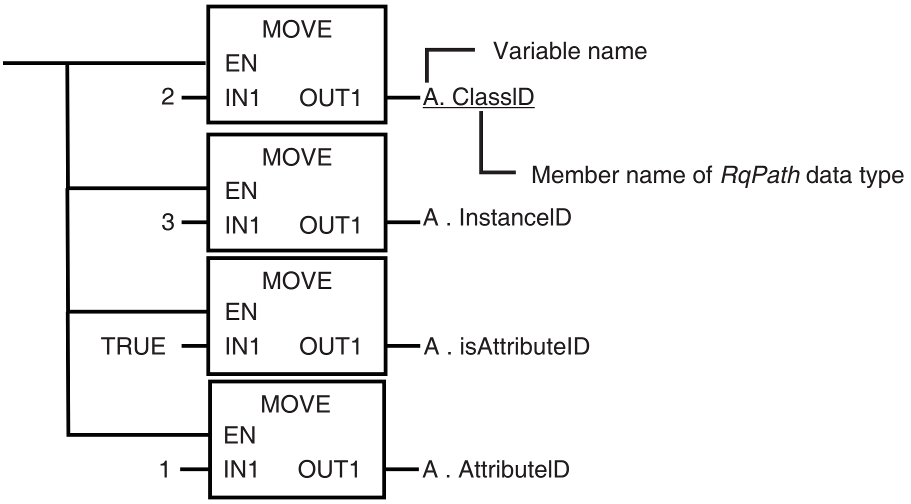

Variable table

Name	Data type
A	_sREQUEST_PATH

Select a standard structure for the data type of variable *A*.

2 Input a value for each standard structure variable member.

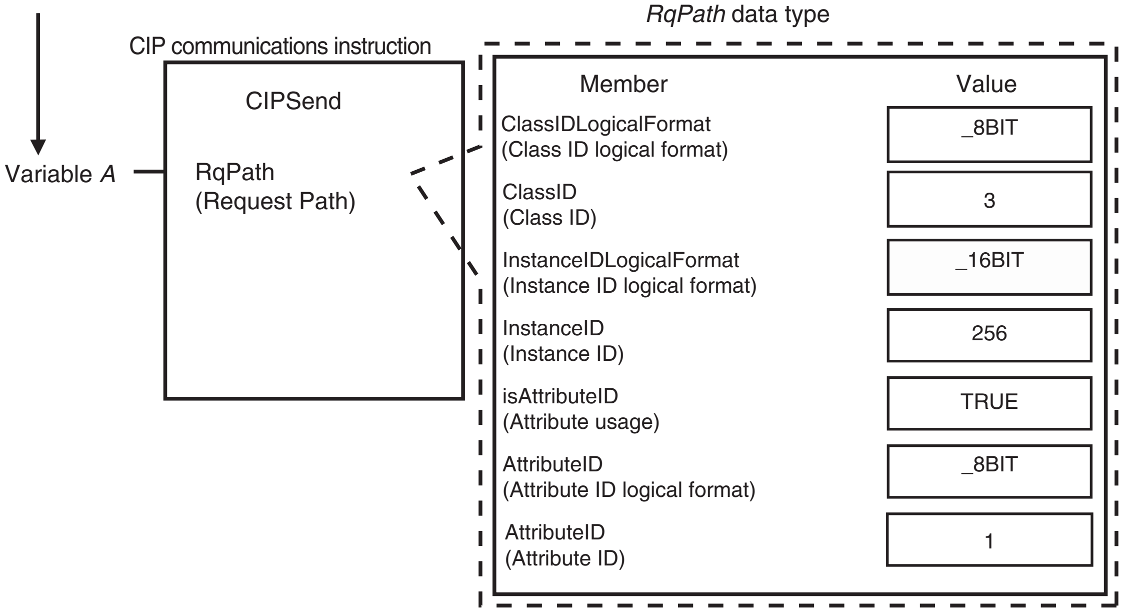
Input the following values into the communications parameters that were registered as members of the standard structure variable.



● When an Extension Structure Variable Is Used

Example: Using an extension structure variable to input values into *RqPath* (Request Path) for the CIPSend instruction

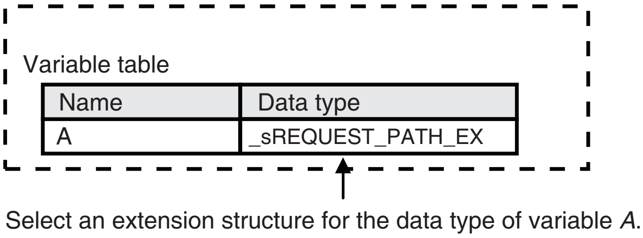
Create variable *A* with a variable with
the extension structure (_sREQUEST_PATH_EX).



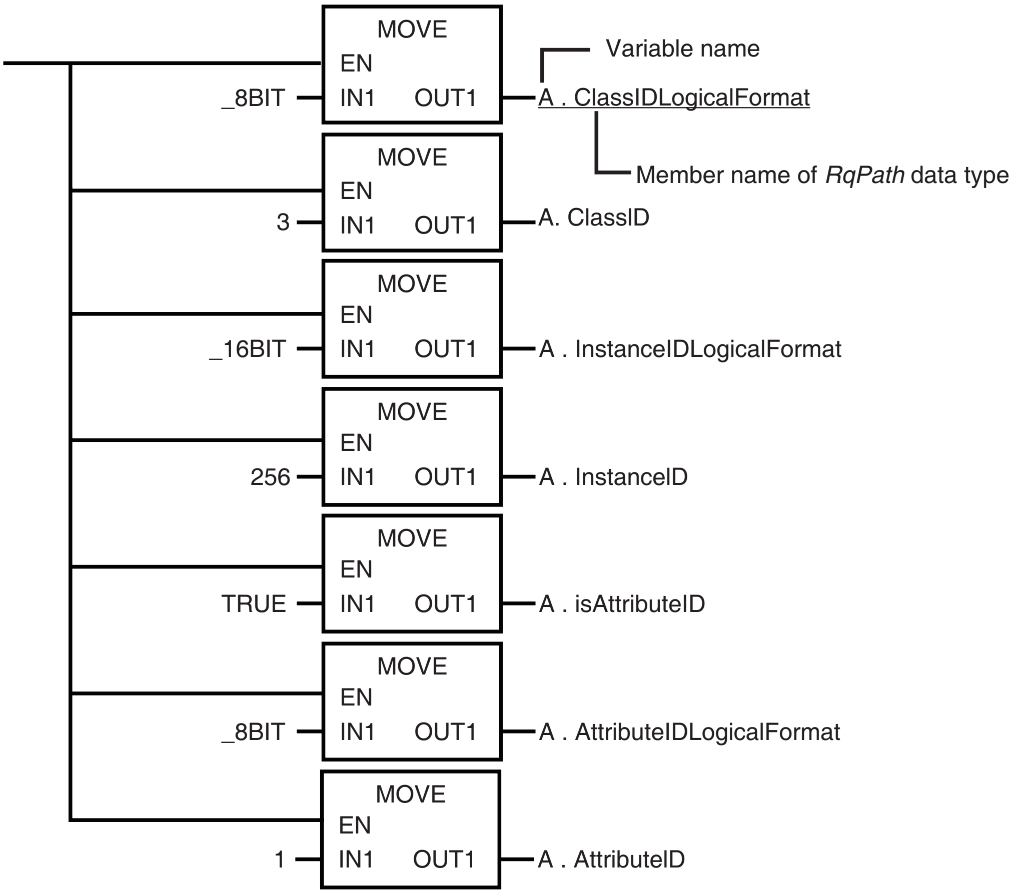
1 Create an extension structure variable.

To use an extension structure variable to input values into *RqPath* (Request Path) for a CIP communications instruction, first you need to create an extension structure user-defined variable.

When you create a variable in a variable table, select the pre-registered extension structure (_sREQUEST_PATH_EX) for a CIP communications instruction.


Variable table
Name
Data type
A
_sREQUEST_PATH_EX
Select an extension structure for the data type of variable *A*.

2 Input a value for each extension structure variable member.
Input the following values into the communications parameters that were registered as members of the extension structure variable.



10-2-6 Service Data and Response Data

CIP communications instructions send and receive data that is stored in array variables.

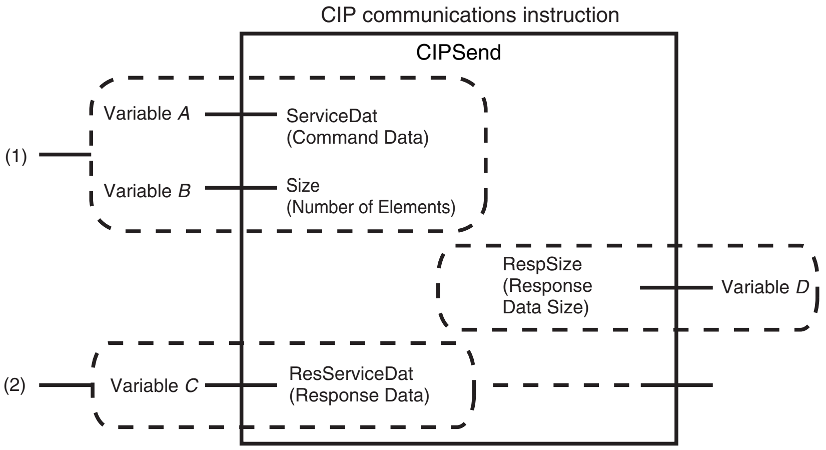
Preparing Array Variables to Input and Output Service Data and Response Data

This section describes the array variables for storing service data and response data that CIP communications instructions send and receive.

● Creating Array Variables

To input a value into the array variable of a CIP communications instruction, you must create a variable with the same configuration as the array variable in advance.

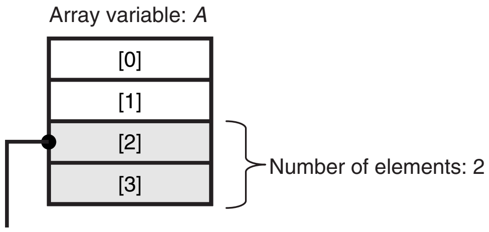
Example: Creating a Variable to Input Data to the CIPSend Instruction Array Variables


CIP communications instruction
CIPSend
(1)
Variable A
ServiceDat (Command Data)
Variable B
Size (Number of Elements)
RespSize (Response Data Size)
Variable D
(2)
Variable C
ResServiceDat (Response Data)

(1) Input the service data to send

The data to send is stored in array variable *A*.

If only certain elements are specified in array variable *A*, specify the number of elements in variable *B*.

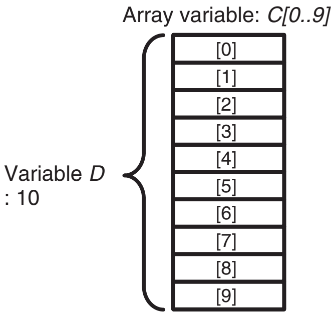


If the service data (*ServiceDat*) is *Array[2]* and number of elements (*Size*) = 2, *Array[2]* and *Array[3]* are sent.

(2) Store received response data

The data that is received is stored in variable *C*.

The byte size of the data that was actually received is stored in variable *D*.



Use the following procedure to create a variable in the variable table.

Specify the element first number, the element last number, and the data type.

Example: UINT Array

Variable table

Variable name	Data type
A	ARRAY[0..19] OF UINT

Specifies the data type.

● CIP Communications Instructions That Use Array Variables

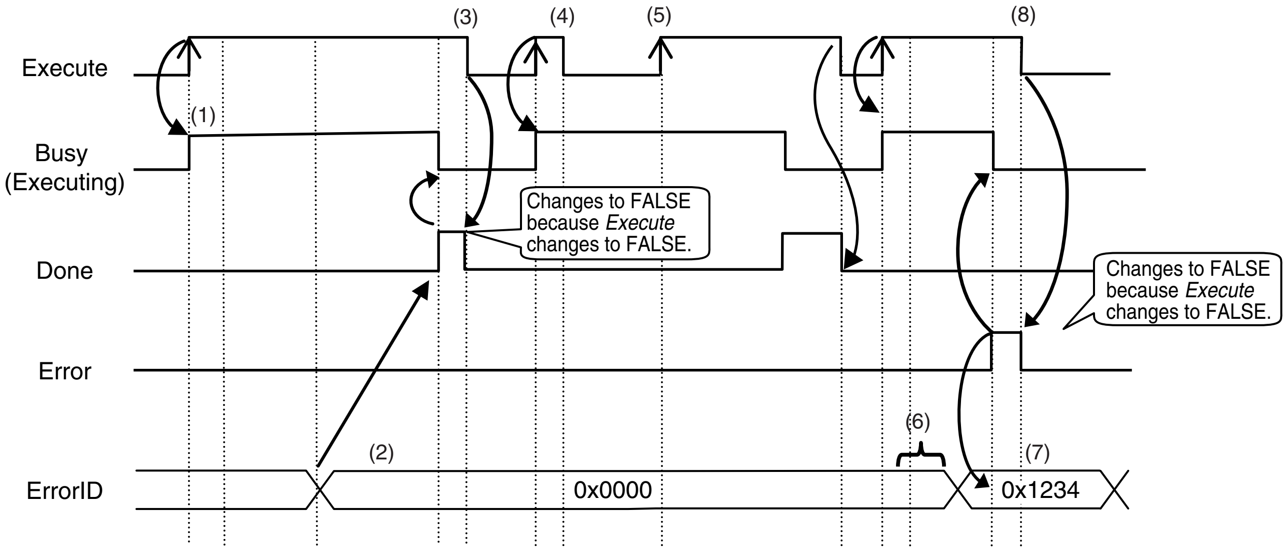
Instruction	Structure variable name		
	Input variable	In-out variable	Output variable
CIPSend	ServiceDat (Command Data)	ResServiceDat (Response Data)	---

10-2-7 Operation Timing

Output Variable Operation and Timing

You can monitor the values of the output variables to determine the status throughout instruction execution.

The following timing chart shows the operation of the output variables.

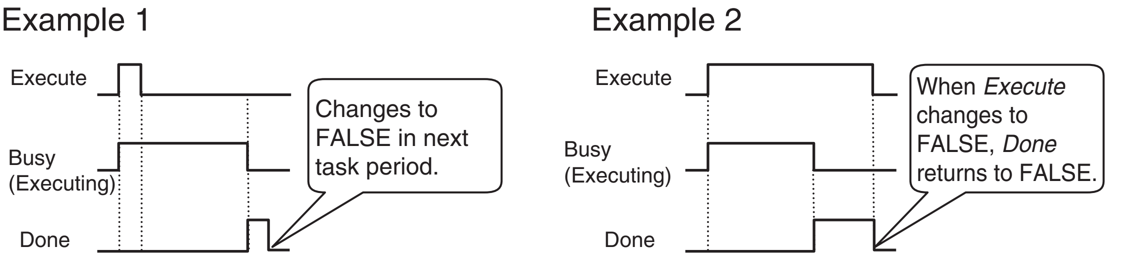


(3)
(4)
(5)
(8)
Execute
(1)
Busy
(Executing)
Changes to FALSE because *Execute* changes to FALSE.
Done
Changes to FALSE because *Execute* changes to FALSE.
Error
(6)
(2)
(7)
ErrorID
0x0000
0x1234

1. When *Execute* changes to TRUE, the instruction is executed and *Busy* changes to TRUE.
2. After the results of instruction execution are stored in the output variables, *Done* changes to TRUE and *Busy* changes to FALSE.
3. When *Execute* changes to FALSE, *Done* returns to FALSE.
4. When *Execute* changes to TRUE again, *Busy* changes to TRUE.
5. *Execute* is ignored if it changes to TRUE during instruction execution (i.e., when *Busy* is TRUE).
6. If an error occurs, several retries are attempted internally. The error code in *ErrorID* is not updated during the retries.
7. When a communications error occurs, *Error* changes to TRUE and the value of *ErrorID* is stored. Also, *Busy* and *Done* change to FALSE.
8. When *Execute* changes to FALSE, *Error* changes to FALSE.

Precautions for Correct Use

If *Execute* changes back to FALSE before *Done* changes to TRUE, *Done* stays TRUE for only one task period. (Example 1)
If you want to see if *Done* is TRUE at any time, make sure to keep *Execute* TRUE until you confirm that *Done* is TRUE.
If *Execute* is TRUE until *Done* changes to TRUE, *Done* stays TRUE until *Execute* changes to FALSE. (Example 2)

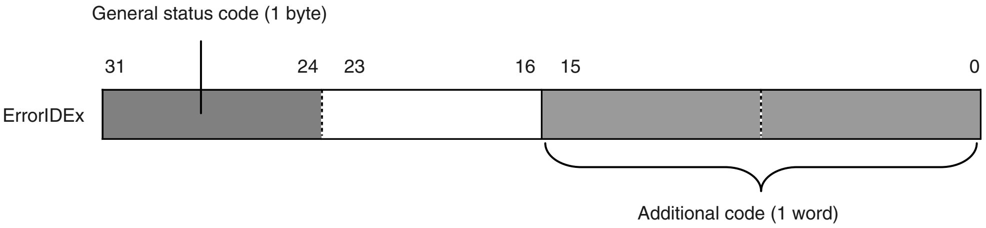

Example 1
Execute
Busy (Executing)
Done
Changes to FALSE in next task period.
Example 2
Execute
Busy (Executing)
Done
When *Execute* changes to FALSE, *Done* returns to FALSE.

10-2-8 Response Codes

This section describes the response codes stored in the *ErrorIDEx* output variable if an error occurs during execution of a CIP message communications instruction.

General Status Codes

As response codes, general codes are stored in the *ErrorIDEx* output variable (DWORD data) after execution of a CIP communications instruction is completed.
If an additional code is added, the additional code is also stored.



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 to 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.
04	Path segment error	The path segment identifier or the segment syntax was not understood by the processing node. Path processing stops when a path segment error occurs.
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 stops when a Path Destination Unknown Error occurs.

General status code (hex)	Status name	Description of status
06	Partial transfer	Only part of the expected data was transferred.
07	Connection lost	The message connection was lost.
08	Service not supported	The requested service was not supported or was not defined for this object class/instance.
09	Invalid attribute value	Invalid attribute data was 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 requested 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	An object that does not exist was specified for the requested service.
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.
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 occurred. The Additional Code Field of the error response defines the error. This is a general error code that is used only for errors that do not correspond to any of the error codes in this table and are not in an object class definition.

General status code (hex)	Status name	Description of status
20	Invalid parameter	A parameter for the requested service is invalid. This code is used when a parameter does not meet the requirements of the 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 or PROM) that was previously written or cannot be changed.
22	Invalid Reply Received	An invalid reply was received. (For example, the reply service code does not match the request service code. Or, the reply message is shorter than the minimum expected reply size.) This status code is used 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 must indicate which part of the key check failed.
26	Path Size Invalid	The size of the path that was sent with the service request is either too large or too small for the request to be routed to an object.
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, and 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 is reported only by group 2 only servers with 4K or less of code space and only in place of *Service not supported, Attribute not supported, or 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. This code range is used only when none of the error codes in this table accurately reflect the error that occurred. The additional code field is used to describe the general error code in more detail.

● Examples of Additional Status When General Status Is 01 hex (Status of Connection Manager Object)

General Status (hex)	Additional Status (hex)	Description
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. There is 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.

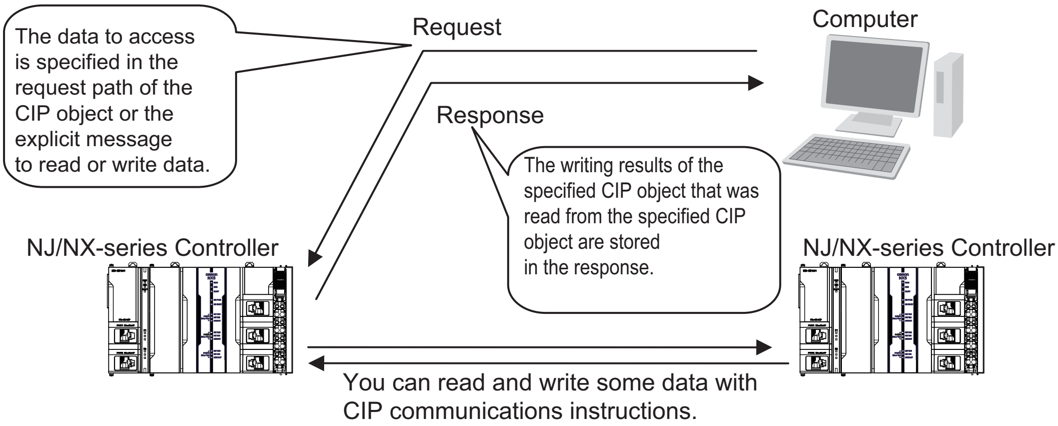
General Status (hex)	Additional Status (hex)	Description
01	0114	Either the vendor ID or the product code in the key segment does not match the device.
01	0115	Device type in the key segment does not match the device.
01	0116	*Major Revision* or *Minor Revision* in the key segment.
01	0117	Invalid connection point.
01	0118	Invalid configuration format.
01	0119	Connection request failed because 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 because the connection has timed out.
01	0204	Unconnected_Send service timed out while waiting for a response.
01	0205	Parameter error in Unconnected_Send service.
01	0206	Message too large for unconnected message service.
01	0207	Unconnected acknowledgment 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 that was specified in port segment is not available.
01	0312	Link address that was specified in port segment is not available.
01	0315	Invalid segment type or segment value in path.
01	0316	Path and connection were not equal when closing the connection.
01	0317	The segment is not present. Or, the encoded value in the network segment is invalid.
01	0318	Link address to self is invalid.
01	0319	Resources on secondary are unavailable.
01	031A	Connection is already established.
01	031B	Direct connection is already established.
01	031C	Others
01	031D	Redundant connection mismatch.
01	031E	There are no more reception resources available on the sending module.
01	031F	No connection resources exist for the target path.
01	0320-07FF	Vendor specific.

10-3 Server Function of CIP Message Communications

After the NX-series EtherNet/IP Unit receives the CIP messages from external devices, this function executes services for a specified self-contained object in the NX-series EtherNet/IP Unit.
This is called the server function of CIP message communications.

This section describes the structure of CIP messages that are sent to read/write CIP objects from/to the NX-series EtherNet/IP Unit from a program on a computer, etc. using the server function of CIP message communications.

To read and write CIP objects between NX-series EtherNet/IP Units or between an NX-series EtherNet/IP Unit and an NJ/NX-series Controller, use the CIP communications instructions.
Refer to *10-2 Client Function of CIP Message Communications* on page 10-3 for information on how to use CIP communications instructions for CIP message communications.


The data to access is specified in the request path of the CIP object or the explicit message to read or write data.
Request
Computer
Response
The writing results of the specified CIP object that was read from the specified CIP object are stored in the response.
NJ/NX-series Controller
NJ/NX-series Controller
You can read and write some data with CIP communications instructions.

Precautions for Correct Use

- To allow the NX-series EtherNet/IP Unit to receive CIP messages, select the **Use** Option for the CIP message server of the EtherNet/IP port. If the **Do not use** Option for the CIP message server is selected, the Unit cannot receive CIP messages. For the details on the settings, refer to *CIP Message Server* on page 7-15.
- If the **Use** Option is selected for Packet Filter of the EtherNet/IP port, make sure to permit packets to be used for CIP messages. If they are not permitted, the CIP message cannot be received. For the details on the settings, refer to *Packet Filter* on page 7-7.
- If the **Do not use**, Option for the CIP message server is selected, EtherNet/IP communications cannot be used. This causes the following restrictions on the functionality of connection tools and Controllers.

Category	Restrictions
Tools	• Tag data link setting using Sysmac Studio is not possible. • CX-Compolet and SYSMAC Gateway cannot be connected. [*1] • Network Configurator cannot be connected. Or, devices cannot be displayed.
Controller features	• The tag data link function cannot be used. • CIP Safety communications cannot be used. • The server function of CIP messages (UCMM, Class3) in the EtherNet/IP port cannot be used.

[*1] The tag monitoring function of CX-Compolet and the tag monitoring function of the EtherNet/IP Monitor Tool included with the SYSMAC Gateway do not allow the NX-series EtherNet/IP Unit to be specified as a connected device.

- NX-series EtherNet/IP Units do not have the server function of CIP message communications to read and write variables. However, they can use CIP routing to read/write variables from/to the NX-series EtherNet/IP Unit. Refer to the *NJ/NX-series CPU Unit Built-in EtherNet/IP Port User’s Manual (Cat. No. W506)* for details on the CIP routing function of the CPU Unit.

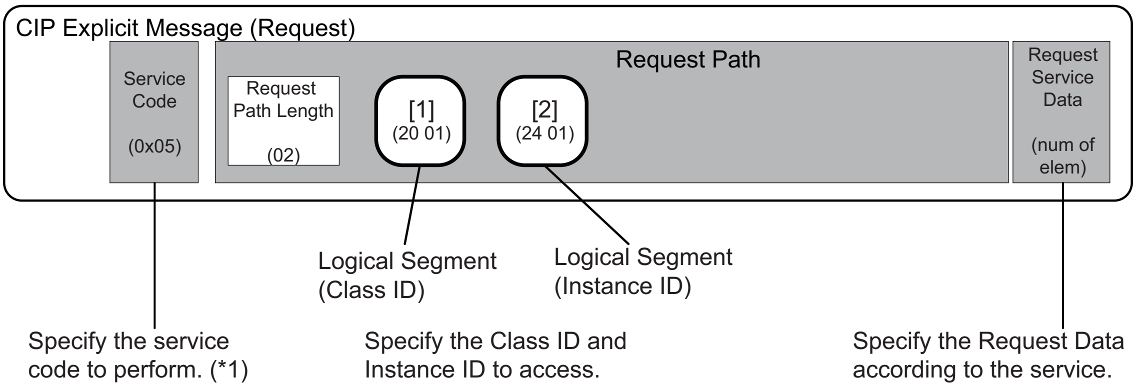
Additional Information

- Selecting the **Do not use** Option for the CIP message server closes the TCP/UDP ports used for EtherNet/IP communications. This improves security of communications over the network.
- Even if the **Do not use** Option for the CIP message server is selected, the TCP/UDP message services can be used. You can also use the client function (CIP communications instructions) of CIP message communications.

10-3-1 CIP Message Structure for Accessing CIP Objects

This section shows how to specify messages to access CIP objects.
The CIP objects to be accessed are expressed by connecting the segments
defined in the CIP Common Specifications in the request path field in a CIP explicit message.

Example: Performing the Reset service (0x05) to the Instance (01 hex) of the Identity object (class: 01 hex)


CIP Explicit Message (Request)
Service Code
(0x05)
Request Path
Request Path Length
(02)
[1]
(20 01)
[2]
(24 01)
Request Service Data
(num of elem)
Logical Segment (Class ID)
Logical Segment (Instance ID)
Specify the service code to perform. (*1)
Specify the Class ID and Instance ID to access.
Specify the Request Data according to the service.

*1. Refer to *10-5 CIP Object Services* on page 10-28 for information about the service codes.

10-4 Specifying Request Path

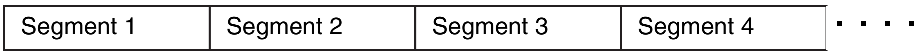
The CIP object is specified in the request path.

In CIP, the EPATH data type is used for the request path.

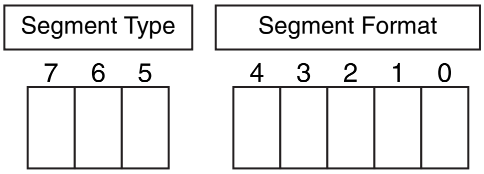
With this method, the request path is divided into segments and a value is assigned to each segment.

The request path notation shows the path to the final destination when the data segments are joined together.

Each segment includes the segment type information and the segment data.



The first byte gives the interpretation method for the segment. It consists of two parts; a 3-bit segment type and a 5-bit segment format.



The segment type specifications are defined as follows in the CIP specifications.

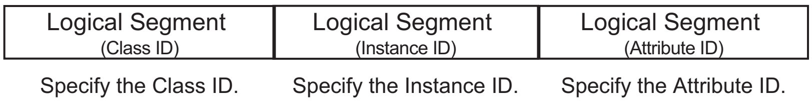
Segment Type			**Meaning**
7	**6**	**5**	
0	0	0	Port Segment
0	0	1	Logical Segment
0	1	0	Network Segment
0	1	1	Symbolic Segment
1	0	0	Data Segment
1	0	1	Data Type
1	1	0	Data Type
1	1	1	Reserved

The specifications for the segment format are different for each segment type. Use the segment format to request a service from a particular object of a particular device.

Logical segments and data segments, which are needed to specify variables in CIP message communications, are described below.

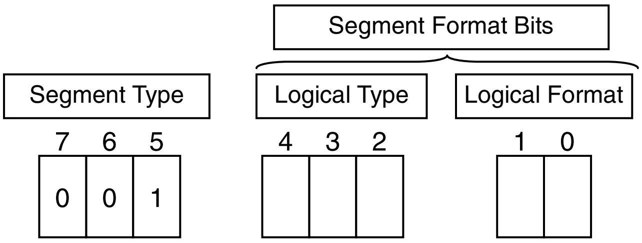
10-4-1 Examples of CIP Object Specifications

Logical Segments are joined to form the request path that specifies the object to access.



10-4-2 Logical Segment

A logical segment is used to give the CIP Object in the request path.



Logical Type			Meaning
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		Meaning
1	0	
0	0	8 bit logical address
0	1	16 bit logical address
1	0	32 bit logical address
1	1	Reserved

An 8-bit or 16-bit logical address can be used for the class ID and attribute ID.

An 8-bit,16-bit, or 32-bit logical address can be used for the instance ID.

10-5 CIP Object Services

This section shows services that specify the CIP object in the Request Path and access the CIP message server function of the NJ/NX-series Controllers.

10-5-1 CIP Objects Sent to the EtherNet/IP Port

The following CIP objects can be sent to an EtherNet/IP port.

Object name	Function	Reference
Identity object	• Reads ID information from the CPU Unit. • Resets the EtherNet/IP port.	page 10-28
TCP/IP interface object	• Writes and reads TCP/IP settings.	page 10-32
Ethernet link object	• Makes Ethernet settings and reads the settings. • Reads Ethernet status.	page 10-35

10-5-2 Identity Object (Class ID: 01 hex)

This object reads the ID information of the Unit and resets the EtherNet/IP port.
Use the route path to specify the port number (1 or 2) of the EtherNet/IP port to access.

Service Codes

Specify the service to execute with the service code.

Service code	Parameter name	Description	Supported services	
			Classes	Instances
01 hex	Get_Attribute_All	Reads the values of the attributes.	Supported	Supported
0E hex	Get_Attribute_Single	Reads the value of the specified attribute.	Supported	Supported
05 hex	Reset	Resets the EtherNet/IP port. This parameter is used to reset the EtherNet/IP port when you change the IP address or other parameter settings and want to apply them. Input one of the following values for the *ServiceDat* input variable to the CIPSend instruction to specify the reset method. 00 hex: Resets the EtherNet/IP port. 02 hex: Clears the saved tag data link settings and resets the EtherNet/IP port.	Not supported	Supported

Class ID

Specify 01 hex.

Instance ID

Specify 00 or 01 hex.

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Read data	
				Data type	Value
01 hex	Revision	Revision of the object	Read	UINT	0001 hex
02 hex	Max Instance	The maximum instance number	Read	UINT	0001 hex

● Instance Attribute ID

The instance attribute ID specifies the attribute of the instance.

Attribute ID	Parameter name	Description	Attribute	Read data	
				Data type	Value
01 hex	Vendor ID	Vendor ID	Read	UINT	002F hex
02 hex	Device Type	Device type	Read	UINT	000C hex
03 hex	Product Code	Product code	Read	UINT	Refer to (1) Product Codes for Each Model, below.
04 hex	Revision	Device revision	Read	Struct	---
	Major Revision	Major revision	Read	USINT	Refer to (2) Major and Minor CIP Revisions, below.
	Minor Revision	Minor revision	Read	USINT	
05 hex	Status	Status of the EtherNet/IP port	Read	WORD	Refer to (3) Status Details of the Built-in EtherNet/IP Port, below.
06 hex	Serial Number	Serial number	Read	UDINT	Set value
07 hex	Product Name	Product name	Read	STRING	Set value

1. Product Codes for Each Model

Model	Product Code
NX701-□□□□	067D hex
NX502-1300	0BF5 hex
NX502-1400	0BF6 hex
NX502-1500	0BF7 hex
NX-EIP201	0BF4 hex
NX102-1200	0BBB hex
NX102-1100	0BBA hex
NX102-1000	0BB9 hex

Model	Product Code
NX102-9000	0BB8 hex
NX102-1220	0BBF hex
NX102-1120	0BBE hex
NX102-1020	0BBD hex
NX102-9020	0BBC hex
NX1P2-□□□□	068B hex
NJ501-13□□	0665 hex
NJ501-14□□	0666 hex
NJ501-15□□	0667 hex
NJ501-43□□	066E hex
NJ501-44□□	066F hex
NJ501-45□□	0670 hex
NJ501-5300	068C hex
NJ501-R300	069C hex
NJ501-R400	069D hex
NJ501-R500	069E hex
NJ501-R320	069F hex
NJ501-R420	06A0 hex
NJ501-R520	06A1 hex
NJ301-11□□	066B hex
NJ301-12□□	066C hex
NJ101-□□□□	0680 hex

2. Major and Minor CIP Revisions

Model	Unit version	CIP revisions	
		Major revision	Minor revision
All CPU Unit models	Unit version 1.00	01 hex	01 hex
	Unit version 1.01 or 1.02		03 hex
	Unit version 1.03 to 1.08	02 hex	01 hex
	Unit version 1.09		02 hex
	Unit version 1.10		03 hex
	Unit version 1.11 or 1.12		04 hex
	Unit version 1.13 to 1.20		05 hex
NJ Series	Unit version 1.21 to 1.23		06 hex
	Unit version 1.26		08 hex
	Unit version 1.27		09 hex
	Unit version 1.40 to 1.41		06 hex
	Unit version 1.46		08 hex
	Unit version 1.47		09 hex
NX Series	Unit version 1.21 to 1.22		06 hex
	Unit version 1.28		09 hex
	Unit version 1.30 to 1.43		06 hex
	Unit version 1.44		08 hex
	Unit version 1.60		0A hex
NX-series EtherNet/IP Unit	Unit version 1.00		0A hex

3. Status Details of the EtherNet/IP Port

Bit	Name	Description
0	Owned	Indicates when the EtherNet/IP port has an open connection as the target of a tag data link.
1	Reserved	Always FALSE.
2	Configured	Tag data link settings exist.
3	Reserved	Always FALSE.
4 to 7	Extended Device Status	Indicates the status of the EtherNet/IP port.[*1]
8	Minor Recoverable Fault	TRUE when any of the following errors occurs. • IP Router Table Setting Error • Tag Data Link Setting Error • Tag Data Link Timeout • Tag Data Link Connection Timeout • FTP Server Setting Error • SNMP Setting Error • Tag Name Resolution Error
9	Minor Unrecoverable Fault	TRUE when the following error occurs. • Identity Error
10	Major Recoverable Fault	TRUE when any of the following errors occurs. • IP Address Duplication Error • BOOTP Server Error • Basic Ethernet Setting Error • IP Address Setting Error
11	Major Unrecoverable Fault	TRUE when any of the following errors occurs. • Communications Controller Error • MAC Address Error
12 to 15	Reserved	Always FALSE.

*1. Bits 7 to 4 indicate the status of the EtherNet/IP port.

b7	b6	b5	b4	
0	1	0	1	A major fault occurred.
0	0	1	0	A timeout occurred in one or more target connections.
0	0	1	1	Indicates that there are no tag data link settings.
0	1	1	0	Indicates that one or more connections are performing communications normally.
0	1	1	1	Other than the above.

Request Paths (IOIs) to Specify Objects

When you specify an object, specify the request path (IOI) for each service code as given below.

Service code		Class ID	Instance ID	Attribute ID
01 hex	Get_Attribute_All	01 hex	• Specifying a service for a class : 00 hex • Specifying a service for an instance : Always 01 hex	Not required.
0E hex	Get_Attribute_Single			• Reading a class attribute : 01 or 02 hex • Reading an instance attribute : 01 to 07 hex
05 hex	Reset		Always 01 hex	Not required.

10-5-3 TCP/IP Interface Object (Class ID: F5 hex)

This object is used to read and write settings such as the IP address, subnet mask, and default gateway.

It is necessary to use the route path of the CIP communications instruction (the *RoutePath* input variable) to specify the port number (1 or 2) of the EtherNet/IP port to access.

Service Codes

Specify the service to execute with the service code.

Service code	Parameter name	Description	Supported services	
			Classes	Instances
01 hex	Get_Attribute_All	Reads the values of the attributes.	Supported	Not supported
0E hex	Get_Attribute_Single	Reads the value of the specified attribute.	Supported	Supported
10 hex	Set_Attribute_Single	Writes a value to the specified attribute. The EtherNet/IP port restarts automatically after the value is written to the attribute. When the next Set_Attribute_Single is executed before the restart process is completed, the general status "0C hex" (Object State Conflict) is returned.	Not supported	Supported

Class ID

Specify F5 hex.

Instance ID

Specify 00 or 01 hex.
00: Specify the class
01: EtherNet/IP port

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Read data	
				Data type	Value
01 hex	Revision	Revision of the object	Read	UINT	0001 hex: Unit version 1.01 or earlier 0002 hex: Unit version 1.02 to 1.09 0003 hex: Unit version 1.10 0004 hex: Unit version 1.11 or later
02 hex	Max Instance	The maximum instance number	Read	UINT	0001 hex
03 hex	Number of Instances	The number of object instances	Read	UINT	0001 hex

● Instance Attribute ID

The instance attribute ID specifies the attribute of the instance.

Attribute ID	Parameter name	Description	Attribute	Read/write data	
				Data type	Value
01 hex	Interface Configuration Status	Indicates the IP address setting status of the interface.	Read	DWORD	Bits 0 to 3: Interface Configuration Status: 0 = IP address is not set. (This includes when BOOTP is starting.) 1 = IP address is set. Bits 4 and 5: Reserved (always FALSE). Bit 6: AcdStatus[*1]: FALSE = IP address collisions have not been detected. TRUE = IP address collisions have been detected. Bits 7 to 31: Reserved (always FALSE).

Attribute ID	Parameter name	Description	Attribute	Read/write data	
				Data type	Value
02 hex	Configuration Capability	Indicates a Controller Configurations and Setup that can be set to the interface.	Read	DWORD	Bit 0: BOOTP Client: Always TRUE. Bit 1: DNS Client: Always TRUE. Bit 2: DHCP Client: Always FALSE. Bit 3: DHCP-DNS Update: Always FALSE. Bit 4: Configuration Settable: Always TRUE. Bit 5: Hardware Configurable: Always FALSE. Bit 6: Interface Configuration Change Requires Reset: Always FALSE. Bit 7: ACD Capable*1: Always TRUE. Bits 8 to 31: Reserved (always FALSE).
03 hex	Configuration Control	Sets the method used to set the IP address when the interface starts.	Read/Write	DWORD	Bit 0 to 3: IP Address Setting Method 0 = Setting the static IP address. 1 = Setting by BOOTP. Bit 4: DNS Enable/Disable Setting FALSE = DNS disabled. TRUE = DNS enabled. Bits 5 to 31: Reserved (always FALSE).
04 hex	Physical Link Object	The path to the link object in the physical layer.	Read	Struct	---
	Path size	The path size (WORD size).		UINT	0002 hex
	Path	The path to the link object in the physical layer (static).		EPATH	20 F6 24 01 hex
05 hex	Interface Configuration	The interface settings.	Read/Write	Struct	---
	IP Address	IP address.		UDINT	Set value
	Network Mask	Subnet mask.		UDINT	Set value
	Gateway Address	The default gateway.		UDINT	Set value
	Name Server	The primary name server.		UDINT	Set value
	Name Server2	The secondary name server.		UDINT	Set value
	Domain Name	The domain name.		STRING	Set value*2
06 hex	Host Name	The host name (reserved).	Read/Write	STRING	Set value*3

*1. The value is always FALSE for a CPU Unit with unit version 1.01 or earlier.

*2. The value is the size of domain name (2 bytes) + domain name (48 bytes max.).

*3. The value is the size of host name (2 bytes) + host name (64 bytes max.).

*4. The value is always TRUE for CPU Units that support the DHCP client. The value is always FALSE for unsupported CPU Units.

Request Paths (IOIs) to Specify Objects

When you specify an object, specify the request path (IOI) for each service code as given below.

Service code		Class ID	Instance ID	Attribute ID
01 hex	Get_Attribute_All	F5 hex	• Specifying a service for a class: 00 hex • Specifying a service for an instance: 01 hex	Not required.
0E hex	Get_Attribute_Single			• Reading a class attribute: 01 or 03 hex • Reading and writing an instance attribute: 01 to 06 hex
10 hex	Set_Attribute_Single			

10-5-4 Ethernet Link Object (Class ID: F6 hex)

This object is used to set and read Ethernet communications and read Ethernet communications status information.

It is necessary to use the route path of the CIP communications instruction (the *RoutePath* input variable) to specify the port number (1 or 2) of the EtherNet/IP port to access.

Service Codes

Specify the service to execute with the service code.

Service code	Parameter name	Description	Supported service range	
			Class	Instance
0E hex	Get_Attribute_Single	Reads the value of the specified attribute.	Supported	Supported
10 hex	Set_Attribute_Single	Writes a value to the specified attribute.	Supported	Supported
4C hex	Get_and_Clear	Specify Attribute4 or Attribute5 to reset the value of the attribute to 0.	Not supported	Supported

Class ID

Specify F6 hex.

Instance ID

Specify 00 or 01 hex.

00: Specify the class

01: EtherNet/IP port

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Read data	
				Data type	Value
01 hex	Revision	Revision of the object	Read	UINT	0002 hex: Unit version 1.11 or earlier 0004 hex: Unit version 1.12 or later
02 hex	Max Instance	The maximum instance number	Read	UINT	0001 hex
03 hex	Number of Instances	The number of object instances	Read	UINT	0001 hex

● Instance Attribute ID

The instance attribute ID specifies the attribute of the instance.

Attribute ID	Parameter name	Description	Attribute	Read/write data	
				Data type	Value
01 hex	Interface Speed	Gives the baud rate for the interface.	Read	UDINT	Reads the current value.
02 hex	Interface Flags	Gives the status of the interface.	Read	DWORD	Refer to (1) Interface Flag Details, below.
03 hex	Physical Address	Gives the MAC address of the interface.	Read	ARRAY [0...5] OF USINT	Reads the current value of the MAC address.

Attribute ID	Parameter name	Description	Attribute	Read/write data	
				Data type	Value
04 hex	Interface Counters	The number of packets sent/ received through the interface.	Read	Struct	---
	In Octets	The number of octets received through the interface. This includes unnecessary multicast packets and discarded packets counted by InDiscards.		UDINT	Reads the current value.
	In Unicast Packets	The number of unicast packets received through the interface. This does not include discarded packets counted by InDiscards.		UDINT	Reads the current value.
	In NonUnicast Packets	The number of packets besides unicast packets received through the interface. This includes unnecessary multicast packets, but does not include discarded packets counted by InDiscards.		UDINT	Reads the current value.
	In Discards	The number of discarded incoming packets received through the interface.		UDINT	Reads the current value.
	In Errors	The number of incoming packets that had errors. This is not included in InDiscards.		UDINT	Reads the current value.
	In Unknown Protos	The number of incoming packets that were of an unknown protocol.		UDINT	Reads the current value.
	Out Octets	The number of octets sent through the interface.		UDINT	Reads the current value.
	Out Unicast Packets	The number of unicast packets sent through the interface.		UDINT	Reads the current value.
	Out NonUnicast Packets	The number of packets besides unicast packets sent through the interface.		UDINT	Reads the current value.
	Out Discards	The number of discarded sent packets.		UDINT	Reads the current value.
	Out Errors	The number of sent packets that had errors.		UDINT	Reads the current value.

Attribute ID	Parameter name	Description	Attrib-ute	Read/write data	
				Data type	Value
05 hex	Media Counters	Media counters for the communications port.	Read	Struct	---
	Alignment Errors	Number of frames received that were not octets in length.		UDINT	Reads the current value.
	FCS Errors	Number of frames received that did not pass the FCS check.		UDINT	Reads the current value.
	Single Collisions	Number of frames sent successfully with only one collision.		UDINT	Reads the current value.
	Multiple Collisions	Number of frames sent successfully with two or more collisions.		UDINT	Reads the current value.
	SQE Test Errors	Number of times a SQE test error message was generated.		UDINT	Reads the current value.
	Deferred Transmissions	The number of frames for which the first attempt to send was delayed because the media was busy.		UDINT	Reads the current value.
	Late Collisions	The number of collisions detected in packets that were sent after 512 bit times.		UDINT	Reads the current value.
	Excessive Collisions	The number of frames that failed to be sent because of excessive collisions.		UDINT	Reads the current value.
	MAC Transmit Errors	The number of frames that failed to be sent due to an internal MAC sublayer transmission error.		UDINT	Reads the current value.
	Carrier Sense Errors	The number of times the carrier sense condition was lost or the number of times an assertion did not occur when an attempt was made to send the frame.		UDINT	Reads the current value.
	Frame Too Long	The number of frames received that exceeded the maximum allowed frame size.		UDINT	Reads the current value.
	MAC Receive Errors	The number of frames that could not be received through the interface due to an internal MAC sublayer reception error.		UDINT	Reads the current value.

Attribute ID	Parameter name	Description	Attribute	Read/write data	
				Data type	Value
06 hex	Interface Control	Control settings for the interface.	Read/ Write	Struct	---
	Control Bits	Auto Nego for Ethernet communications that specifies full duplex.		WORD	Refer to (2) Control Bit Details, below.
	Forced Interface Speed	Gives the set value of the Ethernet baud rate.		UINT	Reads the set value.
0C hex [*1]	HC Interface Counters	The number of packets sent/ received through the HC interface.	Read	Struct	---
	HCInOctets	The number of octets received through the interface. This counter is the 64-bit edition of In Octets.		ULINT	Reads the current value.
	HCInUnicastPkts	The number of unicast packets received through the interface. This counter is the 64-bit edition of In Ucast Packets.		ULINT	Reads the current value.
	HCInMulticastPkts	The number of multicast packets received through the interface.		ULINT	Reads the current value.
	HCInBroadcastPkts	The number of broadcast packets received through the interface.		ULINT	Reads the current value.
	HCOutOctets	The number of octets sent through the interface.		ULINT	Reads the current value.
	HCOutUnicastPkts	The number of unicast packets sent through the interface. This counter is the 64-bit edition of Out Octets.		ULINT	Reads the current value.
	HCOutMulticastPkts	The number of multicast packets sent through the interface.		ULINT	Reads the current value.
	HCOutBroadcastPkts	The number of broadcast packets sent through the interface.		ULINT	Reads the current value.

Attribute ID	Parameter name	Description	Attribute	Read/write data	
				Data type	Value
0D hex[*1]	HC Media Counters	Media counters for the communications port.	Read	Struct	---
	HCStatsAlignmentErrors	The number of frames received that were not octets in length. This counter is the 64-bit edition of Alignment Errors.		ULINT	Reads the current value.
	HCStatsFCSErrors	The number of frames received that did not pass the FCS check. This counter is the 64-bit edition of FCS Errors.		ULINT	Reads the current value.
	HCStatsInternalMacTransmitErrors	The number of frames that failed to be sent due to an internal MAC sublayer transmission error. This counter is the 64-bit edition of MAC Transmit Errors.		ULINT	Reads the current value.
	HCStatsFrameTooLongs	The number of frames received that exceeded the maximum allowed frame size. This counter is the 64-bit edition of Frame Too Long.		ULINT	Reads the current value.
	HCStatsInternalMacReceiveErrors	The number of frames that could not be received through the interface due to an internal MAC sublayer reception error. This counter is the 64-bit edition of MAC Receive Errors.		ULINT	Reads the current value.
	HCStatsMacSymbolErrors	The number of frames that could not be received through the interface due to an internal MAC sublayer rsymbol error.		ULINT	Reads the current value.

[*1] A CPU Unit with unit version 1.13 or later is required to use this attribute.

1. Interface Flag Details

Bit	Name	Description
0	LinkStatus	FALSE: The link is down. TRUE: The link is up.
1	Half/FullDuplex	FALSE: Half duplex TRUE: Full duplex
2 to 4	Negotiation Status	00 hex: Auto-negotiation is in progress. 01 hex: Auto-negotiation and speed detection failed. 02 hex: Auto-negotiation failed, but speed detection succeeded. 03 hex: Speed and duplex mode negotiation succeeded. 04 hex: Auto-negotiation was not attempted.
5	Manual Setting Requires Speed	Always FALSE: Changes can be applied automatically.
6	Local Hardware Fault	Always FALSE

Bit	Name	Description
7 to 31	Reserved	Always FALSE

2. Control Bit Details

Bit	Name	Description
0	Auto-negotiate	FALSE: Auto-negotiation is disabled. TRUE: Auto-negotiation is enabled.
1	ForcedDuplex Mode	FALSE: Half duplex TRUE: Full duplex[*1]
2 to 16	Reserved	Always FALSE

*1. When auto-negotiation is enabled (bit 0 is TRUE), this should always be FALSE.

Request Paths (IOIs) to Specify Objects

When you specify an object, specify the request path (IOI) for each service code as given below.

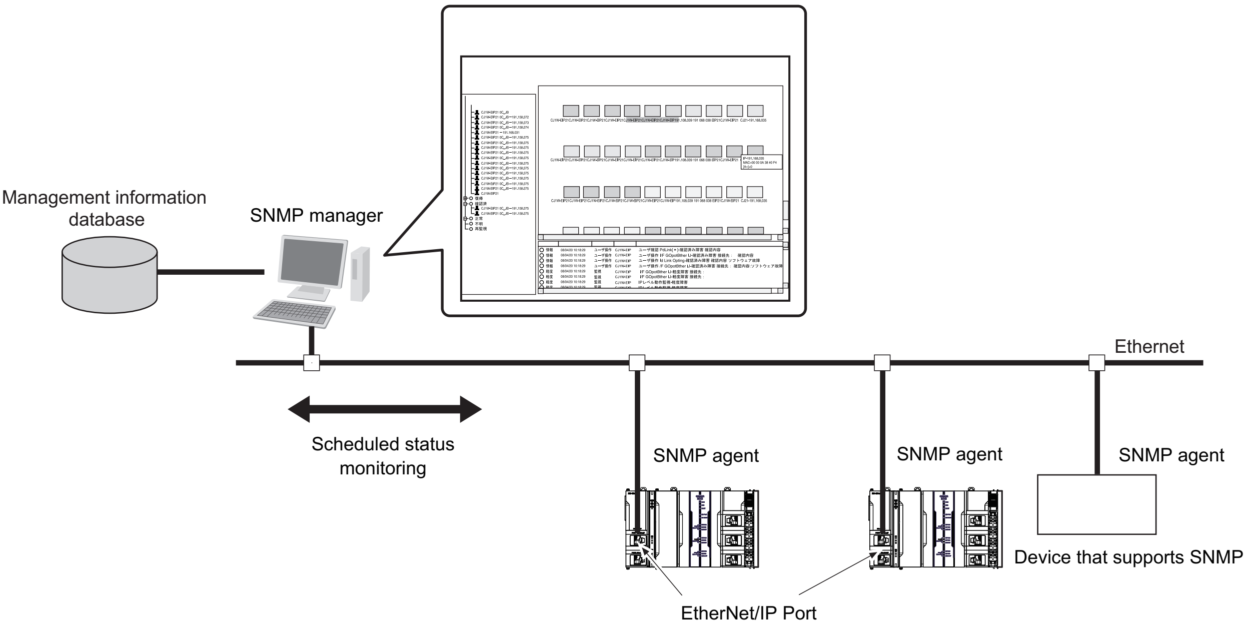
Service code		Class ID	Instance ID	Attribute ID
0E hex	Get_Attribute_Single	F6 hex	• Specifying a service for a class: 00 hex • Specifying a service for an instance: Always 01 hex	• Reading a class attribute: 01 to 03 hex • Reading and writing a instance attribute: 01 to 06 hex, 0C hex, and 0D hex
10 hex	Set_Attribute_Single			
4C hex	Get_and_Clear			Specify an attribute to clear the value to 0: 04 hex, 05 hex, 0C hex, 0D hex

11

SNMP Agent

11-1 SNMP Agent

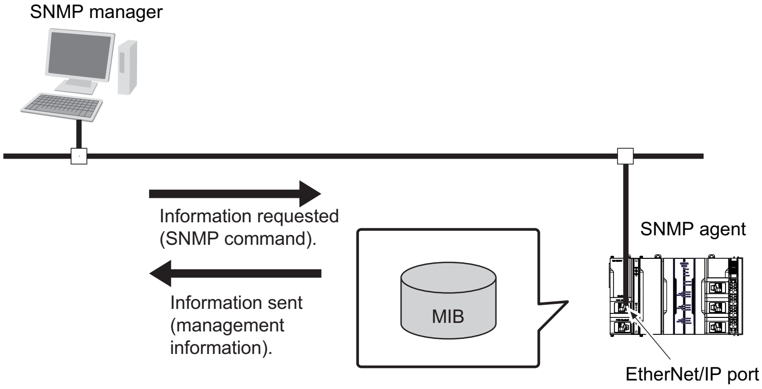
The SNMP (simple network management protocol) is a network management protocol.
You can use the SNMP to manage any network that consists of devices that support SNMP.
The server that manages the network is called the SNMP manager. The managed network devices are called SNMP agents.


Management information database
SNMP manager
Ethernet
Scheduled status monitoring
SNMP agent
SNMP agent
SNMP agent
Device that supports SNMP
EtherNet/IP Port

11-1-1 Overview

SNMP Agent

The EtherNet/IP port has its own management information called the MIB (management information base). This information can be provided to the SNMP manager.
The SNMP manager is software that gathers and processes information about devices on the SNMP network and provides that information to the network administrator.
You can use the SNMP manager to monitor the EtherNet/IP port.

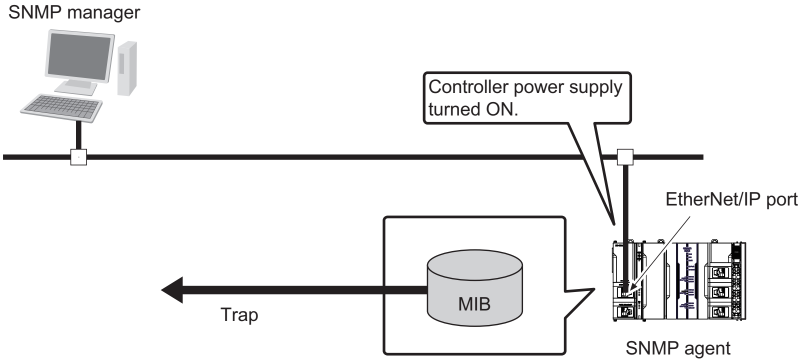

SNMP manager
Information requested (SNMP command).
Information sent (management information).
MIB
SNMP agent
EtherNet/IP port

The SNMP manager has a SNMP command to request MIB information.

The EtherNet/IP port SNMP agent function supports SNMPv1 (RFC1157) and SNMPv2C (RFC1901). Use the SNMPv1 or SNMPv2C protocol to manage the EtherNet/IP port with the SNMP manager. You can also use both the SNMPv1 and SNMPv2C protocols together at the same time.

SNMP Traps

When a failure or some other specific problem occurs, a status report called a trap is sent.
This enables monitoring changes in status even if the SNMP manager does not monitor the EtherNet/IP port periodically.
However, traps use UDP. Therefore, you cannot check to see if the SNMP manager receives traps from the EtherNet/IP port.
Thus, depending on the network status, some traps may not reach the SNMP manager.

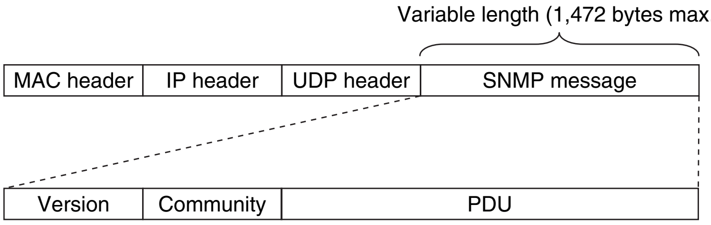


11-1-2 Specifications

Item	Specification
Protocol	SNMP
Agent	SNMPv1, SNMPv2C
MIB	MIB-II
Port No.	SNMP agent: 161 (UDP) SNMP trap: 162 (UDP) These can be changed in the EtherNet/IP Port Settings from the Sysmac Studio.
Timing of SNMP trap operation	Status reports are sent to the SNMP manager at the following times. • When the Controller is turned ON • When links are established • When an SNMP agent fails to be authorized
Supported MIB commands	GetRequest/GetNextRequest

11-1-3 SNMP Messages

The structure of SNMP messages is as follows:



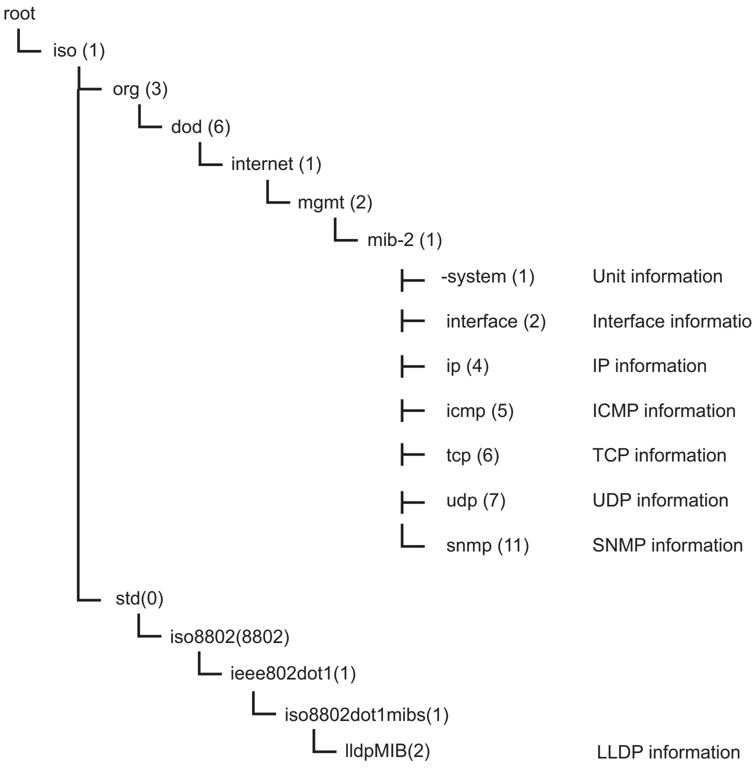
Item	Set value
Version	This value gives the SNMP version. SNMPv1: 0 SNMPv2C: 1
Community	Community name for verification
PDU	This depends on the PDU type.

11-1-4 MIB Specifications

This section describes the specifications of the MIB that is supported by the EtherNet/IP port.

MIB System Diagram

The EtherNet/IP port MIB consists of the following tree structure.



MIB Groups

MIB group			Stored information
Standard MIB	system group		The MIB for information related to the device.
	interfaces group		The MIB for information related to the interface.
	ip group	ip	The MIB for IP information.
		ipAddrTable	The MIB for addressing table information related to IP addresses.
		ipRouteTable	The MIB for information related to IP routing tables.
		ipNetToMediaTable	The MIB for information related to IP address conversion tables.
		ipForward	The MIB for information related to IP forwarding tables.
	icmp group		The MIB for ICMP information.
	tcp group	tcp	The MIB for TCP information.
	udp group	udp	The MIB for UDP information.
	snmp group	snmp	The MIB for SNMP information.
	lldp group		The MIB for LLDP information.

Detailed Descriptions of MIB Objects

System Group

Subtree name	Standard [(identifier) attribute]	Support	Implementation specifications
sysDescr	[(1) RO] Device information (including hardware, OS, software names, and versions) ASCII characters only.	Supported	"OMRON Corporation" + CPU Unit model + CPU Unit version • CPU Unit model (example): NJ501-1200 • CPU Unit version (example): Version 1.0
sysObjectID	[(2) RO] Vendor OID. Tells where this device information was assigned in the private MIB.	Supported	1.3.6.1.4.1.16838.1.1025.5
sysUpTime	[(3) RO] The time elapsed since the system was started (unit: 1/100 s).	Supported	According to the standard.
sysContact	[(4) RW] How to contact the administrator and information on the administrator.	Supported	Set by the user.
sysName	[(5) RW] The name for management. Sets the full domain name of the device.	Supported	Host Name

Subtree name	Standard [(identifier) attribute]	Support	Implementation specifications
sysLocation	[(6) RW] The physical location of the device.	Supported	Set by the user.
sysServices	[(7) RO] The value of the provided service.	Supported	64

● Interfaces Group

Subtree name	Standard [(identifier) attribute]	Support	Implementation specifications
ifNumber	[(1) RO] The number of network interfaces.	Supported	4
ifTable	[(2) NA] Interface entity table	---	---
ifEntry	[(1) NA] Row data for interface information The index is *ifIndex*.	---	---
ifIndex	[(1) RO] A number used to identify the interface.	Supported	1 to 4
ifDescr	[(2) RO] Information related to the interface (includes manufacturer name, product name, and hardware interface version).	Supported	• 10/100/1000M Gigabit Ethernet Port • Internal Network Port
ifType	[(3) RO] The type of interface classified according to the physical/link layer protocol directly under the network layer of the protocol stack.	Supported	ethernet-csmacd (6)
ifMtu	[(4) RO] MTU value The maximum size (in octets) of datagrams that can be sent and received through this interface.	Supported	1500
ifSpeed	[(5) RO] Estimated bandwidth If a stable, accurate value cannot be obtained for the bandwidth, a nominal value is set instead.	Supported	10000000/ 100000000/ 1000000000
ifPhysAddress	[(6) RO] MAC address The physical address under the network layer of the interface.	Supported	The MAC address of the EtherNet/IP port
ifAdminStatus	[(7) RW] The preferred status of the interface. You cannot send normal packets in the testing state. up (1) down (2) testing (3)	Supported	According to the standard.

Subtree name	Standard [(identifier) attribute]	Support	Implementation specifications
ifOperStatus	[(8) RO] The current status of the interface. You cannot send normal packets in the testing state. up (1) down (2) testing (3)	Supported	According to the standard.
ifLastChange	[(9) RO] The sysUpTime (in 0.01 seconds) at the last change in ifOperStatus for this interface.	Supported	According to the standard.
ifInOctets	[(10) RO] The number of octets received through this interface. This includes framing characters.	Supported	According to the standard.
ifInUcastPkts	[(11) RO] The number of unicast packets reported to a higher level protocol.	Supported	According to the standard.
ifInNUcastPkts	[(12) RO] The number of non-unicast packets (broadcast or multicast packets) reported to a higher level protocol.	Supported	According to the standard.
ifInDiscards	[(13) RO] The number of packets that had no errors but could not be passed to a higher level protocol (i.e., the number of packets received but discarded due to a buffer overflow).	Supported	According to the standard.
ifInErrors	[(14) RO] The number of packets discarded because they contained errors.	Supported	According to the standard.
ifInUnknownProtos	[(15) RO] The number of packets received, but discarded because they were of an illegal or unsupported protocol. For example, Ethernet packets did not have IP set for the field that identifies their higher level protocol.	Supported	According to the standard.
ifOutOctets	[(16) RO] The number of octets of packets sent through this interface. This includes framing characters.	Supported	According to the standard.
ifOutUcastPkts	[(17) RO] The number of unicast packets sent by higher level protocols. This includes discarded packets and unsent packets.	Supported	According to the standard.
ifOutNUcastPkts	[(18) RO] The number of non-unicast packets sent by higher level protocols. This includes discarded packets and unsent packets.	Supported	According to the standard.

Subtree name	Standard [(identifier) attribute]	Support	Implementation specifications
ifOutDiscards	[(19) RO] The number of packets that had no errors but were discarded in the sending process (due to a send buffer overflow, etc.).	Supported	According to the standard.
ifOutErrors	[(20) RO] The number of packets that could not be sent because of an error.	Supported	According to the standard.
ifOutQLen	[(21) RO] The size of the send packet queue (i.e., the number of packets).	Supported	Always 0.
ifSpecific	[(22) RO] The object ID that represents a reference to the media-specific MIB for the interface. For example, for Ethernet, set the object ID of the MIB that defines Ethernet. If there is no information, set { 0.0 }.	Supported	0.0

● Ip Group: Ip

Subtree name	Standard [(identifier) attribute]	Support	Implementation specifications
ipForwarding	[(1) RW] Indicates if the device operates as a gateway. IP gateways can transfer datagrams, but IP hosts can perform only source routing. Some nodes take only one of these values. Therefore, if you attempt to change this object from the SNMP Manager, a badValue error is returned. forwarding (1) not-forwarding (2)	Supported	forwarding (1), not-forwarding (2) Depends on the settings in **EtherNet/IP Port Settings** - **TCP/IP Settings** - **Port Forward** on the Sysmac Studio.
IpDefaultTTL	[(2) RW] The default value set for the IP header TTL if no TTL value was given by the transport layer protocol.	Supported	64
IpInReceives	[(3) RO] The number of all IP datagrams that reached the interface, including errors.	Supported	According to the standard.
IpInHdrErrors	[(4) RO] The number of received datagrams that were discarded because of an IP header error (checksum error, version number error, format error, TTL error, IP option error, etc.).	Supported	According to the standard.
IpInAddrErrors	[(5) RO] The number of packets that were discarded because the destination address in the IP header was not valid.	Supported	According to the standard.

Subtree name	Standard [(identifier) attribute]	Support	Implementation specifications
ipForwDatagrams	[(6) RO] The number of IP datagrams that were transferred to their final destination. If this node does not operate as an IP gateway, this is the number of datagrams that were successfully transferred through source routing.	Supported	According to the standard.
ipInUnknownProtos	[(7) RO] The number of IP datagrams that were received but discarded because they were of an unsupported or unrecognized protocol.	Supported	According to the standard.
ipInDiscards	[(8) RO] The number of IP datagrams that could have continued to be processed without any problems, but were discarded (for example, because of insufficient buffer space).	Supported	According to the standard.
ipInDelivers	[(9) RO] The number of datagrams delivered to an IP user protocol (any higher level protocol, including ICMP).	Supported	According to the standard.
ipOutRequests	[(10) RO] The number of times a send request was made for an IP datagram by a local IP user protocol (any higher level protocol, including ICMP). This counter does not include ipForwDatagrams.	Supported	According to the standard.
ipOutDiscards	[(11) RO] The number of IP datagrams that could have been sent without any problems, but were discarded (for example, because of insufficient buffer space).	Supported	According to the standard.
ipOutNoRoutes	[(12) RO] The number of IP datagrams that were discarded because there was no transmission path. This counter includes datagrams that attempted to be sent through ipForwDatagrams, but were discarded because they were set with no-route. This value indicates the number of datagrams that could not be transferred because the default gateway was down.	Supported	According to the standard.
ipReasmTimeout	[(13) RO] The maximum number of seconds to wait to receive all IP datagrams for reassembly if a fragmented IP datagram is received.	Supported	60 s
ipReasmReqds	[(14) RO] The number of IP datagrams received that require reassembly. There is a flag in the IP header that indicates if the datagram is fragmented. You can use that flag to identify fragments.	Supported	According to the standard.

Subtree name	Standard [(identifier) attribute]	Support	Implementation specifications
ipReasmOKs	[(15) RO] The number of IP datagrams received that were successfully reassembled.	Supported	According to the standard.
ipReasmFails	[(16) RO] The number of IP datagrams received that were not successfully reassembled.	Supported	According to the standard.
ipFragOKs	[(17) RO] The number of IP datagrams that were successfully fragmented.	Supported	According to the standard.
ipFragFails	[(18) RO] The number of IP datagrams that were not successfully fragmented. (For example, because the Don't Fragment flag was set for the IP datagram.)	Supported	According to the standard.
ipFragCreates	[(19) RO] The number of IP datagrams created as a result of fragmentation.	Supported	According to the standard.
ipAddrTable	[(20) NA] An address information table for IP addresses.	---	---
ipAddrEntry	[(1) NA] Row data of address information for IP addresses. The index is *ipAdEntAddr*.	---	---
ipAdEntAddr	[(1) RO] The IP address.	Supported	According to the standard.
ipAdEntIfIndex	[(2) RO] The index value of the interface that this entry applies to. This is the same value as ifIndex.	Supported	According to the standard.
ipAdEntNetMask	[(3) RO] The subnet mask for the IP address of this entry.	Supported	According to the standard.
ipAdEntBcastAddr	[(4) RO] The value of the least significant bit of the address when an IP broadcast is sent. An address represented by all 1 bits is used for broadcasting as an Internet standard. In that case, this value is always 1.	Supported	According to the standard.
ipAdEntReasmMaxSize	[(5) RO] The maximum IP packet size that can be reassembled from IP fragmented input IP datagrams received through the interface.	Supported	According to the standard.
ipRouteTable	[(21) NA] The IP routing table for this entity.	---	---

Subtree name	Standard [(identifier) attribute]	Support	Implementation specifications
ipRouteEntry	[(1) NA] Route information for a specific destination. The index is *ipRouteDest*.	---	---
ipRouteDest	[(1) RW] The destination IP address for this route. A value of 0.0.0.0 for this entry indicates the default route.	Supported	According to the standard.
ipRouteIfIndex	[(2) RW] The ID number of the interface required to send to the next destination host in this route. This ID number is the same number as ifIndex, which is used to identify the interface.	Supported	According to the standard.
ipRouteMetric1	[(3) RW] The primary routing metric for this route. This value is determined based on the protocol specified in ipRouteProto. Set to -1 if you do not want to use this metric (this is also the same for ipRouteMetric 2 through 4).	Supported	According to the standard.
ipRouteMetric2	[(4) RW] The alternative routing metric for this route.	Supported	According to the standard.
ipRouteMetric3	[(5) RW] The alternative routing metric for this route.	Supported	According to the standard.
ipRouteMetric4	[(6) RW] The alternative routing metric for this route.	Supported	According to the standard.
ipRouteNextHop	[(7) RW] The IP address of the next hop in this route (for routes connected by a broadcast or media, this is the agent address or address of that interface).	Supported	According to the standard.
ipRouteType	[(8) RW] The type of route. other (1): Not any of the following types. invalid (2): An invalid route. direct (3): A direct connection. indirect (4): An indirect connection (not connected to LOCAL).	Supported	According to the standard.

Subtree name	Standard [(identifier) attribute]	Support	Implementation specifications
ipRouteProto	[(9) RO] This is the routing mechanism used to determine routes. Some values correspond to gateway routing protocols, but be aware that the host may not support those protocols. other (1): Other than the following items. local (2): A route set on the local machine. netmgmt (3): A route set by network management. icmp (4): A route set by an ICMP redirect or some other ICMP function. egp (5): EGP The following are gateway protocols: ggp (6): GGP hello (7): HELLO rip (8): RIP is-is (9) es-is (10) ciscoIgrp (11) bbnSpfIgp (12) ospf (13): OSPF bgp (14)	Supported	According to the standard.
ipRouteAge	[(10) RW] The elapsed time since this route was updated (in seconds).	Supported	Always 0.
ipRouteMask	[(11) RW] The subnet mask value in relation to ipRouteDest. On systems that do not support a custom subnet mask value, this value is based on the address class of the ipRouteDest field. If ipRouteDest is 0.0.0.0, this value is also 0.0.0.0.	Supported	According to the standard.
ipRouteMetric5	[(12) RW] The alternative routing metric.	Supported	According to the standard.
ipRouteInfo	[(13) RO] The MIB object ID for the routing protocol used by this route. If not defined, set to {0.0}.	Supported	0.0
ipNetToMediaTable	[(22) NA] The IP address conversion table used to map IP addresses to physical addresses.	---	---

Subtree name	Standard [(identifier) attribute]	Support	Implementation specifications
ipNetToMediaEntry	[(1) NA] Row data for the conversion table. The indices are *ipNetToMediaIfIndex* and *ipNetToMediaNetAddress*.	---	---
ipNetToMediaIfIndex	[(1) RW] The interface ID number for this entry. The value of ifIndex is used for this value.	Supported	According to the standard.
ipNetToMediaPhysAddress	[(2) RW] The media-dependent physical address.	Supported	According to the standard.
ipNetToMediaNetAddress	[(3) RW] The IP address that corresponds to the media-dependent physical address.	Supported	According to the standard.
ipNetToMediaType	[(4) RW] The address conversion method. other (1): A method other than the following items. invalid (2): An invalid value. dynamic (3): Dynamic conversion. static (4): Static conversion.	Supported	According to the standard.
ipRoutingDiscards	[(23) RO] The number of routing entries that were valid but discarded. For example, if there was not enough buffer space because of other routing entries.	Supported	According to the standard.

● Ip Group: Icmp

Name	Standard [(identifier) attribute]	Support	Implementation specifications
icmpInMsgs	[(1) RO] The total number of received ICMP messages. This includes messages counted by icmpInErrors.	Supported	According to the standard.
icmpInErrors	[(2) RO] The number of received ICMP message errors. (Checksum errors, frame length errors, etc.)	Supported	According to the standard.
icmpInDestUnreachs	[(3) RO] The number of Destination Unreachable messages received.	Supported	According to the standard.
icmpInTimeExcds	[(4) RO] The number of Time Exceed messages received.	Supported	According to the standard.
icmpInParmProbs	[(5) RO] The number of Parameter Problem messages received.	Supported	According to the standard.
icmpInSrcQuenchs	[(6) RO] The number of Source Quench messages received.	Supported	According to the standard.
icmpInRedirects	[(7) RO] The number of Redirect messages received.	Supported	According to the standard.

Name	Standard [(identifier) attribute]	Support	Implementation specifications
icmpInEchos	[(8) RO] The number of Echo (request) messages received.	Supported	According to the standard.
icmpInEchoReps	[(9) RO] The number of Echo Reply messages received.	Supported	According to the standard.
icmpInTimestamps	[(10) RO] The number of Timestamp messages received.	Supported	According to the standard.
icmpInTimestampReps	[(11) RO] The number of Timestamp Reply messages received.	Supported	According to the standard.
icmpInAddrMasks	[(12) RO] The number of Address Mask Request messages received.	Supported	According to the standard.
icmpInAddrMaskReps	[(13) RO] The number of Address Mask Reply messages received.	Supported	According to the standard.
icmpOutMsgs	[(14) RO] The total number of ICMP messages sent. This includes messages counted by icmpOutErrors.	Supported	According to the standard.
icmpOutErrors	[(15) RO] The number of ICMP messages that could not be sent because of an error.	Supported	According to the standard.
icmpOutDestUnreachs	[(16) RO] The number of Destination Unreachable messages sent.	Supported	According to the standard.
icmpOutTimeExcds	[(17) RO] The number of Time Exceed messages sent.	Supported	According to the standard.
icmpOutParmProbs	[(18) RO] The number of Parameter Problem messages sent.	Supported	According to the standard.
icmpOutSrcQuenchs	[(19) RO] The number of Source Quench messages sent.	Supported	According to the standard.
icmpOutRedirects	[(20) RO] The number of Redirect messages sent.	Supported	According to the standard.
icmpOutEchos	[(21) RO] The number of Echo (request) messages sent.	Supported	According to the standard.
icmpOutEchoReps	[(22) RO] The number of Echo Reply messages sent.	Supported	According to the standard.
icmpOutTimestamps	[(23) RO] The number of Timestamp messages sent.	Supported	According to the standard.
icmpOutTimestampReps	[(24) RO] The number of Timestamp Reply messages sent.	Supported	According to the standard.
icmpOutAddrMasks	[(25) RO] The number of Address Mask Request messages sent.	Supported	According to the standard.

Name	Standard [(identifier) attribute]	Support	Implementation specifications
icmpOutAddrMaskReps	[(26) RO] The number of Address Mask Reply messages sent.	Supported	According to the standard.

● Ip Group: Tcp

Name	Standard [(identifier) attribute]	Support	Implementation specifications
tcpRtoAlgorithm	[(1) RO] The algorithm used to determine the timeout value for resending. other (1): Other than the following items. constant (2): A constant RTO value. rsre (3): The algorithm specified by the MIL-STD-1778 standard. vanj (4): The Van Jacobson algorithm.	Supported	According to the standard.
tcpRtoMin	[(2) RO] The minimum resend timeout value (in 0.01 s). This value depends on the algorithm used to determine the resend timeout value.	Supported	According to the standard.
tcpRtoMax	[(3) RO] The maximum resend timeout value (in 0.01 s). This value depends on the algorithm used to determine the resend timeout value.	Supported	According to the standard.
tcpMaxConn	[(4) RO] The total number of supported TCP connections. If the maximum number of connections is dynamic, this value is -1.	Supported	According to the standard.
tcpActiveOpens	[(5) RO] The number of times the TCP connection changed from the CLOSE state directly to the SYN-SENT state. (Active connection establishment.)	Supported	According to the standard.
tcpPassiveOpens	[(6) RO] The number of times the TCP connection changed from the LISTEN state directly to the SYN-RCVD state. (Passive connection establishment.)	Supported	According to the standard.
tcpAttemptFails	[(7) RO] The total number of times the TCP connection changed from the SYN-SENT or SYN-RCVD state directly to the CLOSE state and from the SYN-RCVD state directly to the LISTEN state.	Supported	According to the standard.
tcpEstabResets	[(8) RO] The number of times the TCP connection changed from the ESTABLISHED or the CLOSE-WAIT state directly to the CLOSE state.	Supported	According to the standard.

Name	Standard [(identifier) attribute]	Support	Implementation specifications
tcpCurrEstab	[(9) RO] The total number of TCP connections currently in the ESTABLISHED or the CLOSE-WAIT state.	Supported	According to the standard.
tcpInSegs	[(10) RO] The total number of received segments. This includes the number of error segments.	Supported	According to the standard.
tcpOutSegs	[(11) RO] The total number of sent segments. This includes the number of segments for the current connection, but does not include the number of segments for resent data only.	Supported	According to the standard.
tcpRetransSegs	[(12) RO] The total number of resent segments.	Supported	According to the standard.
tcpConnTable	[(13) NA] The information table specific to the TCP connection.	---	---
tcpConnEntry	[(1) NA] Entry information related to a specific TCP connection. This value is deleted if the connection changes to the CLOSE state. The indices are *tcpConnLocalAddress*, *tcpConnLocalPort*, *tcpConnRemAddress*, and *tcpConnRemPort*.	---	---
tcpConnState	[(1) RW] The status of the TCP connection. closed (1) listen (2) synSent (3) synReceived (4) established (5) finWait1 (6) finWait2 (7) closeWait (8) lastAck (9) closing (10) timeWait (11)	Supported	According to the standard.
tcpConnLocalAddress	[(2) RO] The local IP address of this TCP connection. A value of 0.0.0.0 is used for connections in the LISTEN state that accept connections from any IP interface related to the node.	Supported	According to the standard.
tcpConnLocalPort	[(3) RO] The local port number for this TCP connection.	Supported	According to the standard.
tcpConnRemAddress	[(4) RO] The remote IP address for this TCP connection.	Supported	According to the standard.
tcpConnRemPort	[(5) RO] The remote port number for this TCP connection.	Supported	According to the standard.

Name	Standard [(identifier) attribute]	Support	Implementation specifications
tcpInErrs	[(14) RO] The total number of error segments received (TCP checksum errors, etc.).	Supported	According to the standard.
tcpOutRsts	[(15) RO] The number of segments sent with the RST flag (the number of times the TCP connection was reset).	Supported	According to the standard.

● Ip Group: Udp

Name	Standard [(identifier) attribute]	Support	Implementation specifications
udpInDatagrams	[(1) RO] The total number of UDP datagrams (i.e., the number of packets) sent to the UDP user.	Supported	According to the standard.
udpNoPorts	[(2) RO] The number of UDP datagrams that were received but did not start an application at the destination port.	Supported	According to the standard.
udpInErrors	[(3) RO] The number of UDP datagrams that were not sent to a higher level protocol for a reason other than udpNoPorts.	Supported	According to the standard.
udpOutDatagrams	[(4) RO] The total number of sent UDP datagrams.	Supported	According to the standard.
udpTable	[(5) NA] The information table for the UDP listener.	---	---
udpEntry	[(1) NA] An entry related to a specific UDP listener. The indices are *udpLocalAddress* and *udpLocalPort*.	---	---
udpLocalAddress	[(1) RO] The local IP address of this UDP listener. A value of 0.0.0.0 is used for UDP listeners that accept datagrams from any IP interface related to the node.	Supported	According to the standard.
udpLocalPort	[(2) RO] The local port number for this UDP listener.	Supported	According to the standard.

● Ip Group: Snmp

Name	Standard [(identifier) attribute]	Support	Implementation specifications
snmpInPkts	[(1) RO] The total number of SNMP messages received.	Supported	According to the standard.
snmpOutPkts	[(2) RO] The total number of SNMP messages sent.	Supported	According to the standard.
snmpInBadVersions	[(3) RO] The total number of messages received of an unsupported version.	Supported	According to the standard.

Name	Standard [(identifier) attribute]	Support	Implementation specifications
snmpInBadCommunityNames	[(4) RO] The total number of messages received from an unregistered community.	Supported	According to the standard.
snmpInBadCommunityUses	[(5) RO] The total number of messages received that specify an operation that is not allowed by that community.	Supported	According to the standard.
snmpInASNParseErrs	[(6) RO] The total number of messages received that resulted in an ASN.1 error or BER error during decoding.	Supported	According to the standard.
snmpInTooBigs	[(8) RO] The total number of PDUs received with an error status of tooBig.	Supported	According to the standard.
snmpInNoSuchNames	[(9) RO] The total number of PDUs received with an error status of noSuchName.	Supported	According to the standard.
snmpInBadValues	[(10) RO] The total number of PDUs received with an error status of badValue.	Supported	According to the standard.
snmpInReadOnlys	[(11) RO] The total number of PDUs received with an error status of readOnly.	Supported	According to the standard.
snmpInGenErrs	[(12) RO] The total number of PDUs received with an error status of genErr.	Supported	According to the standard.
snmpInTotalReqVars	[(13) RO] The total number of MIB objects read normally after receiving GetRequest or GetNextRequest.	Supported	According to the standard.
snmpInTotalSetVars	[(14) RO] The total number of MIB objects updated normally after receiving SetRequest.	Supported	According to the standard.
snmpInGetRequests	[(15) RO] The total number of GetRequest PDUs received.	Supported	According to the standard.
snmpInGetNexts	[(16) RO] The total number of GetNextRequest PDUs received.	Supported	According to the standard.
snmpInSetRequests	[(17) RO] The total number of SetRequest PDUs received.	Supported	According to the standard.
snmpInGetResponses	[(18) RO] The total number of GetResponse PDUs received.	Supported	According to the standard.
snmpInTraps	[(19) RO] The total number of trap PDUs received.	Supported	According to the standard.
snmpOutTooBigs	[(20) RO] The total number of PDUs sent with an error status of tooBig.	Supported	According to the standard.

Name	Standard [(identifier) attribute]	Support	Implementation specifications
snmpOutNoSuchNames	[(21) RO] The total number of PDUs sent with an error status of noSuchName.	Supported	According to the standard.
snmpOutBadValues	[(22) RO] The total number of PDUs sent with an error status of badValue.	Supported	According to the standard.
snmpOutGenErrs	[(24) RO] The total number of PDUs sent with an error status of genErr.	Supported	According to the standard.
snmpOutGetRequests	[(25) RO] The total number of GetRequest PDUs sent.	Supported	According to the standard.
snmpOutGetNexts	[(26) RO] The total number of GetNextRequest PDUs sent.	Supported	According to the standard.
snmpOutSetRequests	[(27) RO] The total number of SetRequest PDUs sent.	Supported	According to the standard.
snmpOutGetResponses	[(28) RO] The total number of GetResponse PDUs sent.	Supported	According to the standard.
snmpOutTraps	[(29) RO] The total number of trap PDUs sent.	Supported	According to the standard.
snmpEnableAuthenTraps	[(30) RW] Determines if the agent generates verification failed traps. enabled (1) disabled (2)	Supported	According to the standard.

● Lldp Group

Name		Standard [(identifier) attribute]	Support	Implementation specifications
lldpConfiguration		[(1) NA] The MIB for LLDP configuration.	---	---
	lldpMessageTxInterval	[(1) RW] The LLDP frame transmission interval. Default value: 30 (seconds)	Supported	Variable value depending on setting: 5 to 32,768
	lldpMessageTxHoldMultiplier	[(2) RW] The value to determine TTL of the LLDP frame, this is placed in the LLDP frame header. TTL (seconds) = lldpMessageTxHoldMultipler × lldpMessageTxInterval However, the maximum value of TTL shall be 65,535 seconds. Default value: 4	Supported	Variable value depending on setting: 1 to 100
	lldpReinitDelay	[(3) RW] The time until re-initialization process is attempted when lldpPortConfigAdminStatus becomes “disabled”. Default value: 2 (seconds)	Supported	Always 2.

Name	Standard [(identifier) attribute]	Support	Implementation specifications
lldpTxDelay	[(4) RW] The interval between successive LLDP frame transmissions. Default value: 2 (seconds)	Supported	Always 2.
lldpNotificationInterval	[(5) RW] Indicates the transmission interval at which SNMP notifications are sent due to information updates from the remote system. Only one SNMP notification is sent even if multiple remote system information updates occur within the transmission interval. Default value: 30 (seconds)	Supported	Always 0.
lldpStatistics	[(2) NA] The MIB for LLDP statistics information.	---	---
lldpStatsRemTablesLastChangeTime	[(1) RO] Last time when the addition/change/deletion of neighbor information occurred.	Supported	According to the standard.
lldpStatsRemTablesInserts	[(2) RO] Counts up when neighbor information increased.	Supported	According to the standard.
lldpStatsRemTablesDeletes	[(3) RO] Counts up when neighbor information is deleted.	Supported	According to the standard.
lldpStatsRemTablesDrops	[(4) RO] Counts up when neighbor information cannot be added due to lack of resources.	Supported	According to the standard.
lldpStatsRemTablesAgeouts	[(5) RO] Counts up when the retention time expired and the neighbor information became invalid.	Supported	According to the standard.
lldpStatsTxPortTable	[(6) NA] The table containing transmission frame statistics information for individual LLDP transmission ports.	---	---
lldpStatsTxPortEntry	[(1) NA] The table entry of transmission frame statistics information for individual LLDP transmission ports.	---	---
lldpStatsTxPortFramesTotal	[(2) RO] The number of LLDP frame transmissions on the LLDP transmission port.	Supported	According to the standard.
lldpStatsRxPortTable	[(7) NA] The table containing reception frame statistics information for individual LLDP reception ports.	---	---

Name	Standard [(identifier) attribute]	Support	Implementation specifications
lldpStatsRxPortEntry	[(1) NA] The table entry of reception frame statistics information for individual LLDP reception ports.	---	---
lldpStatsRxPortFramesDiscardedTotal	[(2) RO] The total number of discarded LLDP frames on the LLDP reception port.	Supported	According to the standard.
lldpStatsRxPortFramesErrors	[(3) RO] The number of invalid LLDP frames received on the LLDP reception port.	Supported	According to the standard.
lldpStatsRxPortFramesTotal	[(4) RO] The number of valid LLDP frames received on the LLDP reception port.	Supported	According to the standard.
lldpStatsRxPortTLVsDiscardedTotal	[(5) RO] The total number of discarded TLVs on the LLDP reception port.	Supported	According to the standard.
lldpStatsRxPortTLVsUnrecognizedTotal	[(6) RO] The number of TLVs received in the previous version on the LLDP reception port.	Supported	According to the standard.
lldpStatsRxPortAgeoutsTotal	[(7) RO] Counts up when the retention time expired and the neighbor information became invalid on the LLDP reception port.	Supported	According to the standard.
lldpLocalSystemData	[(3) NA] The MIB for information regarding the LLDP local system.	---	---
lldpLocChassisIdSubtype	[(1) RO] The chassis type for the local system.	Supported	macAddress(4)
lldpLocChassisId	[(2) RO] The identifier of the chassis component for the local system.	Supported	Port 1 macAddress
lldpLocSysName	[(3) RO] The system name for the local system.	Supported	Outputs local host name. Same as sysName in the system group.
lldpLocSysDesc	[(4) RO] The system information for the local system.	Supported	"OMRON Corporation" + CPU Unit model + CPU Unit version • CPU Unit model (example): NX502-1300 • CPU Unit version (example): Version 1.0 Same as sysDescr in the system group.

Name	Standard [(identifier) attribute]	Support	Implementation specifications
lldpLocSysCapSupported	[(5) RO] The bitmap representation of the list of functions supported by the local system.	Supported	stationOnly(7)
lldpLocSysCapEnabled	[(6) RO] The bitmap representation of the list of functions running on the local system.	Supported	stationOnly(7)
lldpLocPortTable	[(7) NA] The table of LLDP ports on the local system.	---	---
lldpLocPortEntry	[(1) NA] The table entry of a LLDP port on the local system.	---	---
lldpLocPortIdSubtype	[(2) RO] The type indicating the port ID of the local system.	Supported	macAddress(3)
lldpLocPortId	[(3) RO] The port ID (string) for the local system port.	Supported	Port 1: Port 1 macAddress Port 2: Port 2 macAddress
lldpLocPortDesc	[(4) RO] The port information (string) for the local system port.	Supported	Port 1: 10/100/1000M Gigabit Ethernet Port 1 Port 2: 10/100/1000M Gigabit Ethernet Port 2 Same as ifDescr in the interfaces group.
lldpLocManAddrTable	[(1) NA] The table of management address on the local system.	---	---
lldpLocManAddrEntry	[(1) NA] The table entry of management address on the local system.	---	---
lldpLocManAddrLen	[(3) RO] The length of LLDP management address field transmitted from the local system.	Supported	Always 5.
lldpLocManAddrIfSubtype	[(4) RO] The type related to the numbering method for the local system interface.	Supported	ifIndex(2)
lldpLocManAddrIfId	[(5) RO] The interface number related to the local system management address.	Supported	Always 2.

Name			Standard [(identifier) attribute]	Support	Implementation specifications
		lldpLocManAddrOID	[(6) RO] The ID that identifies the hardware component or protocol type of the local system.	Supported	SNMPv2-SMI::zeroDotZero
lldpV2RemoteSystemsData			[(4) NA] The MIB for information regarding the remote system that is connected to the LLDP local system.	---	---
lldpRemTable			[(1) NA] The table of information from the remote system.	---	---
	lldpRemEntry		[(1) NA] The table entry of information from the remote system.	---	---
		lldpRemChassisIdSubtype	[(4) RO] The chassis type for the remote system.	Supported	According to the standard.
		lldpRemChassisId	[(5) RO] The chassis ID for the remote system.	Supported	According to the standard.
		lldpRemPortIdSubtype	[(6) RO] The type indicating the port ID for the remote system.	Supported	According to the standard.
		lldpRemPortId	[(7) RO] The port ID for the remote system.	Supported	According to the standard.
		lldpRemPortDesc	[(8) RO] The description (string) to identify the port of remote system.	Supported	According to the standard.
		lldpRemSysName	[(9) RO] The system name for the remote system.	Supported	According to the standard.
		lldpRemSysDesc	[(10) RO] The description (string) to identify the remote system.	Supported	According to the standard.
		lldpRemSysCapSupported	[(11) RO] The bitmap representation of the list of functions supported by the remote system.	Supported	According to the standard.
		lldpRemSysCapEnabled	[(12) RO] The bitmap representation of the list of functions running on the remote system.	Supported	According to the standard.
lldpRemManAddrTable			[(2) NA] The table of management address control on the remote system.	---	---
	lldpRemManAddrEntry		[(1) NA] The table entry of management address on the remote system.	---	---

Name				Standard [(identifier) attribute]	Support	Implementation specifications
			lldpRemManAddrIfSubtype	[(3) RO] The type related to the numbering method for the remote system interface.	Supported	According to the standard.
			lldpRemManAddrIfId	[(4) RO] The interface number related to the management address of the remote system.	Supported	According to the standard.
			lldpRemManAddrOID	[(5) RO] The ID indicating hardware configuration and protocols related to the management address of the remote system.	Supported	According to the standard.

11-2 Procedure to Use the SNMP Agent

11-2-1 Procedures

1. Make the basic settings.

   Refer to *2-2 EtherNet/IP Communications Procedures* on page 2-7 for the basic operation flow.
2. Select **Configurations and Setup** - **CPU/Expansion Racks** - **CPU Rack: X Bus** - **Unit No.: NX-EIP201 ()** - **EtherNet/IP Port Settings** on the Sysmac Studio.

   Make the following settings on the **SNMP Settings** Display or the **SNMP Trap Settings** Display.
   - SNMP Service
   - Recognition 1
   - Recognition 2
3. Select **Transfer to Controller** from the **Controller** Menu and click the **Yes** Button. The EtherNet/IP port settings are transferred to the Controller.

Precautions for Correct Use

If the **Use** Option is selected for Packet Filter of the EtherNet/IP port, allow packets from the SNMP manager. If they are not permitted, communication with SNMP manager is not possible. For the details on the settings, refer to *Packet Filter* on page 7-7.

11-2-2 Settings Required for the SNMP Agent

Make the following EtherNet/IP Port Settings from the Sysmac Studio to use the SNMP agent.

Tab page	Setting		Setting conditions	Reference
SNMP Settings	SNMP service		Required	*7-3* ***SNMP Settings*** *Display* on page 7-11
	Port No.		Specified by user. Required to change from the default value of 161.	
	Contact, location		Specified by user.	
	Send a recognition trap		Specified by user. Select this check box to send a recognition trap if there is access from an SNMP manager that is not specified (Access other than Recognition 1 and 2).	
	Recognition 1 and Recognition 2		Specified by user. Make these settings to permit access by only certain SNMP managers.	*Recognition 1* on page 7-12 *Recognition 2* on page 7-12
		IP address		
		Host name		
		Community name		

Tab page	Setting		Setting conditions	Reference
SNMP Trap Settings	SNMP trap		Required	*7-4* ***SNMP Trap Settings*** *Display* on page 7-13
	Port No.		Specified by user. Required to change from the default value of 162.	
	Trap 1 and trap 2			*Trap 1* on page 7-13 *Trap 2* on page 7-14
		IP address	Required Set an IP address or a host name as the SNMP trap destination.	
		Host name		
		Community name	Specified by user.	
		Version	Required Set the version of the SNMP manager.	

Additional Information

Make the settings in the **SNMP Settings** Display and the **SNMP Trap Settings** Display if the SNMP agent is used.
Refer to *7-3* ***SNMP Settings*** *Display* on page 7-11 for information on the **SNMP Settings** Display. Refer to *7-4* ***SNMP Trap Settings*** *Display* on page 7-13 for information on the **SNMP Trap Settings** Display.

12

Communications Performance and Communications Load

12-1 Communications System

12-1-1 Tag Data Link Communications Method

Requested Packet Interval (RPI) Settings

In tag data links for the EtherNet/IP port, the data transmission period is set for each connection as the RPI.

The target device sends data (i.e., output tags) based on the specified RPI, regardless of the number of nodes.

Also, the heartbeat frame is sent from the originator to the target device for each connection. The target device uses the heartbeat to check if any errors have occurred in the connection with the originator. The data transmission period of the heartbeat frame depends on the RPI settings.

Heartbeat Frame Transmission Period

- If packet interval is shorter than 100 ms, the heartbeat frame transmission period is 100 ms.
- If packet interval is equal to or larger than 100 ms, the heartbeat frame transmission period is the same as the RPI.

Example)

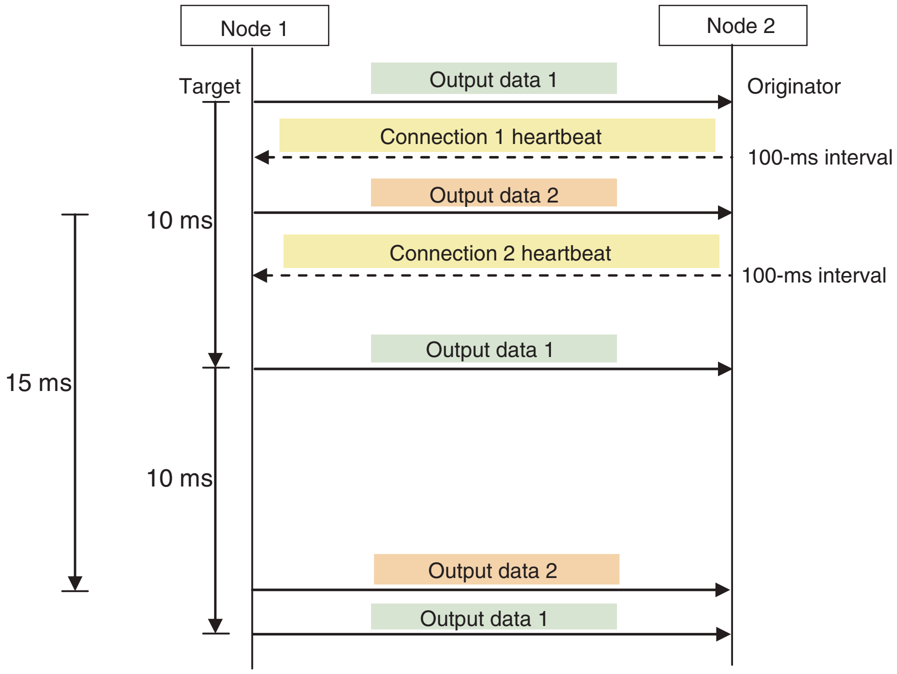
In this example, two tag data link connections are set for node 2 (the originator) and node 1 (the target).

The RPI for output data 1 is set to 10 ms.

The 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 (PPS)

The number of packets transferred each second is called the used bandwidth, or PPS (packets per second).
The PPS is calculated from the RPI and heartbeat for each connection as follows:

PPS for a connection (pps)
= (1,000/RPI (ms)) + (1,000/Heartbeat transmission period (ms))

Use the following equation to calculate the total number of packets transferred by each EtherNet/IP port (Unit) in 1 second.
Total PPS for the EtherNet/IP port = Total PPS of originator connections + Total PPS of target connections (*)

* Connections set as target connections must be added, too.

The following shows the maximum number of packets that each EtherNet/IP port can send and receive per second through tag data links (i.e., the allowed communications bandwidth per Unit). You need to consider these values when configuring connections.
- 40,000 pps

Precautions for Correct Use

When the Unit is performing tag data link communications where the allowable communications bandwidth per Unit is close to or greater than 30,000 pps, the following functions may not be used properly. In that case, use the built-in EtherNet/IP port on the CPU Unit or an EtherNet/IP port of a different NX-series EtherNet/IP Unit.

- Connecting the Sysmac Studio online from the EtherNet/IP port of the NX-series EtherNet/IP Unit
- Connecting the Network Configurator online from the EtherNet/IP port of the NX-series EtherNet/IP Unit
- Connecting the NA-series Programmable Terminal online from the EtherNet/IP port of the NX-series EtherNet/IP Unit
- Port forward via the NX-series EtherNet/IP Unit
- CIP message communications
- SNMP function

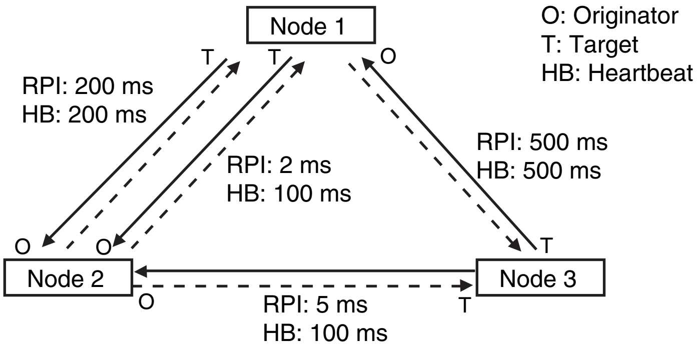
These functions of the NX-series EtherNet/IP Unit can be used via X Bus from the built-in EtherNet/IP port on the CPU Unit or an EtherNet/IP port of a different NX-series EtherNet/IP Unit.

Example)

Node 1 has an originator connection with the receive RPI of 500 ms, and two target connections with the send RPIs of 200 ms and 2 ms.

Node 2 has three originator connections with the receive RPIs of 200 ms, 2 ms, and 5 ms.

Node 3 has two target connections with the send RPIs of 5 ms and 1 ms.



The total PPS of each node is calculated as follows:

- Total PPS of the Unit Node 1
  = 1,000/200 ms + 1,000/2 ms+ 1,000/500 ms (for data)
  + 1,000/200 ms + 1,000/100 ms + 1,000/500 ms (for heartbeat)
  = 524 pps
- Total PPS of the Unit Node 2
  = 1,000/200 ms + 1,000/2 ms + 1,000/5 ms (for data)
  + 1,000/200 ms + 1,000/100 ms + 1,000/100 ms (for heartbeat)
  = 730 pps
- Total PPS of the Unit Node 3
  = 1,000/5 ms + 1,000/500 ms (for data)
  + 1,000/100 ms + 1,000/500 ms (for heartbeat)
  = 214 pps

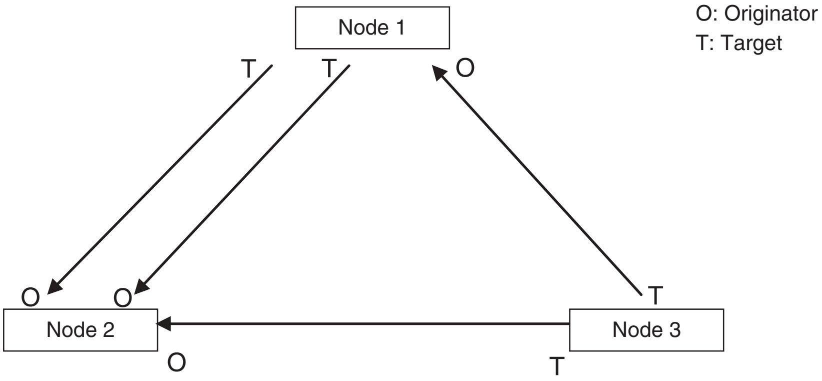
In this example, the total PPS of each Unit is below the maximum bandwidth allowed for the Unit, so data transmission can be successfully performed.

12-1-2 Calculating the Number of Connections

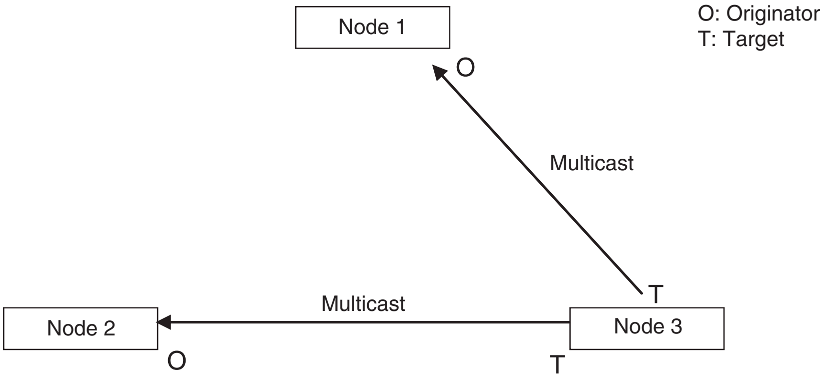
The maximum number of connections per EtherNet/IP port on a CPU Unit is as follows.

- 256

The maximum number of connections for a Unit should not be exceeded by the total number of originator connections, which the Unit opens, and target connections, which other nodes open to the Unit.
Example)
Node 1 has two target connections with Node 2, and opens one originator connection to Node 3. So, Node 1 has three connections in total.
Node 2 opens two originator connections to Node 1, and one originator connection to Node 3. So, Node 2 has three connections in total.
Node 3 has one target connection with Node 1, and one target connection with Node 2. So, Node 3 has two connections in total.
In either case, the connections can be successfully opened since the total number of connections is below the maximum number for an EtherNet/IP port, as shown above.



If multicast is specified for data transmission and the node sends out just one multicast packet to other nodes, it requires respective connections for them.
Example)
Node 3 sends out one multicast packet to Node 1 and Node 2. Node 3 has one target connection with Node 1, and one target connection with Node 2, requiring two connections in total.
You need to keep in mind that the number of required connections is the same, whether multicast or unitcast is specified for the communications.

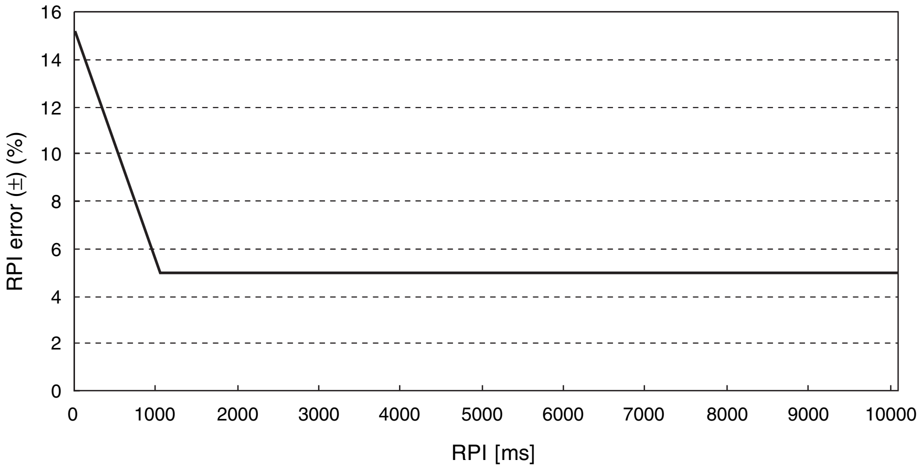


12-1-3 Packet Interval (RPI) Accuracy

A send processing delay occurs in an EtherNet/IP port when data packets are sent based on a packet interval (RPI).

This delay varies within the RPI error margin as shown below, so the send processing may be delayed for the maximum value for each RPI.

Packet interval (RPI)	RPI error margin (±) (%)
1.0 to 1,000 ms	15 − (RPI [ms]/100)
1,000 to 10,000 ms	5% of the RPI



12-2 Adjusting the Communications Load

In an Ethernet network using an Ethernet switch, the network bandwidth is not shared by all of the nodes; independent transmission paths are established between individual nodes through the Ethernet switch.

A dedicated communications buffer is established in the Ethernet switch 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 Ethernet switch 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 Ethernet switch.
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 setting ranges of the tag data link settings that can be made for an EtherNet/IP port.

Item	Specification	NX-series EtherNet/IP Unit
Network bandwidth	Physical Ethernet baud rate	1,000 Mbps
Allowable tag data link communications bandwidth	Maximum number of tag data link packets that can be processed in 1 second (pps: packets per second)	40,000 pps max. (40,000 pps total for two ports)[1]
Connection resources	Number of connections that can be established	256 max. (total of 512 with two ports)
Packet interval (RPI: Requested Packet Interval)	Refresh period for tag data	1.0 to 10,000 ms in 1.0-ms increments

[1] When the Unit is performing tag data link communications where the allowable communications bandwidth per Unit is close to or greater than 30,000 pps, the following functions may not be used properly. In that case, use the built-in EtherNet/IP port on the CPU Unit or an EtherNet/IP port of a different NX-series EtherNet/IP Unit.

- Connecting the Sysmac Studio online from the EtherNet/IP port of the NX-series EtherNet/IP Unit
- Connecting the Network Configurator online from the EtherNet/IP port of the NX-series EtherNet/IP Unit
- Connecting the NA-series Programmable Terminal online from the EtherNet/IP port of the NX-series EtherNet/IP Unit
- Port forward via the NX-series EtherNet/IP Unit
- CIP message communications
- SNMP function

These functions of the NX-series EtherNet/IP Unit can be used via X Bus from the built-in EtherNet/IP port on the CPU Unit or an EtherNet/IP port of a different NX-series EtherNet/IP Unit.

When the tag data link settings exceed the capabilities of the Ethernet switch to be used, increase the packet interval (RPI) value for adjustment.

Particularly when you configure the settings with an Ethernet switch that does not support multicast filtering, you need to consider that multicast packets will be sent to all the nodes on the network without setting the connections.

Additional Information

If you select **Multi-cast Connection** for the connection type in the connection settings on the Network Configurator, multicast packets are used. If the connection type is set to a **Point to Point Connection**, multicast packets are not used.

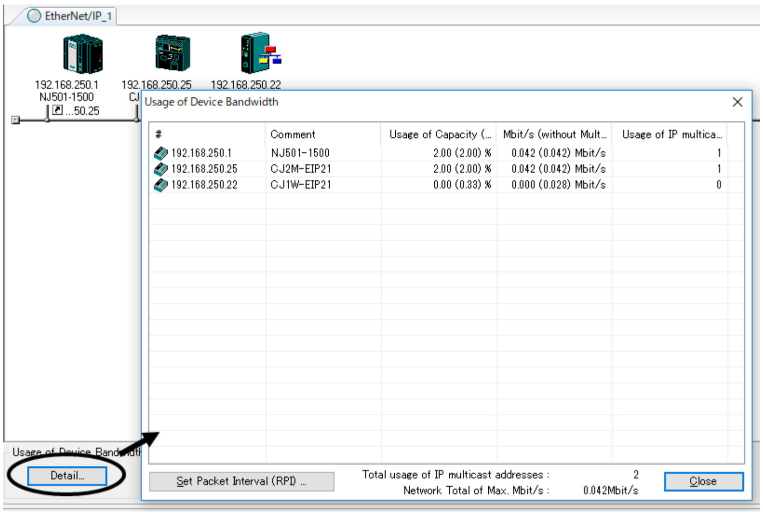
If required tag data link performance cannot be achieved with the Ethernet switch, re-evaluate the overall network configuration and take necessary measures such as selecting a different Ethernet switch or splitting the network.

The following sections show how to check the device bandwidth used by the tag data links in the designed network, and how to set appropriate values.

12-2-1 Checking Bandwidth Usage for Tag Data Links

The Network Configurator can display the bandwidth to be actually used for tag data links at each EtherNet/IP port, based on the connections set in the network configuration.

The device bandwidth used for 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.



#	Comment	Usage of Capacity (...	Mbit/s (without Mult...	Usage of IP multica...
192.168.250.1	NJ501-1500	2.00 (2.00) %	0.042 (0.042) Mbit/s	1
192.168.250.25	CJ2M-EIP21	2.00 (2.00) %	0.042 (0.042) Mbit/s	1
192.168.250.22	CJ1W-EIP21	0.00 (0.33) %	0.000 (0.028) Mbit/s	0

Total usage of IP multicast addresses : 2
Network Total of Max. Mbit/s : 0.042Mbit/s

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 (without Multicast Filter)	The usage rate of allowable tag data link bandwidth for the device is given. 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 (without Multicast Filter)	The network bandwidth used by the device for tag data link communications is given. 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 by the device for communications is given.
Total usage of IP multicast addresses	The number of multicast IP addresses used in the entire network is given. This value is used to estimate the number of multicast filters required for a switch.

Item	Description
Network Total of Max. Mbit/s	The total bandwidth used for tag data link communications in the entire network is given. Tag data links will not normally operate if the bandwidth allowed for the network is exceeded.

● Checking the Usage of Capacity and Network Bandwidth for Tag Data Links

The usage rate of allowable tag data link bandwidth for each EtherNet/IP port is given in the **Usage of Capacity (without Multicast Filter)** column, and the network bandwidth usage for tag data link communications is given in the **Mbit/s (without Multicast Filter)** column.
The usage rate and the network bandwidth usage of tag data link communications for which multicast filtering is not supported by the Ethernet switch are given in parentheses in each corresponding column. These values include bandwidth usage for multicast packets since they are sent to all the nodes without connection settings.
These values can be adjusted as described in *12-2-4 Changing the RPI* on page 12-11.

● Checking the Total Number of Multicast IP Addresses in the Network

When using an Ethernet switch that supports multicast filtering, there must be sufficient multicast filters for the network. Based on the setting of connections, the Network Configurator indicates the number of multicast IP addresses to be used in the entire network.
Make sure that the number of multicast IP addresses to be used in the entire network does not exceed the number of multicast filters supported by the Ethernet switch. If necessary, replace the Ethernet switch with another one with sufficient multicast filters, or adjust the usage rate and network bandwidth usage with the values given for an Ethernet switch without multicast filtering (i.e., the values in parentheses). These values can be adjusted as described in *12-2-4 Changing the RPI* on page 12-11.

● Checking the Total Maximum Network Bandwidth

The Network Configurator displays the total maximum bandwidth to be used for the entire network. This value indicates the maximum possible bandwidth for a transmission path which connects Ethernet switches in cascade. If this value exceeds the bandwidth for each cascade connection in the actual network (1,000 Mbps), the bandwidth for some transmission paths may be exceeded depending on the network wiring, and the tag data links may not operate normally.
If this occurs, calculate the bandwidth usage of each transmission path and make sure that the bandwidth for any cascade connection is not exceeded, or adjust the bandwidth to ensure that the value of **Network Total of Max. Mbit/s** does not exceed the bandwidth for any cascade connection. These values can be adjusted as described in *12-2-4 Changing the RPI* on page 12-11.

12-2-2 Tag Data Link Bandwidth Usage and RPI

The usage rate of allowable tag data link bandwidth as given in the **Usage of Capacity (without Multicast Filter)** column can be adjusted by changing the packet interval (RPI) setting.
If the RPI is set shorter, the **Usage of Capacity (without Multicast Filter)** will increase.
If the RPI is set longer, the **Usage of Capacity (without Multicast Filter)** will decrease.

The RPI can be set in one of the following ways.

- Setting the same PRI for all the connections

- Setting a PRI for connections of a particular device
- Setting a PRI for a particular connection

When the same RPI is set for all the connections, the **Usage of Capacity (without Multicast Filter)** will basically increase proportionally as the RPI is set shorter.
Example: If the **Usage of Capacity (without Multicast Filter)** is 40% with the PRI set to 50 ms for all the connections, the **Usage of Capacity (without Multicast Filter)** may increase to 80% when the RPI is changed to 25 ms for all the connections.

Precautions for Correct Use

If the **Usage of Capacity (without Multicast Filter)** is between 80% and 100%, some operation with the Network Configuator which may cause load on the network, such as monitoring, or message communications with some user application may temporarily cause excessive load on the network and result in timeouts. If timeouts occur, increase one or all of the RPI values and reduce the usage of capacity.

12-2-3 Adjusting Device Bandwidth Usage

This section provides methods for adjusting the device bandwidth usage for tag data links.

Precautions for Correct Use

The Ethernet switch should be able to support the maximum network bandwidth for each CPU Unit. The maximum network bandwidth is as follows.
- 1,000 Mbit/s

Ethernet Switches without Multicast Filtering

- Is the **Mbit/s (without Multicast Filter)** value for each node below the maximum network bandwidth?
  If any node exceeds the maximum network bandwidth, change the connection settings, such as the RPI.
- Is the value of **Usage of Capacity (without Multicast Filter)** for each node below 100%?
  If any node exceeds 100%, change the connections settings, such as the RPI.
- Is the value of **Network Total of Max. Mbit/s** below the maximum network bandwidth?
  If the value exceeds the maximum network bandwidth, the bandwidth for some transmission paths (e.g., an Ethernet switch or media converter) may be exceeded depending on the network wiring (e.g., cascade connection of Ethernet switches), and the tag data links may not operate normally. Check if the bandwidth of the transmission path in each cascade connection is not exceeded. If the bandwidth is exceeded, rewire the network or increase the bandwidth between Ethernet switches (e.g., increase to 1 Gbps). If these countermeasures are not possible, change the connection settings such as the RPI settings, and adjust the bandwidth to ensure that the value of **Network Total of Max. Mbit/s** does not exceed the bandwidth for any cascade connection..

Ethernet Switches with Multicast Filtering

- Is the **Mbit/s** value for each node below the maximum network bandwidth?

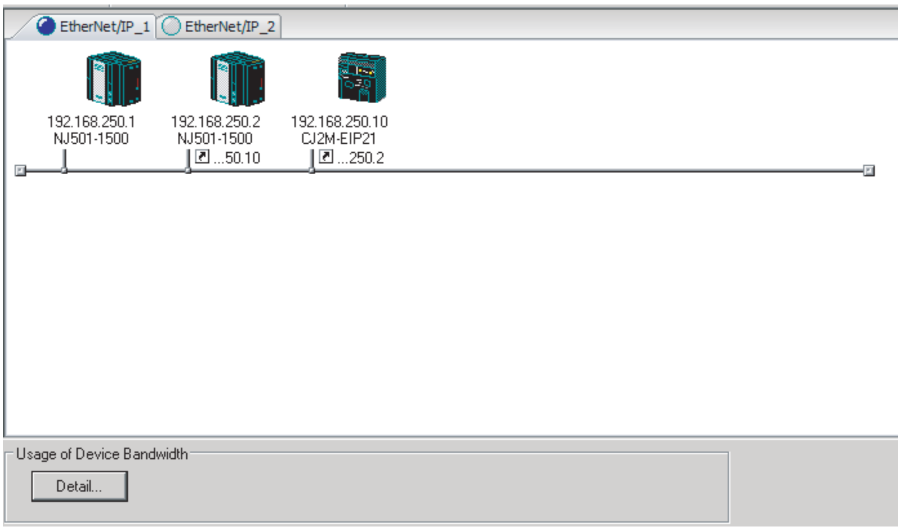
If any node exceeds the maximum network bandwidth, change the connection settings, such as the RPI.

- Is the **Usage of Capacity** value for each node below 100%?
  If any node exceeds the maximum network bandwidth, change the connection settings, such as the RPI.
- Is the **Network Total of Max. Mbit/s** value below the maximum network bandwidth?
  If the value exceeds the maximum network bandwidth, the bandwidth for some transmission paths (e.g., an Ethernet switch or media converter) may be exceeded due to the network wiring (e.g., cascade connection of Ethernet switches), and the tag data links may not operate normally. Check if the bandwidth of the transmission path in each cascade connection is not exceeded. If the bandwidth is exceeded, rewire the network or increase the bandwidth between Ethernet switches (e.g., to 1 Gbps). If these countermeasures are not possible, change the connection settings such as the RPI settings, and adjust the bandwidth to ensure that the value of **Network Total of Max. Mbit/s** does not exceed the bandwidth for any cascade connection.
- Is the **Mbit/s (without Multicast Filter)** value for each node below the maximum network bandwidth? Or, is the value of **Usage of Capacity (without Multicast Filter)** for each node below 100%?
  If any node exceeds either of them, check whether the multicast filtering on the relevant Ethernet switch is functioning correctly. If the number of multicast filters on the Ethernet switch is less than the number of **Total usage of IP multicast addresses**, the bandwidth for some transmission paths may be exceeded depending on the network wiring (e.g., cascade connection of Ethernet switches), and the tag data links may not operate normally. Calculate the number of multicast filters required for each Ethernet switch on the network, and check if the resulting number is below the number of multicast filters provided by the Ethernet switch. If the Ethernet switch does not have a sufficient number of multicast filters, replace it with another one which has sufficient multicast filters, or change the connection settings, such as the RPI settings.

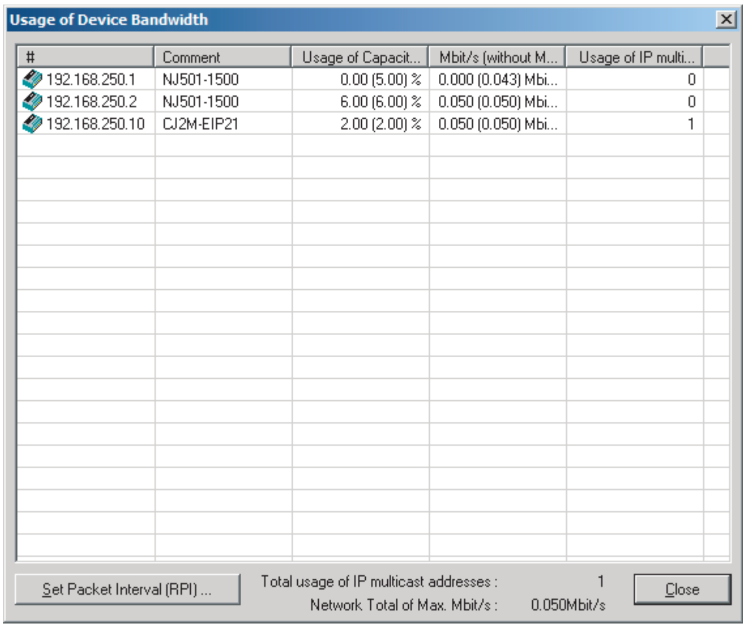
12-2-4 Changing the RPI

You can check **Usage of Capacity (without Multicast Filter)** values offline for the usage rate of allowable tag data link bandwidth if you follow the procedure provided in *12-2-1 Checking Bandwidth Usage for Tag Data Links* on page 12-8.
You can adjust **Usage of Capacity (without Multicast Filter)** values by changing packet interval (RPI) values.
If required communications performance cannot be achieved after the adjustment, re-evaluate the network configuration.

1. Make required settings in the Network Configuration Window on the Network Configurator.
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 is displayed.



#	Comment	Usage of Capacit...	Mbit/s (without M...	Usage of IP multi...
192.168.250.1	NJ501-1500	0.00 (5.00) %	0.000 (0.043) Mbi...	0
192.168.250.2	NJ501-1500	6.00 (6.00) %	0.050 (0.050) Mbi...	0
192.168.250.10	CJ2M-EIP21	2.00 (2.00) %	0.050 (0.050) Mbi...	1

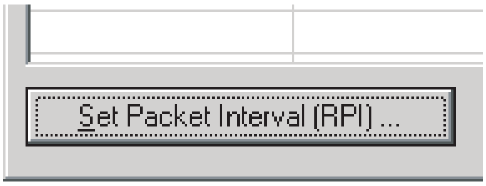
Total usage of IP multicast addresses : 1

Network Total of Max. Mbit/s : 0.050Mbit/s

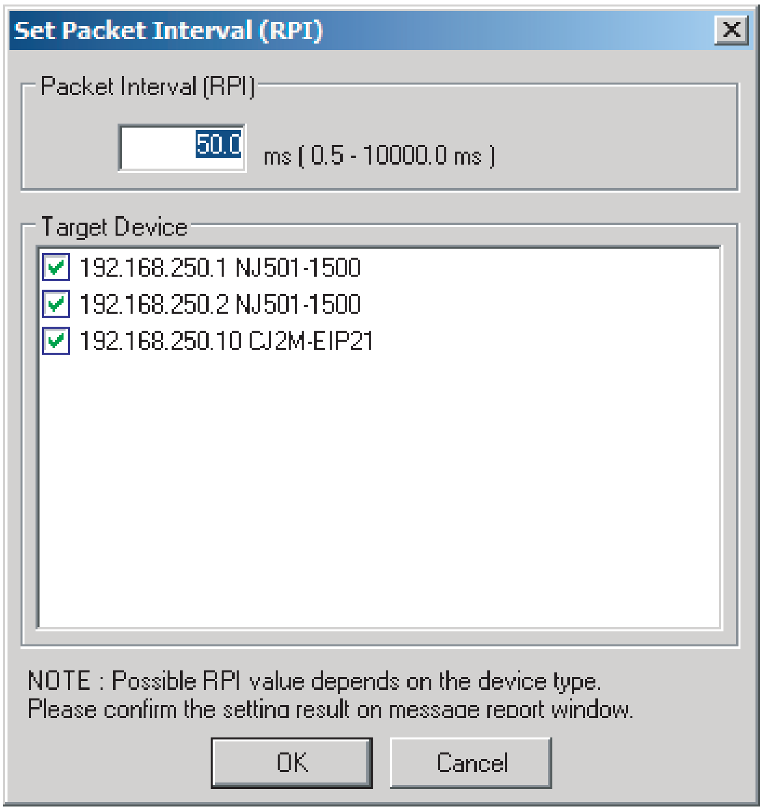
The **Usage of Capacity (without Multicast Filter)** column shows the usage rate of allowable tag data link bandwidth, and the **Mbit/s (without Multicast Filter)** column shows the network bandwidth usage.

3 You can adjust the **Usage of Capacity (without Multicast Filter)** value by changing the packet interval (RPI) for the relevant device.
There are three methods for changing the RPI as shown below.

- Method 1: Set the Same RPI for All the Connections
  You can adjust the **Usage of Capacity (without Multicast Filter)** value by changing the packet interval (RPI) values for all the connections at the same time.
  1) Click the **Set Packet Interval (RPI)** Button in the **Usage of Device Bandwidth** Dialog Box.



2) The **Set Packet Interval (RPI)** Dialog Box is displayed. Input a new RPI value, and click the **OK** Button.



50.0 ms (0.5 - 10000.0 ms)

☑ 192.168.250.1 NJ501-1500
☑ 192.168.250.2 NJ501-1500
☑ 192.168.250.10 CJ2M-EIP21

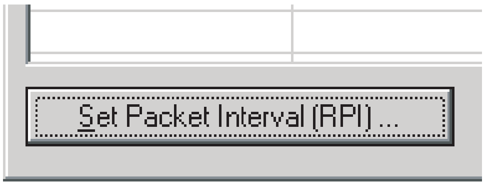
NOTE : Possible RPI value depends on the device type.
Please confirm the setting result on message report window.

- Method 2: Change the RPI for a Specific Device

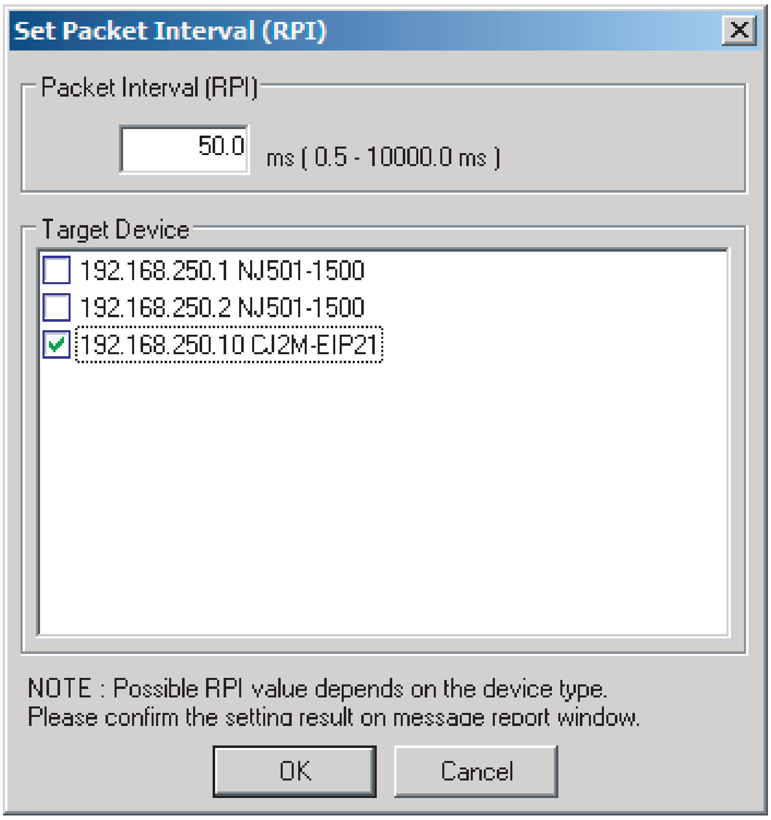
You can adjust the **Usage of Capacity (without Multicast Filter)** value by changing the RPI for all the connections of a specific device.

Note that the **Usage of Capacity (without Multicast Filter)** values for the target devices of the connections are also changed.

1) Click the **Set Packet Interval (RPI)** Button in the **Usage of Device Bandwidth** Dialog Box.



2) The **Set Packet Interval (RPI)** Dialog Box is displayed. In the **Target Device** Area, clear the check boxes for devices to which this RPI setting change is not applied.



50.0 ms (0.5 - 10000.0 ms)

☐ 192.168.250.1 NJ501-1500
☐ 192.168.250.2 NJ501-1500
☑ 192.168.250.10 CJ2M-EIP21

NOTE : Possible RPI value depends on the device type.
Please confirm the setting result on message report window.

3) Input a new RPI value, and click the **OK** Button.

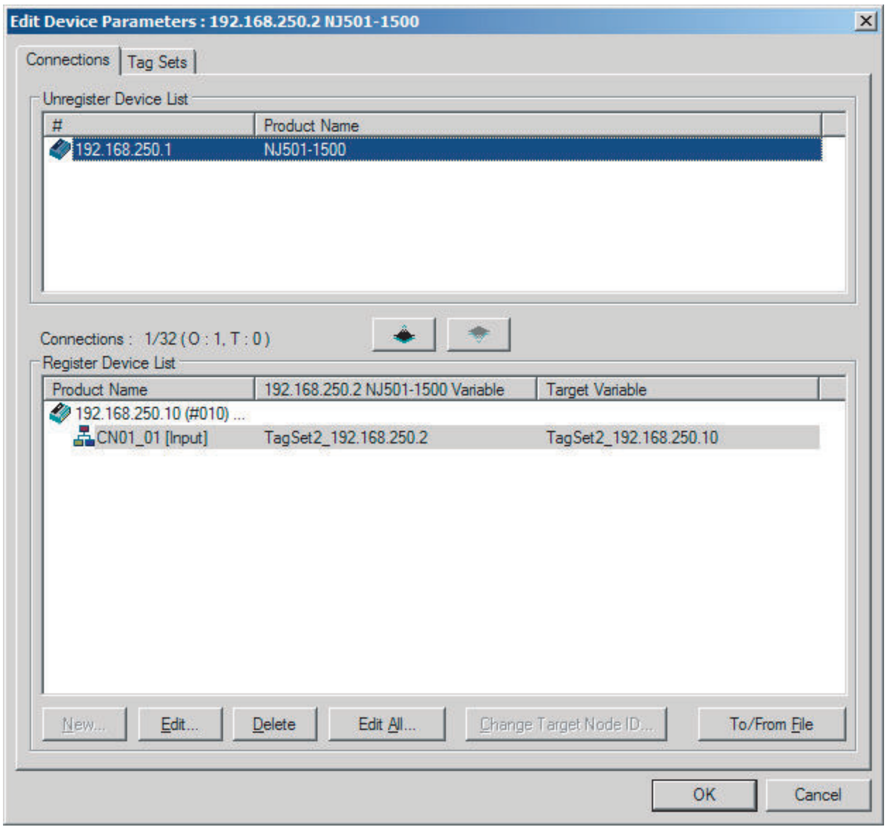
- Method 3: Change the RPI for a Specific Connection

You can adjust the **Usage of Capacity (without Multicast Filter)** value by changing the RPI for a specific connection.

Note that the **Usage of Capacity (without Multicast Filter)** value for the target device of the connection are also changed.

1) Click the **Close** Button in the **Usage of Device Bandwidth** Dialog Box.

2) Double-click the device that is set as the originator of the connection. The **Edit Device Parameters** Dialog Box is displayed.



Unregister Device List

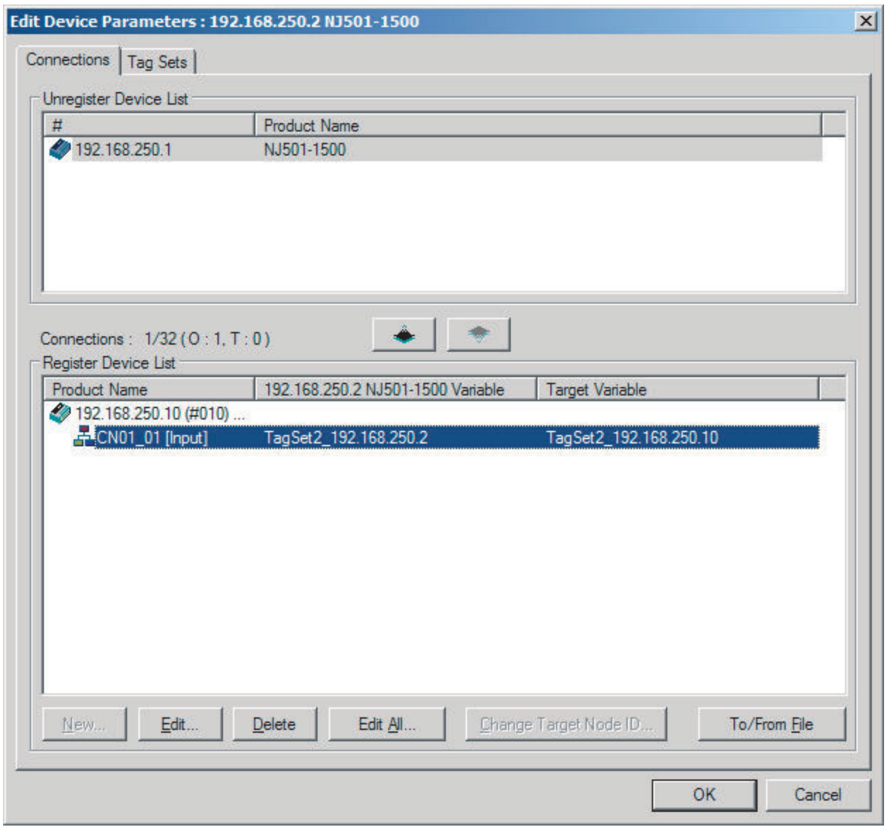
#	Product Name
192.168.250.1	NJ501-1500

Connections : 1/32 (O : 1, T : 0)

Register Device List

Product Name	192.168.250.2 NJ501-1500 Variable	Target Variable
192.168.250.10 (#010) ...		
CN01_01 [Input]	TagSet2_192.168.250.2	TagSet2_192.168.250.10

3) In the **Register Device List** Area, select the connection for which you want to change the RPI, and click the **Edit** Button.



Unregister Device List

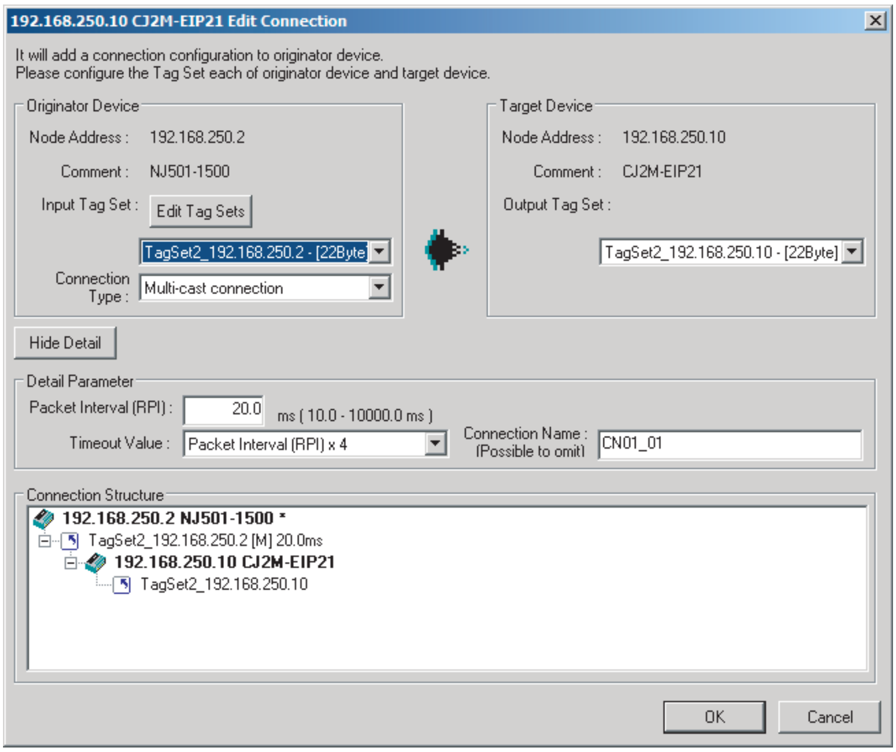
#	Product Name
192.168.250.1	NJ501-1500

Connections : 1/32 (O : 1, T : 0)

Register Device List

Product Name	192.168.250.2 NJ501-1500 Variable	Target Variable
192.168.250.10 (#010) ...		
CN01_01 [Input]	TagSet2_192.168.250.2	TagSet2_192.168.250.10

4) The Edit Connection Dialog Box for the device is displayed. Input a new packet interval (RPI) value, and click the **OK** Button.



192.168.250.10 CJ2M-EIP21 Edit Connection

It will add a connection configuration to originator device.
Please configure the Tag Set each of originator device and target device.

Originator Device
Node Address : 192.168.250.2
Comment : NJ501-1500
Input Tag Set : TagSet2_192.168.250.2 - [22Byte
Connection Type : Multi-cast connection

Target Device
Node Address : 192.168.250.10
Comment : CJ2M-EIP21
Output Tag Set : TagSet2_192.168.250.10 - [22Byte]

Detail Parameter
Packet Interval (RPI) : 20.0 ms (10.0 - 10000.0 ms)
Timeout Value : Packet Interval (RPI) x 4
Connection Name : (Possible to omit) CN01_01

Connection Structure
192.168.250.2 NJ501-1500 *
TagSet2_192.168.250.2 [M] 20.0ms
192.168.250.10 CJ2M-EIP21
TagSet2_192.168.250.10

4 If the bandwidth usage rate is not set as desired even after the above operation, re-evaluate the network configuration,considering the following points. (Refer to *12-2-3 Adjusting Device Bandwidth Usage* on page 12-10.)

- Reduce the number of nodes and connections
- Split the network

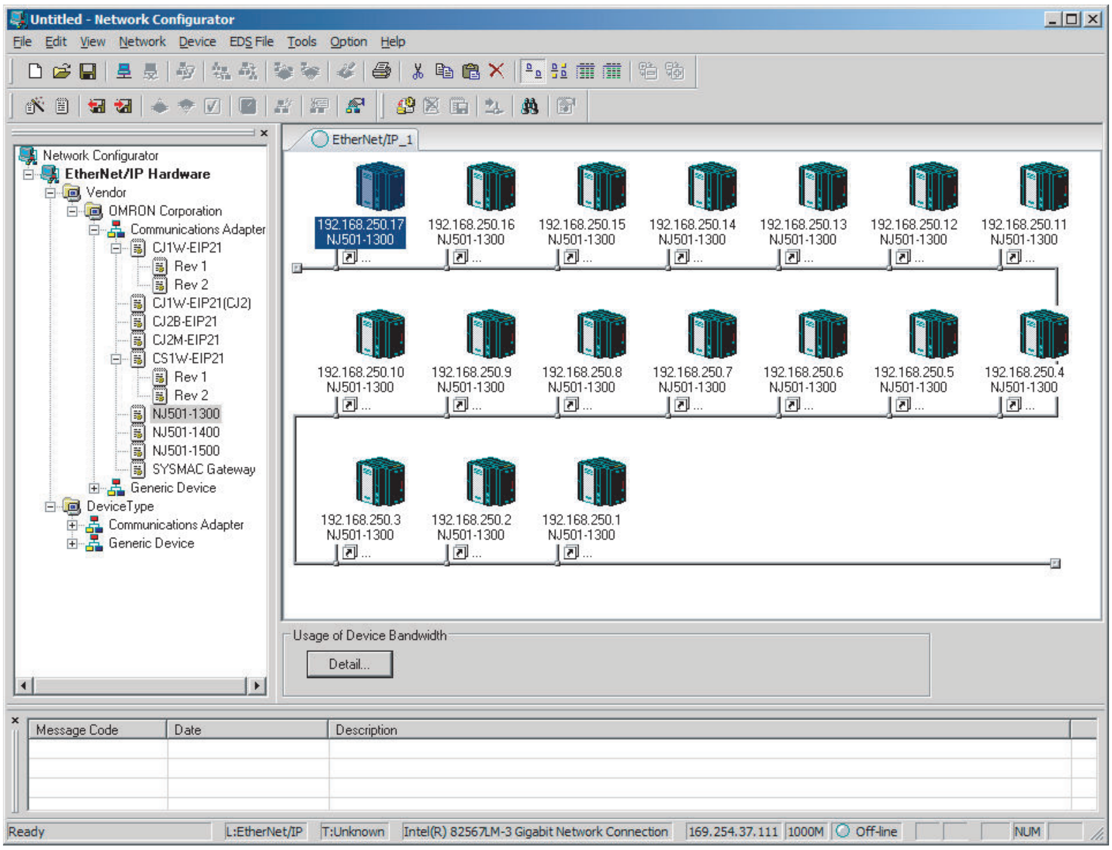
5 Check the bandwidth usage rate again.
After you change the connection settings, click the **Detail** Button in the **Usage of Device Bandwidth** Area at the bottom of the Network Configuration Window to check the bandwidth usage as described in *12-2-1 Checking Bandwidth Usage for Tag Data Links* on page 12-8.
It is important to check the bandwidth usage particularly after you change the RPI values for individual connections, instead of setting the same RPI for all the connections.

6 Run user tests to verify that there are no problems with the new values.

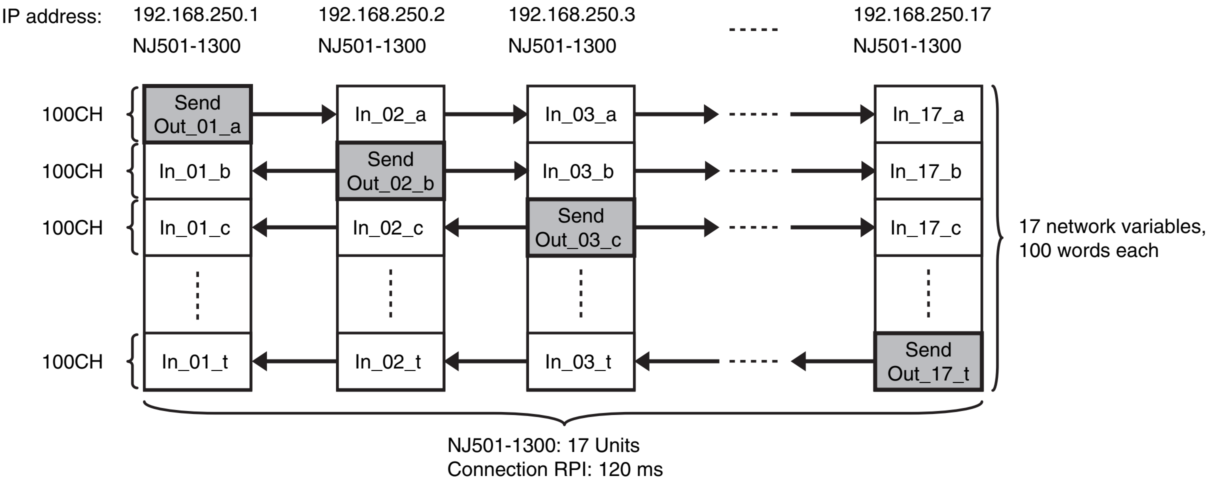
12-2-5 RPI Setting Examples

The following examples explain how to calculate the packet intervals (RPIs) in the following network configuration.

Conditions

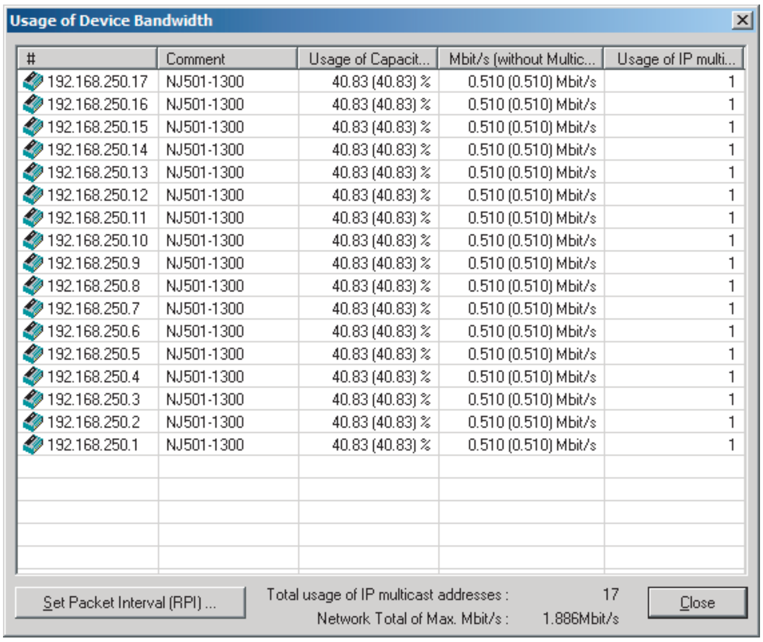


- Connections:
  Example) Seventeen NJ501-1300 Units are connected to the network.
  Each device has one 100-word tag for sending and sixteen 100-word tags for receiving, and exchanges data with each other.
  The packet interval (RPI) for all the connections is set to 120 ms.
  The IP addresses of the devices range from 192.168.250.1 to 192.168.250.17.



Checking the Device Bandwidth Usage

When you click the **Detail** Button in the Usage of Device Bandwidth Area, the window shows that the usage rate of the tag data link bandwidth for each device is 40.83%, as given in the Usage of Capacity column in the following window.



#	Comment	Usage of Capacit...	Mbit/s (without Multic...	Usage of IP multi...
192.168.250.17	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1
192.168.250.16	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1
192.168.250.15	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1
192.168.250.14	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1
192.168.250.13	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1
192.168.250.12	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1
192.168.250.11	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1
192.168.250.10	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1
192.168.250.9	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1
192.168.250.8	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1
192.168.250.7	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1
192.168.250.6	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1
192.168.250.5	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1
192.168.250.4	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1
192.168.250.3	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1
192.168.250.2	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1
192.168.250.1	NJ501-1300	40.83 (40.83) %	0.510 (0.510) Mbit/s	1

Total usage of IP multicast addresses : 17
Network Total of Max. Mbit/s : 1.886Mbit/s

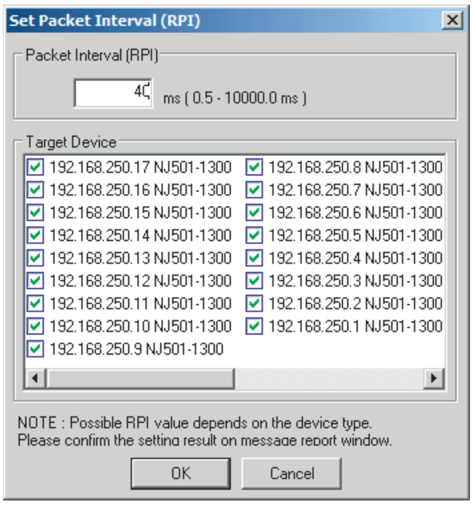
Changing Settings

Method 1: Setting the Same RPI for All the Connections

In the previous example, the usage rate of allowable tag data link bandwidth is 40.83% for all the devices as given in the Usage of Capacity column, and the RPI is set to 120 ms for all the connections. In the next example, change the RPI to 40 ms so as to increase the usage rate of allowable tag data link bandwidth up to 80% or less.

Click the **Set Packet Interval (RPI)** Button in the **Usage of Device Bandwidth** Dialog Box to display the **Set Packet Interval (RPI)** Dialog Box.

Input 40 ms as the new RPI value, and click the **OK** Button.


Set Packet Interval (RPI)

Packet Interval (RPI)

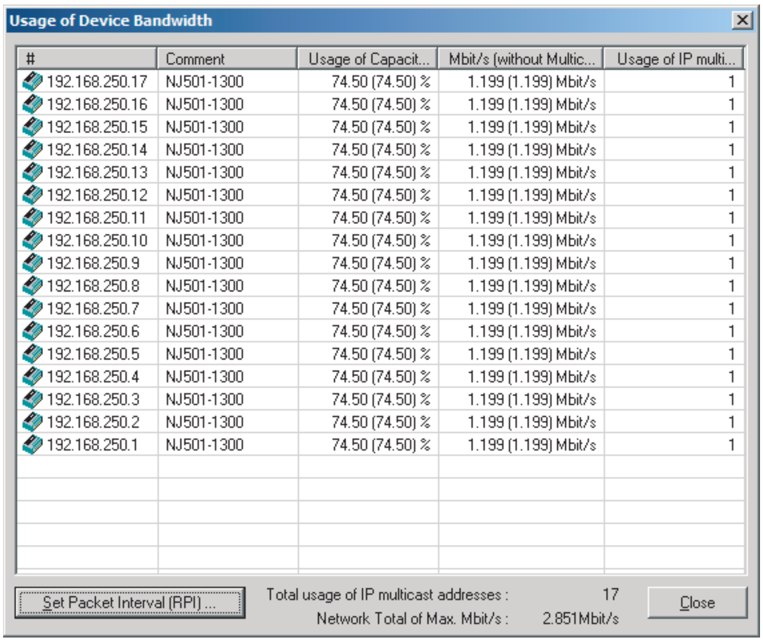
40 ms (0.5 - 10000.0 ms)

Target Device

☑ 192.168.250.17 NJ501-1300
☑ 192.168.250.16 NJ501-1300
☑ 192.168.250.15 NJ501-1300
☑ 192.168.250.14 NJ501-1300
☑ 192.168.250.13 NJ501-1300
☑ 192.168.250.12 NJ501-1300
☑ 192.168.250.11 NJ501-1300
☑ 192.168.250.10 NJ501-1300
☑ 192.168.250.9 NJ501-1300
☑ 192.168.250.8 NJ501-1300
☑ 192.168.250.7 NJ501-1300
☑ 192.168.250.6 NJ501-1300
☑ 192.168.250.5 NJ501-1300
☑ 192.168.250.4 NJ501-1300
☑ 192.168.250.3 NJ501-1300
☑ 192.168.250.2 NJ501-1300
☑ 192.168.250.1 NJ501-1300

NOTE : Possible RPI value depends on the device type.
Please confirm the setting result on message report window.

If you set the same packet interval (RPI) for all the connections, the table shows that the usage rate of allowable tag data link bandwidth is 74.50% for all the device as shown in the Usage of Capacity column, and this indicates that the shortest packet interval is 40 ms.


Usage of Device Bandwidth

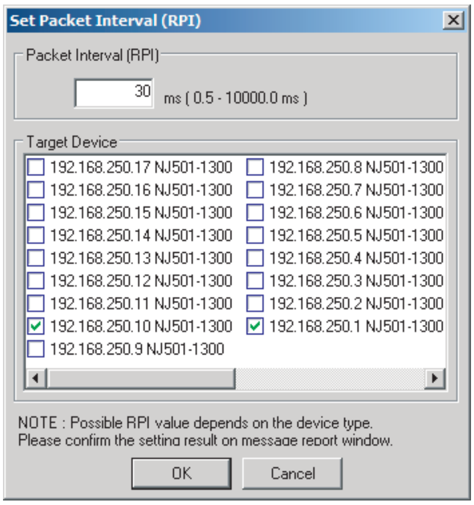
#	Comment	Usage of Capacit...	Mbit/s (without Multic...	Usage of IP multi...
192.168.250.17	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1
192.168.250.16	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1
192.168.250.15	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1
192.168.250.14	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1
192.168.250.13	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1
192.168.250.12	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1
192.168.250.11	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1
192.168.250.10	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1
192.168.250.9	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1
192.168.250.8	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1
192.168.250.7	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1
192.168.250.6	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1
192.168.250.5	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1
192.168.250.4	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1
192.168.250.3	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1
192.168.250.2	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1
192.168.250.1	NJ501-1300	74.50 (74.50) %	1.199 (1.199) Mbit/s	1

Total usage of IP multicast addresses : 17
Network Total of Max. Mbit/s : 2.851Mbit/s

Method 2: Changing the Packet Intervals (RPIs) of Specific Devices

In this example, set faster tag data links for specific two devices: 192.168.250.1 and 192.168.250.10. Click the **Set Packet Interval (RPI)** Button in the **Usage of Device Bandwidth** Dialog Box to display the **Set Packet Interval (RPI)** Dialog Box.

In the **Target Device** Area, clear the check boxes for devices to which this RPI change is not applied (all the devices except 192.168.250.1 and 192.168.250.10). Input 30 ms as the new RPI value, and click the **OK** Button.



Packet Interval (RPI)

30 ms (0.5 - 10000.0 ms)

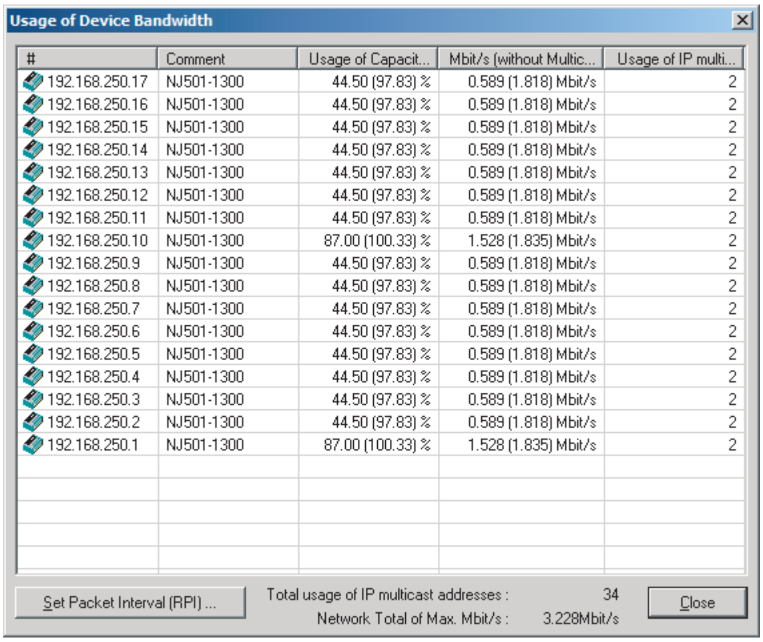
Target Device

- ☐ 192.168.250.17 NJ501-1300
- ☐ 192.168.250.16 NJ501-1300
- ☐ 192.168.250.15 NJ501-1300
- ☐ 192.168.250.14 NJ501-1300
- ☐ 192.168.250.13 NJ501-1300
- ☐ 192.168.250.12 NJ501-1300
- ☐ 192.168.250.11 NJ501-1300
- ☑ 192.168.250.10 NJ501-1300
- ☐ 192.168.250.9 NJ501-1300
- ☐ 192.168.250.8 NJ501-1300
- ☐ 192.168.250.7 NJ501-1300
- ☐ 192.168.250.6 NJ501-1300
- ☐ 192.168.250.5 NJ501-1300
- ☐ 192.168.250.4 NJ501-1300
- ☐ 192.168.250.3 NJ501-1300
- ☐ 192.168.250.2 NJ501-1300
- ☑ 192.168.250.1 NJ501-1300

NOTE : Possible RPI value depends on the device type.
Please confirm the setting result on message report window.

The usage rate of allowable tag data link bandwidth for each of the two devices, 192.168.250.1 and 192.168.250.10, increases to 87.00% as shown in the Usage of Capacity column, and this indicates that the shorter RPI is set for the connections of these devices.

Note that the usage rate of allowable tag data link bandwidth for all the other devices is also increased from 40.83% to 44.50% since they are connected with the two devices, 192.168.250.1 and 192.168.250.10.



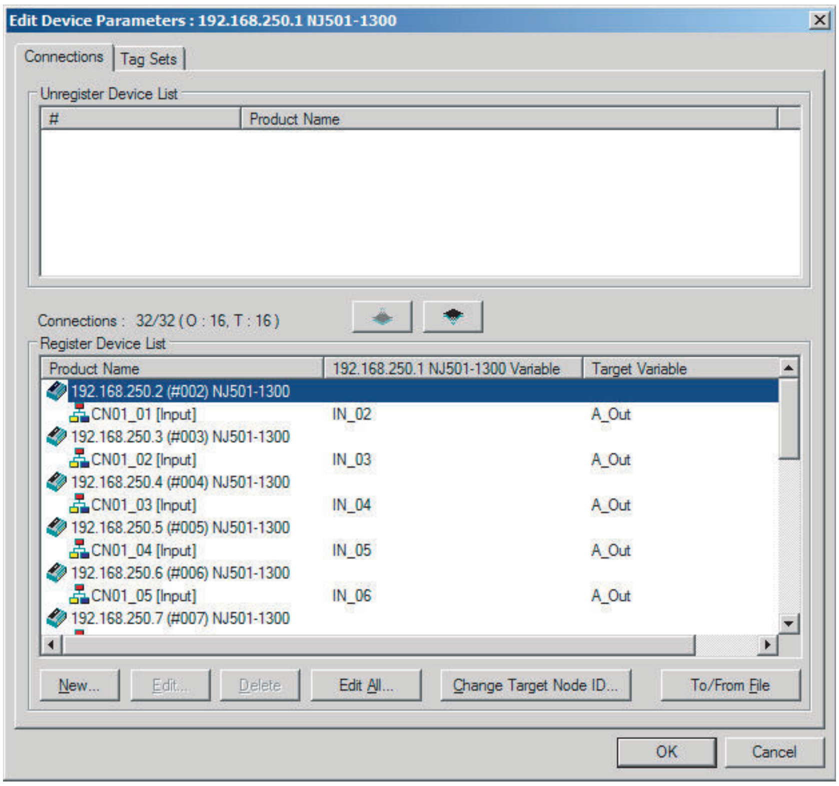
#	Comment	Usage of Capacit...	Mbit/s (without Multic...	Usage of IP multi...
192.168.250.17	NJ501-1300	44.50 (97.83) %	0.589 (1.818) Mbit/s	2
192.168.250.16	NJ501-1300	44.50 (97.83) %	0.589 (1.818) Mbit/s	2
192.168.250.15	NJ501-1300	44.50 (97.83) %	0.589 (1.818) Mbit/s	2
192.168.250.14	NJ501-1300	44.50 (97.83) %	0.589 (1.818) Mbit/s	2
192.168.250.13	NJ501-1300	44.50 (97.83) %	0.589 (1.818) Mbit/s	2
192.168.250.12	NJ501-1300	44.50 (97.83) %	0.589 (1.818) Mbit/s	2
192.168.250.11	NJ501-1300	44.50 (97.83) %	0.589 (1.818) Mbit/s	2
192.168.250.10	NJ501-1300	87.00 (100.33) %	1.528 (1.835) Mbit/s	2
192.168.250.9	NJ501-1300	44.50 (97.83) %	0.589 (1.818) Mbit/s	2
192.168.250.8	NJ501-1300	44.50 (97.83) %	0.589 (1.818) Mbit/s	2
192.168.250.7	NJ501-1300	44.50 (97.83) %	0.589 (1.818) Mbit/s	2
192.168.250.6	NJ501-1300	44.50 (97.83) %	0.589 (1.818) Mbit/s	2
192.168.250.5	NJ501-1300	44.50 (97.83) %	0.589 (1.818) Mbit/s	2
192.168.250.4	NJ501-1300	44.50 (97.83) %	0.589 (1.818) Mbit/s	2
192.168.250.3	NJ501-1300	44.50 (97.83) %	0.589 (1.818) Mbit/s	2
192.168.250.2	NJ501-1300	44.50 (97.83) %	0.589 (1.818) Mbit/s	2
192.168.250.1	NJ501-1300	87.00 (100.33) %	1.528 (1.835) Mbit/s	2

Total usage of IP multicast addresses : 34
Network Total of Max. Mbit/s : 3.228Mbit/s

In this case, if the Ethernet switch has no multicast filter, the Usage of Capacity value would be 100.33% and communications errors might occur due to traffic overload at the EtherNet/IP port.

Method 3: Changing the Packet Interval (RPI) of a Specific Connection

In this example, set faster tag data links for a specific connection of a device, 192.168.250.1. Double-click the device, 192.168.250.1, in the Network Configuration Window.



Edit Device Parameters : 192.168.250.1 NJ501-1300

Unregister Device List

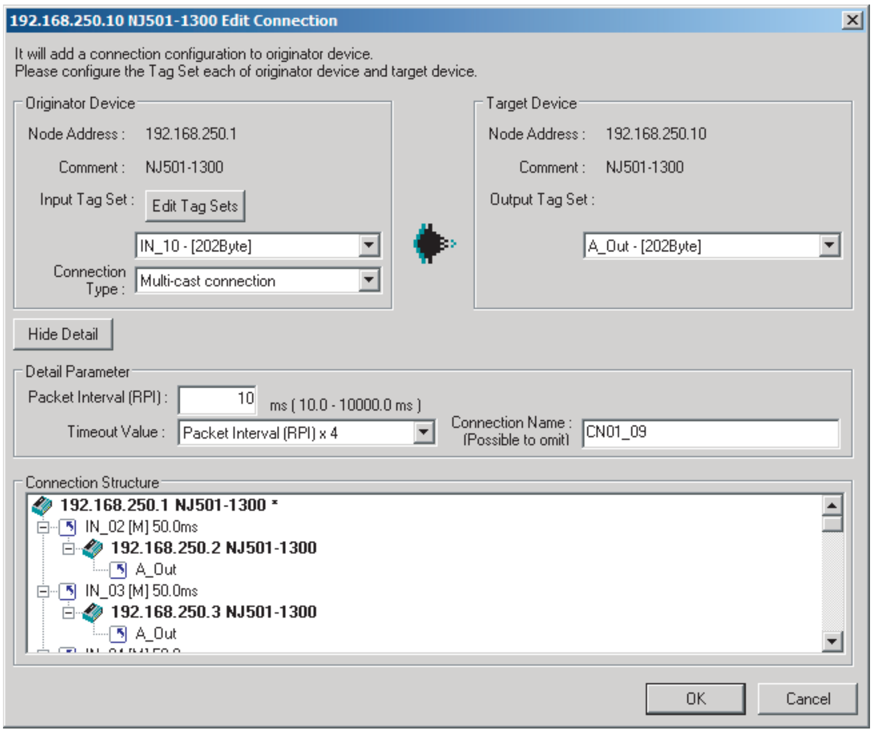
#	Product Name

Connections : 32/32 (O : 16, T : 16)

Register Device List

Product Name	192.168.250.1 NJ501-1300 Variable	Target Variable
192.168.250.2 (#002) NJ501-1300		
CN01_01 [Input]	IN_02	A_Out
192.168.250.3 (#003) NJ501-1300		
CN01_02 [Input]	IN_03	A_Out
192.168.250.4 (#004) NJ501-1300		
CN01_03 [Input]	IN_04	A_Out
192.168.250.5 (#005) NJ501-1300		
CN01_04 [Input]	IN_05	A_Out
192.168.250.6 (#006) NJ501-1300		
CN01_05 [Input]	IN_06	A_Out
192.168.250.7 (#007) NJ501-1300		

Since the Register Device List shows a list of devices connected with 192.168.250.1, double-click a device, 192.168.250.10, in the list.



192.168.250.10 NJ501-1300 Edit Connection

It will add a connection configuration to originator device.
Please configure the Tag Set each of originator device and target device.

Originator Device
Node Address : 192.168.250.1
Comment : NJ501-1300
Input Tag Set : IN_10 - [202Byte]
Connection Type : Multi-cast connection

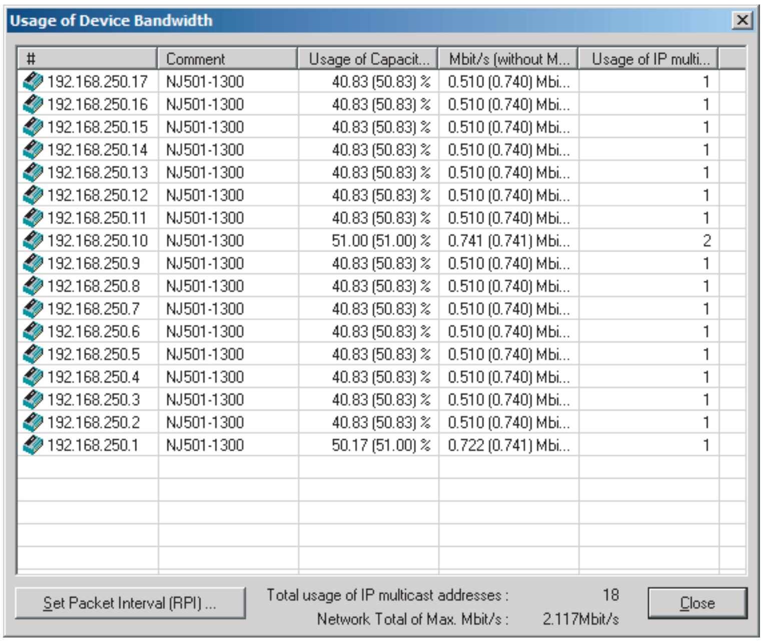
Target Device
Node Address : 192.168.250.10
Comment : NJ501-1300
Output Tag Set : A_Out - [202Byte]

Detail Parameter
Packet Interval (RPI) : 10 ms (10.0 - 10000.0 ms)
Timeout Value : Packet Interval (RPI) x 4
Connection Name : (Possible to omit) CN01_09

Connection Structure

```
192.168.250.1 NJ501-1300 *
  IN_02 [M] 50.0ms
    192.168.250.2 NJ501-1300
      A_Out
  IN_03 [M] 50.0ms
    192.168.250.3 NJ501-1300
      A_Out
```

Input 10 ms as the new RPI value in the Edit Connection Dialog Box, and click the **OK** Button. The usage rate of allowable tag data link bandwidth for the device 192.168.250.1 increases to 50.17% as shown in the Usage of Capacity column, and this indicates that the RPI for the specific connection is set shorter.



#	Comment	Usage of Capacit...	Mbit/s (without M...	Usage of IP multi...
192.168.250.17	NJ501-1300	40.83 (50.83) %	0.510 (0.740) Mbi...	1
192.168.250.16	NJ501-1300	40.83 (50.83) %	0.510 (0.740) Mbi...	1
192.168.250.15	NJ501-1300	40.83 (50.83) %	0.510 (0.740) Mbi...	1
192.168.250.14	NJ501-1300	40.83 (50.83) %	0.510 (0.740) Mbi...	1
192.168.250.13	NJ501-1300	40.83 (50.83) %	0.510 (0.740) Mbi...	1
192.168.250.12	NJ501-1300	40.83 (50.83) %	0.510 (0.740) Mbi...	1
192.168.250.11	NJ501-1300	40.83 (50.83) %	0.510 (0.740) Mbi...	1
192.168.250.10	NJ501-1300	51.00 (51.00) %	0.741 (0.741) Mbi...	2
192.168.250.9	NJ501-1300	40.83 (50.83) %	0.510 (0.740) Mbi...	1
192.168.250.8	NJ501-1300	40.83 (50.83) %	0.510 (0.740) Mbi...	1
192.168.250.7	NJ501-1300	40.83 (50.83) %	0.510 (0.740) Mbi...	1
192.168.250.6	NJ501-1300	40.83 (50.83) %	0.510 (0.740) Mbi...	1
192.168.250.5	NJ501-1300	40.83 (50.83) %	0.510 (0.740) Mbi...	1
192.168.250.4	NJ501-1300	40.83 (50.83) %	0.510 (0.740) Mbi...	1
192.168.250.3	NJ501-1300	40.83 (50.83) %	0.510 (0.740) Mbi...	1
192.168.250.2	NJ501-1300	40.83 (50.83) %	0.510 (0.740) Mbi...	1
192.168.250.1	NJ501-1300	50.17 (51.00) %	0.722 (0.741) Mbi...	1

Total usage of IP multicast addresses : 18
Network Total of Max. Mbit/s : 2.117Mbit/s

Note that the usage rate of allowable tag data link bandwidth for the device, 192.168.250.10, is also increased from 40.83% to 51.00%.

12-3 Tag Data Link I/O Response Time

The following shows how to calculate the guideline for the tag data link I/O response time.

12-3-1 Timing of Data Transmissions

This section describes the timing of transmitting data for tag data link between an NX-series EtherNet/IP Unit and a CPU Unit.

The NX-series EtherNet/IP Unit and the CPU Unit transmit data during I/O refresh time.

Two types of tasks can be set to perform I/O refreshing, primary periodic task and priority-16 periodic task. Tasks to perform I/O refreshing of tag data links are specified for each tag set. Refer to *I/O Refreshing of X Bus Function Module* in the *NJ/NX-series CPU Unit Software User's Manual (Cat. No. W501)* for details on the settings.

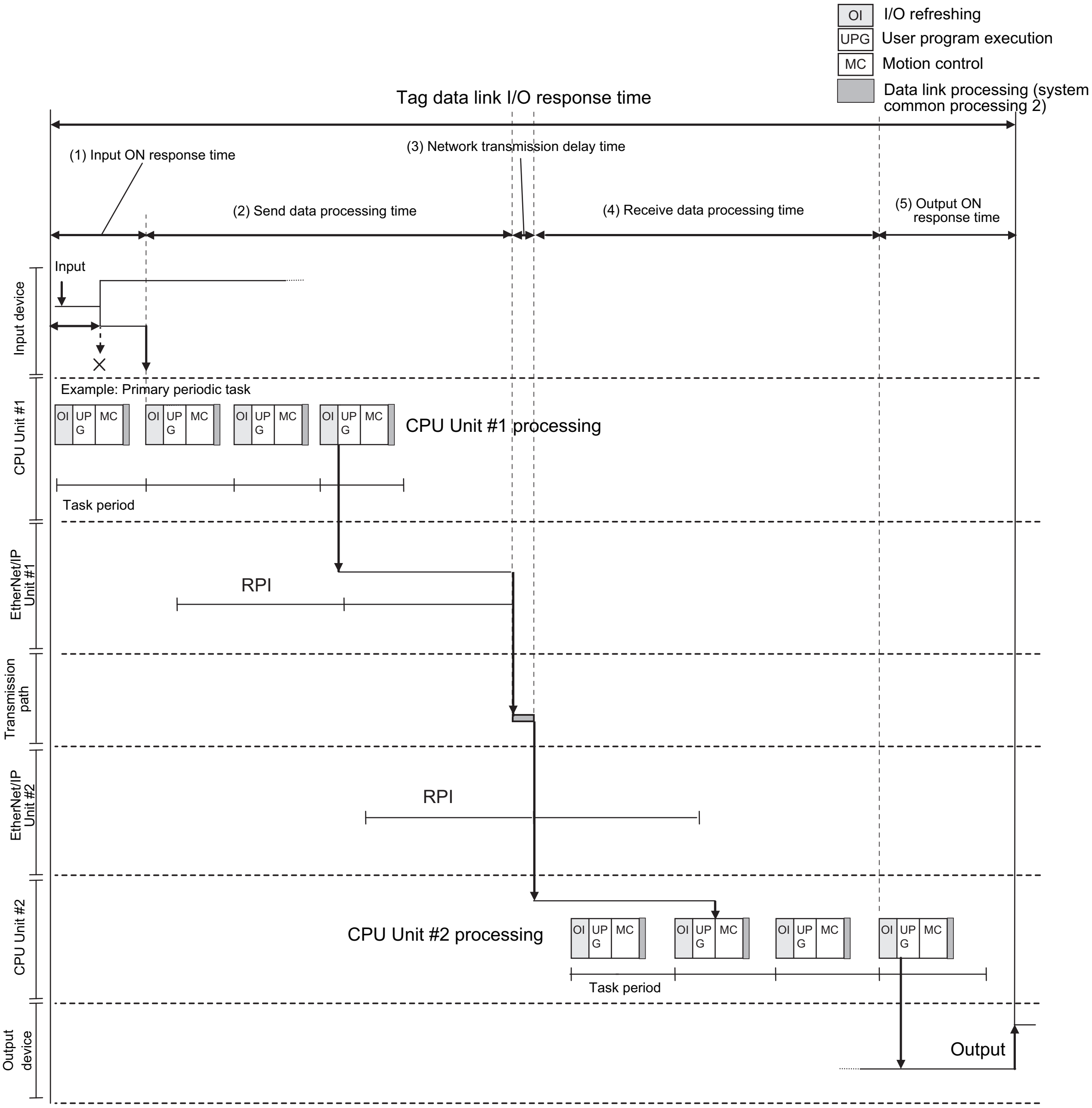
12-3-2 Maximum Tag Data Link I/O Response Time

The following shows how to calculate the guideline for the maximum tag data link I/O response time.

Precautions for Correct Use

The numerical values that are obtained by the calculation described here shall be used as a guideline for the maximum tag data link I/O response time. Always confirm the execution times with the physical Controller and study the designs before starting actual system operation.

You can calculate the maximum tag data link I/O response time by adding up the time of (1) to (5) in the following figure.


OI I/O refreshing
UPG User program execution
MC Motion control
Data link processing (system common processing 2)
Tag data link I/O response time
(1) Input ON response time
(2) Send data processing time
(3) Network transmission delay time
(4) Receive data processing time
(5) Output ON response time
Input device
Input
CPU Unit #1
Example: Primary periodic task
OI UPG MC
CPU Unit #1 processing
Task period
EtherNet/IP Unit #1
RPI
Transmission path
EtherNet/IP Unit #2
RPI
CPU Unit #2
CPU Unit #2 processing
Task period
Output device
Output

1. **Input ON Response Time**

   The input ON response time contains the delay time for the external input device from when the input occurs until the switch actually changes to ON and the time until the input data is stored in the memory area of the CPU Unit. Refer to the input delay information of the device for input switch delay time.
   One task period is required until the input data is stored in the memory area of the CPU Unit. Accordingly, the input ON response time is calculated as below.

   Input ON response time = Input device delay time + Task period

2. **Send Data Processing Time**

   This is the time required to transfer a variable from the CPU Unit to the EtherNet/IP port on the NX-series EtherNet/IP Unit.

The send data processing time is calculated using the task period of the task in which to perform I/O refreshing and to which the tag set is assigned in the CPU Unit that sends data. The calculation procedures is as follows.

Primary periodic task:
Maximum send data processing time = (the greater of the task period of the primary periodic task and the RPI of the tag set) + RPI of the tag set

Priority-16 periodic task
Maximum send data processing time = (the greater of the task period of the priority-16 periodic task and the RPI of the tag set) × 2 + RPI of the tag set

3. **Network Transmission Delay Time**
   The transmission delay on an Ethernet line is 50 μs or less. This delay time can be ignored.

4. **Receive Data Processing Time**
   This is the time required to transfer data that is received on the EtherNet/IP port on the NX-series EtherNet/IP Unit to a variable in the CPU Unit.
   The receive data processing time is calculated using the task period of the task in which to perform I/O refreshing and to which the tag set is assigned in the CPU Unit that receives data. The calculation procedures is as follows.

   Primary periodic task:
   Maximum receive data processing time = (the greater of the task period of the primary periodic task and the RPI of the tag set) + task period of the primary periodic task

   Priority-16 periodic task
   Maximum receive data processing time = (the greater of the task period of the priority-16 periodic task and the RPI of the tag set) × 2 + task period of the priority-16 periodic task

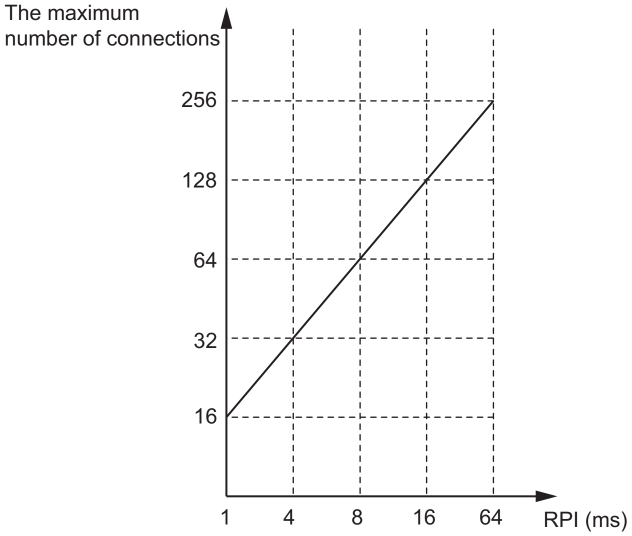
5. **Output ON Response Time**
   This is the delay time from when an output command is issued by the Controller until the output is executed on the external output device.
   Output ON response time = Output device delay time + task period of the CPU Unit

Additional Information

The I/O response time may be longer due to noise, or other causes.

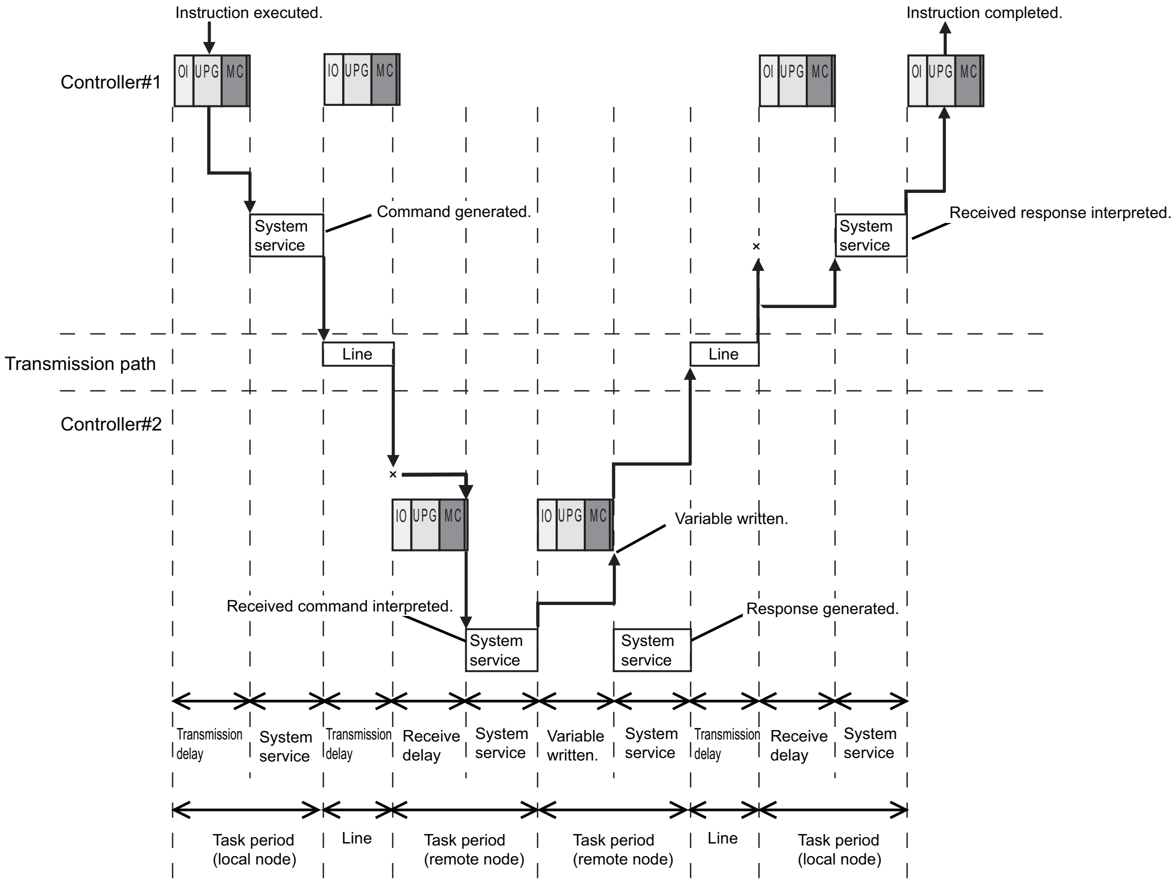
Precautions for Correct Use

Set the number of tag data link connections so that it does not exceed the upper limit for the RPI shown in the figure below.



12-4 Message Service Transmission Delay

This section describes delay time in the service processing of a CIP communications instruction.



$$\text{Maximum transmission delay time} = \underbrace{\text{Send delay} + \text{System service execution time}}_{\text{(Local node task period)}} + \text{Transmission delay} + \underbrace{\text{Receive delay} + \text{System service execution time}}_{\text{(Remote node task period)}}$$

$$+ \underbrace{\text{Variable write time} + \text{System service execution time}}_{\text{(Remote node task period)}} + \text{Transmission delay} + \underbrace{\text{Receive delay} + \text{System service execution time}}_{\text{(Local node task period)}}$$

Processes with delay time are processed within the task period of each node as shown in the above diagram.
Delay time related to transmission lines is as below.

● Transmission Delay

The transmission delay on an Ethernet line is 50 µs or less. This delay time can be ignored.

Additional Information

Depending on the actual operating environment, the transmission time may be longer than the one calculated with the equations given above.
The following factors can cause longer transmission time: the load rate of the network (the degree of network congestion), the window size of each network node, traffic load on the EtherNet/IP port (e.g., simultaneous tag data link communications), and the system configuration.

CIP communications instructions are executed in the system service process.
If a timeout occurs for a CIP communications instruction, reconsider the execution time for the system service.

13

Instructions Specific to NX-series EtherNet/IP Units

Commonly Used Structure Variables

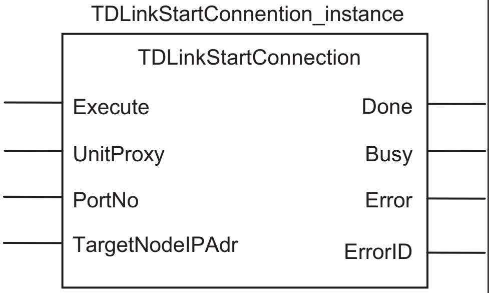
The following gives the definition of structure variables commonly used in instructions specific to the NX-series EtherNet/IP Unit.

- **UnitProxy**

Variable name		Meaning	Data type	Description
	Member name			
UnitProxy		Specified Unit	_sXBU_ID	A structure that specifies the NX-series EtherNet/IP Unit to control.
	UnitNo	Unit Number	UINT	Unit number

TDLinkStartConnection

The TDLinkStartConnection instruction specifies the target node and starts the tag data link connection.

Instruction	Name	FB/FUN	Graphic expression	ST expression
TDLinkStartConnection	Start Tag Data Link Target Connection	FB	 TDLinkStartConnention_instance TDLinkStartConnection Execute UnitProxy PortNo TargetNodeIPAdr Done Busy Error ErrorID	TDLinkStartConnection_instance (Execute, UnitProxy, PortNo. TargetNodeIPAdr, Done, Busy, Error, ErrorID);

Variables

Input Variables

Input variable		Meaning	Data type	Valid range	Unit	Initial value	Description
Execute		Execute	BOOL	TRUE or FALSE	---	FALSE	TRUE: Instruction is executed. FALSE: Instruction is not executed.
UnitProxy		Specified Unit	_sXBU_ID	Depends on data type.	---	*1	Specifies the NX-series EtherNet/IP Unit to control.
	UnitNo	Unit Number	UINT	1 to 4	---	0	Unit number of the NX-series EtherNet/IP Unit to access.
PortNo		Port Number	USINT	1 or 2	---	1	Specifies the port number. 1: Port 1 2: Port 2
TargetNodeIPAdr		Target Node IP Address	ARRAY[0..3] OF BYTE	Depends on data type.	---	{0,0,0,0}	Specifies the target IP address to start the tag data link in big endian.

*1. If you omit an initial value, a building error will occur.

Output Variables

Output variable	Meaning	Data type	Valid range	Unit	Description
Done	Done	BOOL	TRUE or FALSE	---	TRUE: Normal end FALSE: Error end, execution in progress, or execution condition not met.

Output variable	Meaning	Data type	Valid range	Unit	Description
Busy	Executing	BOOL	TRUE or FALSE	---	TRUE: Execution processing is in progress. FALSE: Execution processing is not in progress.
Error	Error	BOOL	TRUE or FALSE	---	TRUE: Error end FALSE: Normal end, execution in progress, or execution condition not met.
ErrorID	Error Code	WORD	16#0000 to 16#FFFF	---	This is the error code for an error end. The value is WORD#16#0 for a normal end.

Related Device Variables

Device variable	Meaning	Data type	Reference
EIP_Comm1Status.EstbTargetSta	CIP Communications1 Normal Target Node Information	ARRAY[0..255] OF BOOL	page 6-26
EIP_Comm2Status.EstbTargetSta	CIP Communications2 Normal Target Node Information	ARRAY[0..255] OF BOOL	page 6-26
EIP_Comm1Status.TargetNodeErr	CIP Communications1 Target Node Error Information	ARRAY[0..255] OF BOOL	page 6-28
EIP_Comm2Status.TargetNodeErr	CIP Communications2 Target Node Error Information	ARRAY[0..255] OF BOOL	page 6-28
EIP_Comm1Status.TDLinkAllRunSta	CIP Communications1 All Tag Data Link Communications Status	BOOL	page 6-25
EIP_Comm2Status.TDLinkAllRunSta	CIP Communications2 All Tag Data Link Communications Status	BOOL	page 6-25
EIP_Comm1Status.TDLinkRunSta	CIP Communications1 Tag Data Link Communications Status	BOOL	page 6-24
EIP_Comm2Status.TDLinkRunSta	CIP Communications2 Tag Data Link Communications Status	BOOL	page 6-25

Related Error Codes

Error code	Name	Description
0400 hex	Input Value Out of Range	• UnitProxy is out of range • PortNo is out of range
5C00 hex	Cannot Execute at Specified Unit/Port	The EtherNet/IP port designated by the specified Unit and port number does not exist. An instruction was executed when execution was not possible.
5C01 hex	Too Many Simultaneous Instruction Executions	Tag data link control instructions (TDLinkStartConnection and TDLinkStopConnection) were executed more than the number that can be executed at the same time.
5C03 hex	Target Node IP Address Does Not Exist	Connection settings with the target node IP address do not exist on the Ethernet/IP port specified by the specified Unit and port number.
5C04 hex	Connection Communications Error	Communications can not be established with the target node specified by target node IP address.
5C05 hex	Connection Setting Error	An abnormal response from the target node was received.

Function

The TDLinkStartConnection instruction starts all tag data link connections for the target specified with *TargetNodeIPAdr* when *Execute* changes from FALSE to TRUE.

Busy changes to TRUE during execution and *Done* changes to TRUE after the start of all connections for the specified target. *Error* changes to TRUE if one of the specified targets cannot start the connection.

- Only one tag data link control instruction (TDLinkStartConnection and TDLinkStopConnection instructions) can be executed for each CPU Unit. Perform exclusive control processing if more than two instructions are written in the user program.
- Refer to the *EIP_Comm1Status.EstbTargetSta* (CIP Communications1 Normal Target Node Information) device variable or the *EIP_Comm2Status.EstbTargetSta* (CIP Communications2 Normal Target Node Information) device variable for the start and stop status of the connection.
- The settings changed by this instruction are saved in non-volatile memory and remain valid even after cycling the power supply.
- You cannot use this instruction in the CIPSafety routing.

Differences When Executing This Instruction in the Simulator

If this instruction is executed in the Simulator, when *Execute* changes from FALSE to TRUE, *Busy* changes to TRUE only in the first task period, and *Busy* changes to FALSE and *Done* changes to TRUE from the next task period.

The input parameters are discarded.

Precautions for Correct Use

- This instruction is executed over more than one task period. The execution continues even if *Execute* changes to FALSE once execution started.
- You cannot use this instruction in an event task. If you use this instruction in an event task, a building error will occur.

Sample Programming

The following sample programming is given below.

- The tag data link connection is started for the IP address provided in advance when *ChangeTrigger* changes to TRUE.

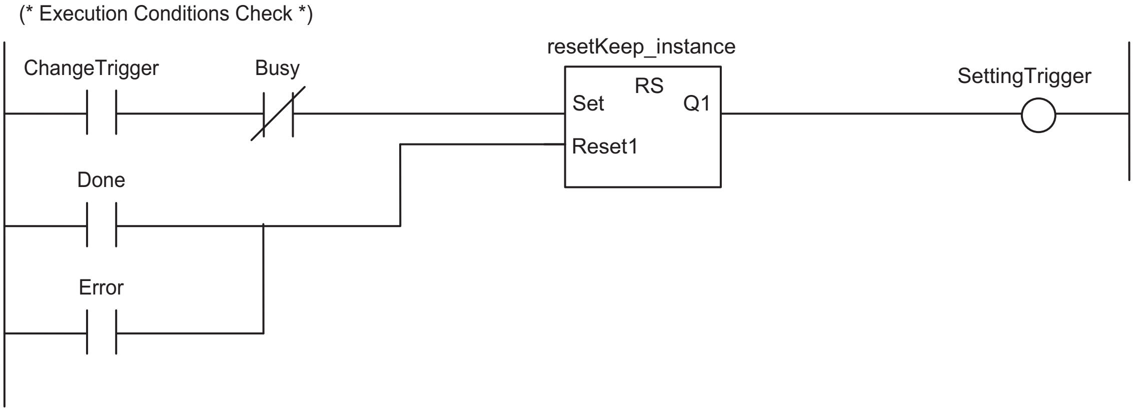
Ladder Diagram

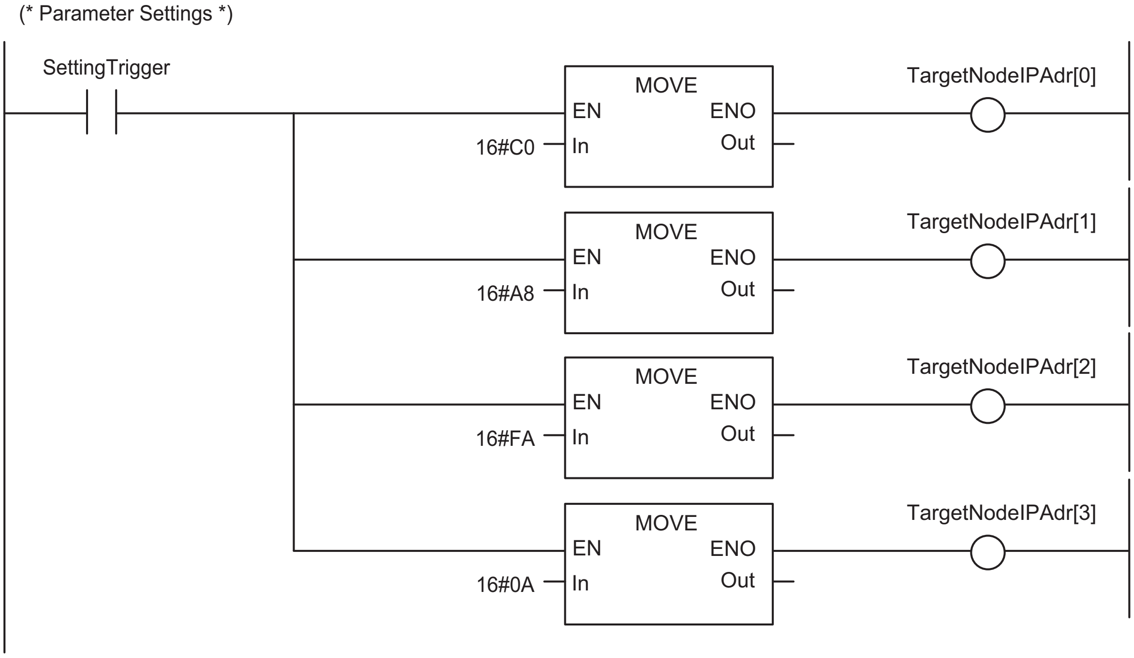
● Main Variables

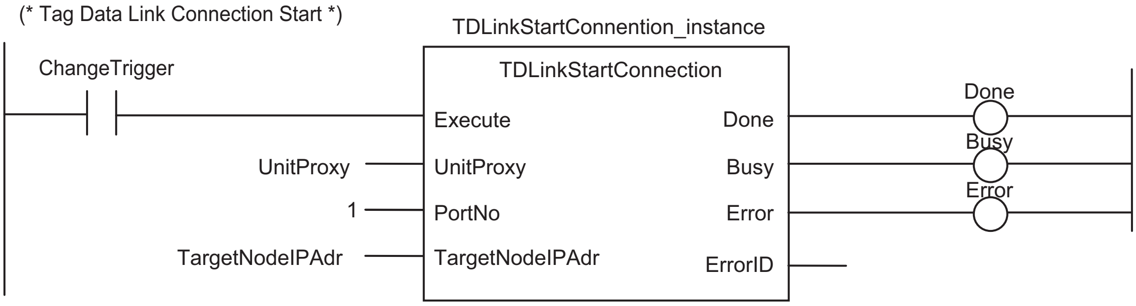
Name	Data type	Initial value	Comment
TDLinkStartConnection_Instance	TDLinkStartConnection	---	Instance of TDLinkStartConnection instruction
ChangeTrigger	BOOL	---	Start condition

Name	Data type	Initial value	Comment
SettingTrigger	BOOL	---	Parameter setting trigger
Done	BOOL	---	Done
Busy	BOOL	---	Executing
Error	BOOL	---	Error
TargetNodeIPAdr	ARRAY[0..3] OF BYTE	{0,0,0,0}	Target node IP address

● Algorithm







Structured Text (ST)

● Main Variables

Name	Data type	Initial value	Comment
TDLinkStartConnection_Instance	TDLinkStartConnection	---	Instance of TDLinkStartConnection instruction
ChangeTrigger	BOOL	---	Start condition
SettingTrigger	BOOL	---	Parameter setting trigger
Done	BOOL	---	Done
Busy	BOOL	---	Executing
Error	BOOL	---	Error
TargetNodeIPAdr	ARRAY[0..3] OF BYTE	{0,0,0,0}	Target node IP address

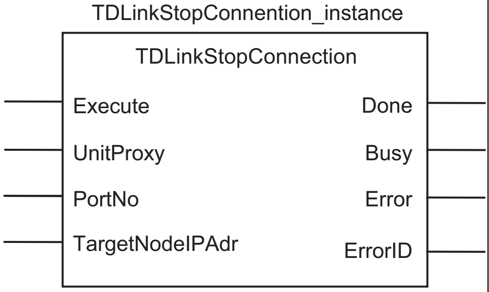
● Algorithm

```
(* Start condition ON check *)
         IF (ChangeTrigger = TRUE) AND (Busy = FALSE) THEN
         SettingTrigger := TRUE;
         END_IF;
         (* Start condition OFF check *)
         IF (Done = TRUE) OR (Error = TRUE) THEN
         SettingTrigger := FALSE;
         END_IF;
         (* Set parameters. *)
         IF  SettingTrigger = TRUE  THEN
         TargetNodeIPAdr[0]              := 16#C0;
         TargetNodeIPAdr[1]              := 16#A8;
         TargetNodeIPAdr[2]              := 16#FA;
         TargetNodeIPAdr[3]              := 16#0A;

         END_IF;
         (* Execute TDLinkStartConnection instruction. *)
         TDLinkStartConnection_Instance( Execute  := SettingTrigger,
         UnitProxy              := UnitProxy,
         PortNo                 := 1,
         TargetNodeIPAdr        := TargetNodeIPAdr,
         Done      => Done,
         Busy      => Busy,
         Error     => Error);
```

TDLinkStopConnection

The TDLinkStopConnection instruction specifies the target node and stops the tag data link connection.

Instruction	Name	FB/FUN	Graphic expression	ST expression
TDLinkStopConnection	Stop Tag Data Link Target Connection	FB	 TDLinkStopConnention_instance TDLinkStopConnection Execute UnitProxy PortNo TargetNodeIPAdr Done Busy Error ErrorID	TDLinkStopConnection_instance (Execute, UnitProxy, PortNo. TargetNodeIPAdr, Done, Busy, Error, ErrorID);

Variables

Input Variables

Input variable	Meaning	Data type	Valid range	Unit	Initial value	Description
Execute	Execute	BOOL	TRUE or FALSE	---	FALSE	TRUE: Instruction is executed. FALSE: Instruction is not executed.
UnitProxy	Specified Unit	_sXBU_ID	Depends on data type.	---	*1	Specifies the NX-series EtherNet/IP Unit to control.
UnitNo	Unit Number	UINT	1 to 4	---	0	Unit number of the NX-series EtherNet/IP Unit to access.
PortNo	Port Number	USINT	1 or 2	---	1	Specifies the port number. 1: Port 1 2: Port 2
TargetNodeIPAdr	Target Node IP Address	ARRAY[0..3] OF BYTE	Depends on data type.	---	{0,0,0,0}	Specifies the target IP address to stop the tag data link in big endian.

*1. If you omit an initial value, a building error will occur.

Output Variables

Output variable	Meaning	Data type	Valid range	Unit	Description
Done	Done	BOOL	TRUE or FALSE	---	TRUE: Normal end FALSE: Error end, execution in progress, or execution condition not met.

Output variable	Meaning	Data type	Valid range	Unit	Description
Busy	Executing	BOOL	TRUE or FALSE	---	TRUE: Execution processing is in progress. FALSE: Execution processing is not in progress.
Error	Error	BOOL	TRUE or FALSE	---	TRUE: Error end FALSE: Normal end, execution in progress, or execution condition not met.
ErrorID	Error Code	WORD	16#0000 to 16#FFFF	---	This is the error code for an error end. The value is WORD#16#0 for a normal end.

Related Device Variables

Device variable	Meaning	Data type	Reference
EIP_Comm1Status.EstbTargetSta	CIP Communications1 Normal Target Node Information	ARRAY[0..255] OF BOOL	page 6-26
EIP_Comm2Status.EstbTargetSta	CIP Communications2 Normal Target Node Information	ARRAY[0..255] OF BOOL	page 6-26
EIP_Comm1Status.TargetNodeErr	CIP Communications1 Target Node Error Information	ARRAY[0..255] OF BOOL	page 6-28
EIP_Comm2Status.TargetNodeErr	CIP Communications2 Target Node Error Information	ARRAY[0..255] OF BOOL	page 6-28
EIP_Comm1Status.TDLinkAllRunSta	CIP Communications1 All Tag Data Link Communications Status	BOOL	page 6-25
EIP_Comm2Status.TDLinkAllRunSta	CIP Communications2 All Tag Data Link Communications Status	BOOL	page 6-25
EIP_Comm1Status.TDLinkRunSta	CIP Communications1 Tag Data Link Communications Status	BOOL	page 6-24
EIP_Comm2Status.TDLinkRunSta	CIP Communications2 Tag Data Link Communications Status	BOOL	page 6-25

Related Error Codes

Error code	Name	Description
0400 hex	Input Value Out of Range	• UnitProxy is out of range • PortNo is out of range
5C00 hex	Cannot Execute at Specified Unit/Port	The EtherNet/IP port designated by the specified Unit and port number does not exist. An instruction was executed when execution was not possible.
5C01 hex	Too Many Simultaneous Instruction Executions	Tag data link control instructions (TDLinkStartConnection and TDLinkStopConnection) were executed more than the number that can be executed at the same time.
5C03 hex	Target Node IP Address Does Not Exist	Connection settings with the target node IP address do not exist on the Ethernet/IP port specified by the specified Unit and port number.
5C04 hex	Connection Communications Error	Communications can not be established with the target node specified by target node IP address.
5C05 hex	Connection Setting Error	An abnormal response from the target node was received.

Function

The TDLinkStopConnection instruction stops all tag data link connections for the target specified with *TargetNodeIPAdr* when *Execute* changes from FALSE to TRUE.
Busy changes to TRUE during execution and *Done* changes to TRUE after all connections for the specified target stop. *Error* changes to TRUE if one of the specified targets cannot stop the connection.

- Only one tag data link control instruction (TDLinkStartConnection and TDLinkStopConnection instructions) can be executed for each CPU Unit. Perform exclusive control processing if more than two instructions are written in the user program.
- Refer to the *EIP_Comm1Status.EstbTargetSta* (CIP Communications1 Normal Target Node Information) device variable or the *EIP_Comm2Status.EstbTargetSta* (CIP Communications2 Normal Target Node Information) device variable for the start and stop status of the connection.
- The settings changed by this instruction are saved in non-volatile memory and remain valid even after cycling the power supply.
- You cannot use this instruction in the CIPSafety routing.

Differences When Executing This Instruction in the Simulator

If this instruction is executed in the Simulator, when *Execute* changes from FALSE to TRUE, *Busy* changes to TRUE only in the first task period, and *Busy* changes to FALSE and *Done* changes to TRUE from the next task period.
The input parameters are discarded.

Precautions for Correct Use

- This instruction is executed over more than one task period. The execution continues even if *Execute* changes to FALSE once execution started.
- You cannot use this instruction in an event task. If you use this instruction in an event task, a building error will occur.

Sample Programming

The following sample programming is given below.

- The tag data link connection is stopped for the IP address provided in advance when *ChangeTrigger* changes to TRUE.

Ladder Diagram

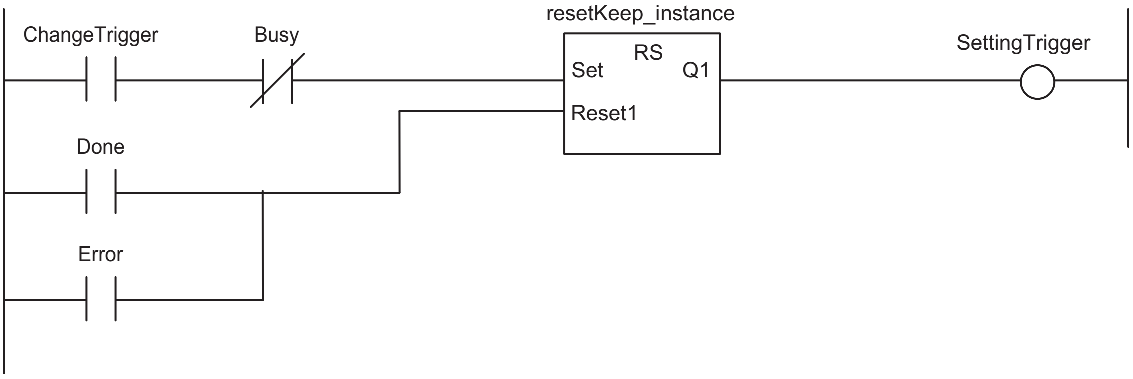
● Main Variables

Name	Data type	Initial value	Comment
TDLinkStopConnection_Instance	TDLinkStopConnection	---	Instance of TDLinkStopConnection instruction
ChangeTrigger	BOOL	---	Start condition

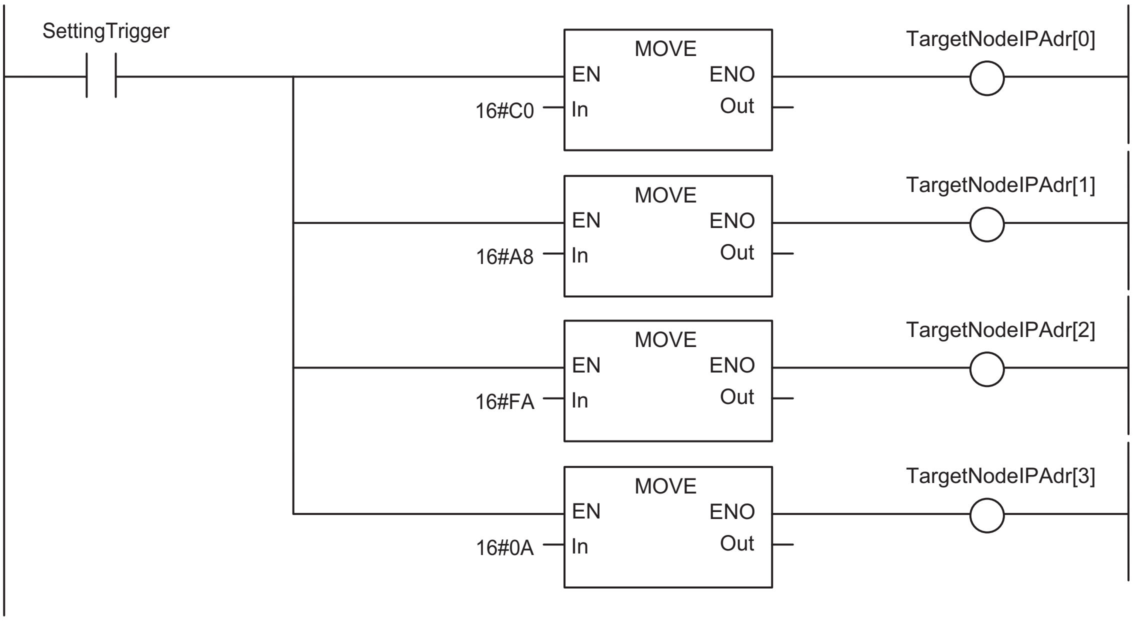
Name	Data type	Initial value	Comment
SettingTrigger	BOOL	---	Parameter setting trigger
Done	BOOL	---	Done
Busy	BOOL	---	Executing
Error	BOOL	---	Error
TargetNodeIPAdr	ARRAY[0..3] OF BYTE	{0,0,0,0}	Target node IP address

● Algorithm

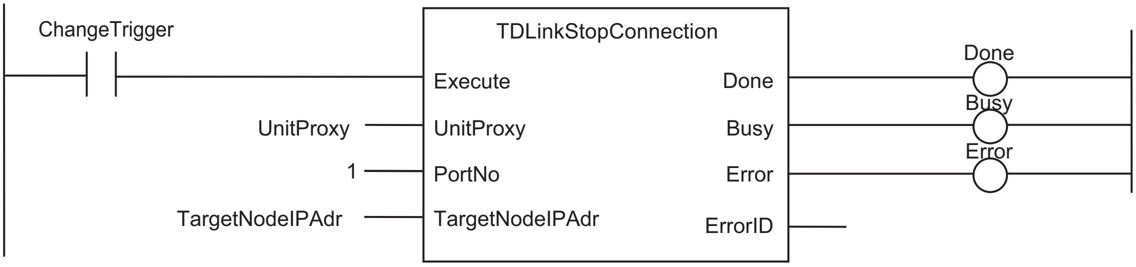
(* Execution Conditions Check *)



(* Parameter Settings *)



(* Tag Data Link Connection Stop *)



Structured Text (ST)

● Main Variables

Name	Data type	Initial value	Comment
TDLinkStopConnection_Instance	TDLinkStopConnection	---	Instance of TDLinkStopConnection instruction
ChangeTrigger	BOOL	---	Start condition
SettingTrigger	BOOL	---	Parameter setting trigger
Done	BOOL	---	Done
Busy	BOOL	---	Executing
Error	BOOL	---	Error
TargetNodeIPAdr	ARRAY[0..3] OF BYTE	{0,0,0,0}	Target node IP address

● Algorithm

```
(* Start condition ON check *)
          IF (ChangeTrigger = TRUE) AND (Busy = FALSE) THEN
          SettingTrigger := TRUE;
          END_IF;
          (* Start condition OFF check *)
          IF (Done = TRUE) OR (Error = TRUE) THEN
          SettingTrigger := FALSE;
          END_IF;
          (* Set parameters. *)
          IF  SettingTrigger = TRUE  THEN
          TargetNodeIPAdr[0]              := 16#C0;
          TargetNodeIPAdr[1]              := 16#A8;
          TargetNodeIPAdr[2]              := 16#FA;
          TargetNodeIPAdr[3]              := 16#0A;

          END_IF;
          (* Execute TDLinkStopConnection instruction. *)
          TDLinkStopConnection_Instance( Execute  := SettingTrigger,
          UnitProxy               := UnitProxy,
          PortNo                  := 1,
          TargetNodeIPAdr         := TargetNodeIPAdr,
          Done      => Done,
          Busy      => Busy,
          Error     => Error);
```

14

Troubleshooting

This section explains how to check the errors that occur on an NX-series EtherNet/IP Unit and resolve them.

14-1 Checking Methods for Errors

The following table shows the checking methods for errors that occur on an NX-series EtherNet/IP Unit and what you can check for.

Identify the errors that occur on the NX-series EtherNet/IP Unit by using these methods.

Checking method	What you can check	Reference
Checking with the Unit status indicators on the NX-series EtherNet/IP Unit	Level of current Controller error in the NX-series EtherNet/IP Unit and error state	*14-2 Checking with the Unit Status Indicators on the NX-series EtherNet/IP Unit* on page 14-3
Checking with the EtherNet/IP status indicators on the NX-series EtherNet/IP Unit	Current communications related error states in the NX-series EtherNet/IP Unit	*14-3 Checking with the EtherNet/IP Status Indicators on the NX-series EtherNet/IP Unit* on page 14-5
Checking with the troubleshooting function of Sysmac Studio	Current Controller errors in the NX-series EtherNet/IP Unit, a log of past errors, error sources, error causes, and corrections	*14-4 Checking with the Sysmac Studio, an HMI, and Instructions That Read Error Status* on page 14-6
Checking with the Troubleshooter of an HMI	Current Controller errors in the NX-series EtherNet/IP Unit, a log of past errors, error sources, error causes, and corrections	*14-4 Checking with the Sysmac Studio, an HMI, and Instructions That Read Error Status* on page 14-6
Checking with instructions that read error status	The highest level status and highest level event code of current Controller errors in the NX-series EtherNet/IP Unit	*14-4 Checking with the Sysmac Studio, an HMI, and Instructions That Read Error Status* on page 14-6
Checking with device variables	Status of current Controller errors in the X Bus Ethernet Function Module, X Bus EtherNet/IP Function Module, and X Bus Unit Common Function Module	*14-5 Checking with Device Variables* on page 14-46
Checking with the Network Configurator	Communications status of each device on the EtherNet/IP network (e.g. tag data link connection status)	*14-6 Checking with the Network Configurator* on page 14-47

14-2 Checking with the Unit Status Indicators on the NX-series EtherNet/IP Unit

You can check the operation status of the NX-series EtherNet/IP Unit by using the Unit status indicators on the NX-series EtherNet/IP Unit.

Refer to *3-2-1 Operation Status Indicators* on page 3-3 for the location of the Unit status indicators.

The status of Unit status indicators, operation status of an NX-series EtherNet/IP Unit, description of the operation status and correction are listed in the following table.

Indicators		Operation status of an NX-series EtherNet/IP Unit	Description	Correction
RUN (green)	**ERR (red)**			
Lit	Not lit	Normal operation	Operating normally.	---
Not lit	Not lit	Power Supply Error	The power supply to the NX-series EtherNet/IP Unit is not turned ON.	Turn ON the power supply.
			The voltage is out of allowable power supply range.	Check the power supply system to the Controller and modify to fit within the allowable power supply range.
			The power supply part of the NX-series EtherNet/IP Unit failed.	Replace the NX-series EtherNet/IP Unit.
		Hardware Initialization Error	A data error occurred in the firmware which is the minimum requirement to initialize the hardware of the NX-series EtherNet/IP Unit.	Cycle the power supply. If the NX-series EtherNet/IP Unit does not start normally after cycling the power supply, replace the NX-series EtherNet/IP Unit.

Indicators		Operation status of an NX-series EtherNet/IP Unit	Description	Correction
RUN (green)	**ERR (red)**			
Not lit	Lit	X Bus Unit Hardware Error	An error in the critical part occurred, i.e., the CPU of the NX-series EtherNet/IP Unit stopped, etc.	Cycle the power supply. If the NX-series EtherNet/IP Unit does not start normally after cycling the power supply, replace the NX-series EtherNet/IP Unit.
		X Bus Unit Common Function Processing Error	An error that causes all system control operations in the X Bus Unit to stop occurred.	Connect the Sysmac Studio and an HMI to the CPU Unit, refer to *Errors in the X Bus Unit Common Function Module* in the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* and troubleshoot the problem.
		CPU Unit Error	The NX-series EtherNet/IP Unit stopped operation due to an error that occurred in the NX502 CPU Unit.	• If the Sysmac Studio and an HMI can be connected to the CPU Unit, refer to *Troubleshooting Non-fatal Errors* in the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* and troubleshoot the problem. • If the Sysmac Studio and an HMI cannot be connected to the CPU Unit, cycle the power supply. If the CPU Unit does not start normally after cycling the power supply, replace the CPU Unit.
Flashing status continues more than 30 seconds.	Not lit	System Initialization Error	A hardware failure or data error in the NX-series EtherNet/IP Unit that is not detected as a Hardware Initialization Error or X Bus Unit Hardware Error occurred.	Cycle the power supply. If the NX-series EtherNet/IP Unit does not start normally after cycling the power supply, replace the NX-series EtherNet/IP Unit.
Lit	Flashing	Errors in the X Bus Function Module	An error in the X Bus Function Module occurred.	Refer to *Errors in the X Bus Function Module* in the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)*.
		Errors in the X Bus EtherNet/IP Function Module	An error in the X Bus EtherNet/IP Function Module occurred.	• *14-3 Checking with the EtherNet/IP Status Indicators on the NX-series EtherNet/IP Unit* on page 14-5 • *14-4 Checking with the Sysmac Studio, an HMI, and Instructions That Read Error Status* on page 14-6 • *14-5 Checking with Device Variables* on page 14-46 • *14-6 Checking with the Network Configurator* on page 14-47
		Errors in the X Bus Ethernet Function Module	An error in the X Bus Ethernet Function Module occurred.	

14-3 Checking with the EtherNet/IP Status Indicators on the NX-series EtherNet/IP Unit

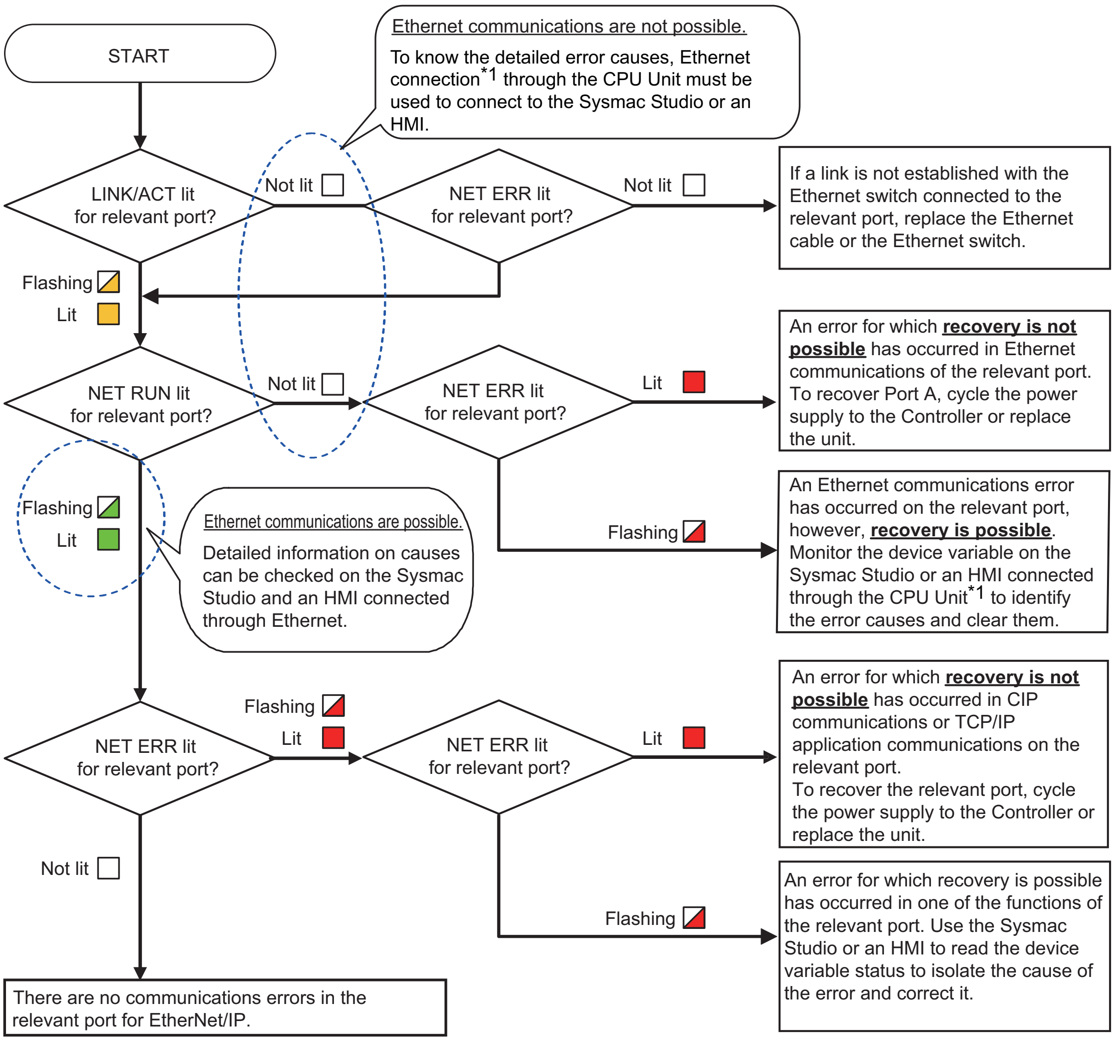
You can check whether an error related to the communications port of the NX-series EtherNet/IP Unit occurred or not and the error state with the EtherNet/IP status indicators on the NX-series EtherNet/IP Unit.

Refer to *3-2-1 Operation Status Indicators* on page 3-3 for the location of the EtherNet/IP status indicators.

The error state is checked for each communications port. The following flow diagram shows the procedure for checking the error state for a single communications port.

Refer to the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* for details on how to identify the cause of the error and resetting the error using the Sysmac Studio or an HMI.

In addition, refer to *Section 6 Device Variables Related to the NX-series EtherNet/IP Unit* on page 6-1 for details on device variables related to the NX-series EtherNet/IP Unit.


START
LINK/ACT lit for relevant port?
Not lit
NET ERR lit for relevant port?
Not lit
Flashing
Lit
NET RUN lit for relevant port?
Not lit
NET ERR lit for relevant port?
Lit
Flashing
Flashing
Lit
NET ERR lit for relevant port?
Flashing
Lit
NET ERR lit for relevant port?
Lit
Flashing
Not lit

Ethernet communications are not possible.

To know the detailed error causes, Ethernet connection[*1] through the CPU Unit must be used to connect to the Sysmac Studio or an HMI.

If a link is not established with the Ethernet switch connected to the relevant port, replace the Ethernet cable or the Ethernet switch.

An error for which **recovery is not possible** has occurred in Ethernet communications of the relevant port. To recover Port A, cycle the power supply to the Controller or replace the unit.

Ethernet communications are possible.

Detailed information on causes can be checked on the Sysmac Studio and an HMI connected through Ethernet.

An Ethernet communications error has occurred on the relevant port, however, **recovery is possible**. Monitor the device variable on the Sysmac Studio or an HMI connected through the CPU Unit[*1] to identify the error causes and clear them.

An error for which **recovery is not possible** has occurred in CIP communications or TCP/IP application communications on the relevant port.
To recover the relevant port, cycle the power supply to the Controller or replace the unit.

An error for which recovery is possible has occurred in one of the functions of the relevant port. Use the Sysmac Studio or an HMI to read the device variable status to isolate the cause of the error and correct it.

There are no communications errors in the relevant port for EtherNet/IP.

[*1] You can connect the Sysmac Studio or an HMI to the other port to confirm error details when Ethernet communications are possible for the other port.

14-4 Checking with the Sysmac Studio, an HMI, and Instructions That Read Error Status

You can check for current Controller errors in the NX-series EtherNet/IP Unit, a log of past errors, error sources, error causes, and corrections with the Sysmac Studio, HMI, and instructions that read error status.
Refer to *Checking with the Troubleshooting Function of Sysmac Studio*, *Checking with the Troubleshooter of an HMI*, and *Checking with Instructions That Read Error Status* in the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* for details on how to use each of the above.

The following describes the errors in the X Bus Ethernet Function Module and the X Bus EtherNet/IP Function Module, which are the communications errors that occur in the NX-series EtherNet/IP Unit.
The definitions of the X Bus Ethernet Function Module and the X Bus EtherNet/IP Function Module are as follows.

Function module	Definition
X Bus Ethernet Function Module	A function module that performs Ethernet functions of the X Bus Unit other than the EtherNet/IP function. With the NX-series EtherNet/IP Unit, a function module that performs TCP/IP or SNMP agent.
X Bus EtherNet/IP Function Module	A function module that performs EtherNet/IP function of the X Bus Unit. With the NX-series EtherNet/IP Unit, a function module that performs tag data links or CIP message communications.

Additional Information

The function modules related to the X Bus Unit other than the above include the X Bus Function Module and the X Bus Unit Common Function Module. The definitions of each module are given in the following table.

Function module	Definition
X Bus Function Module	A function module that manages the status of X Bus Unit which is connected to the X Bus of CPU Unit and also performs the processing of I/O refresh with the X Bus Unit, etc. as an X Bus master.
X Bus Unit Common Function Module	A function module of the X Bus Unit that manages the X Bus Unit common information, i.e. total power ON time and unit version, etc., the event log of X Bus Unit, and the status, and also performs the processing of I/O refresh with the CPU Unit, etc.

Refer to *Errors in the X Bus Function Module* in the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* for details on errors in the X Bus Function Module.
Refer to *Errors in the X Bus Unit Common Function Module* in the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* for details on errors in the X Bus Unit Common Function Module.

14-4-1 Types of Communications Errors

The communications errors that occur in the NX-series EtherNet/IP Unit are classified by the source as follows.

Error source	Communications port	Error source details	Description
X Bus Ethernet Function Module	Port 1	Communications port 1	This is an error related to all communications using EtherNet/IP ports. This includes BOOTP and DNS-related errors.
	Port 2	Communications port 2	
	Both ports	SNMP	This error is SNMP agent/trap related error.
X Bus EtherNet/IP Function Module	Port 1	CIP1	This is an error related to CIP communications. Other communication functions are not affected.
	Port 2	CIP2	

14-4-2 Source and Level of Communications Errors

The relationship between the source and level of communications error that may occur in the NX-series EtherNet/IP Unit and examples of communications error are shown below.
For information about the meaning of error level, refer to the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)*.

Level	Error source	
	X Bus Ethernet Function Module	X Bus EtherNet/IP Function Module
Major fault	None	None
Partial fault	None	None
Minor fault	• MAC Address Error • Communications Controller Error • Basic Ethernet Setting Error • IP Address Setting Error • IP Address Duplication Error • BOOTP Server Connection Error • DNS Setting Error • IP Router Table Setting Error • SNMP Setting Error • Ethernet Processing Error	• Identity Error • Tag Data Link Setting Error • Tag Data Link Connection Failed • Tag Name Resolution Error • Tag Data Link Timeout • Tag Data Link Connection Timeout • Allowed Communications Bandwidth per Unit Exceeded • Number of Tag Sets for Tag Data Links Exceeded
Observation	• Packet Discarded Due to Full Reception Buffer • Link OFF Detected	• Unit Configuration Error, Combined Use of CIP Safety and Tag Data Link • Access Detected Outside Range of Variable
Information	• Link Detected • IP Address Fixed • BOOTP Client Started • SNMP Started • IP Address Changed • SNMP Settings Changed • Subnet Mask Changed	• Tag Data Link Download Started • Tag Data Link Download Finished • Tag Data Link Stopped • Tag Data Link Started • Tag Data Link All Run • Restarting Ethernet Port

In addition, the behaviors of the NX-series EtherNet/IP Unit to the source of communications error when each level of error occurred are as shown below.

Level	Error source	
	X Bus Ethernet Function Module	X Bus EtherNet/IP Function Module
Major fault	None	None

Level	Error source	
	X Bus Ethernet Function Module	X Bus EtherNet/IP Function Module
Partial fault	None	None
Minor fault	• Ethernet communications stop (online connection with the Sysmac Studio and communication with an HMI are not possible). • Ethernet communications partially stop (if the error is caused by communications other than connection with the Sysmac Studio or an HMI, online connection with the Sysmac Studio and communication with an HMI are possible).	• EtherNet/IP communications stop. • EtherNet/IP communications partially stop.
Observation	Ethernet communications continue.	EtherNet/IP communications continue.
Information	Ethernet communications continue.	EtherNet/IP communications continue.

Additional Information

For the behaviors of the X Bus Unit and the X Bus Unit Common Function Module for each level of error, refer to *Operation Related to the X Bus Unit* in the appendix of the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)*.

14-4-3 Error Tables

This section provides tables of errors (events) that occur on the NX-series EtherNet/IP Unit. The following abbreviations and symbols are used for Level, which means the severity level of the event.

Abbreviation	Name
Min	Minor fault level
Obs	Observation
Info	Information

Symbol	Meaning
○	Event levels that are defined by the system.
8	Event levels that can be changed by the user. [*1]

[*1] This symbol is used only for the event whose level can be changed.

For all event codes of NJ/NX-series Controllers, refer to the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)*.

X Bus Ethernet Function Module

This section provides the list of errors (events) related to the X Bus Ethernet Function Module.

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
04310000 hex	Communications Controller Error	A hardware error was detected in the Communications Controller of the EtherNet/IP port.	• Hardware failure of Communications Controller			○			page 14-16
14310000 hex	MAC Address Error	MAC address in non-volatile memory could not be read correctly.	• Non-volatile memory failure			○			page 14-17
14340000 hex	Ethernet Processing Error	A fatal error was detected in the Ethernet Function Module.	• Hardware failure			○			page 14-17
36010000 hex	Basic Ethernet Setting Error	An Ethernet setting error was detected.	• Parameter error • Power interruption while downloading EtherNet/IP port settings • Memory error			○			page 14-18
36020000 hex	IP Address Setting Error	An IP address setting error was detected.	• Parameter error • Power interruption while downloading EtherNet/IP port settings • The IP address obtained from the BOOTP server is invalid. • Memory error			○			page 14-19
36030000 hex	IP Router Table Setting Error	An error was detected in the IP routing function settings.	• Parameter error • Power interruption while downloading EtherNet/IP port settings • Memory error			○			page 14-20
36060000 hex	SNMP Setting Error	A setting error in SNMP agent/trap was detected.	• Parameter error • Power interruption while downloading SNMP agent/trap settings • Memory error			○			page 14-21
36080000 hex	DNS Setting Error	Errors were detected in DNS setting and Hosts setting.	• Parameter error • Power interruption while downloading EtherNet/IP port settings • Memory error			○			page 14-22
85D00000 hex	IP Address Duplication Error	The same IP address is used more than once.	• The IP address of the EtherNet/IP port is duplicated with the IP address of another node.			○			page 14-23
85D10000 hex	BOOTP Server Connection Error	Connection with the BOOTP server failed.	• The server is misconfigured. • The server went down. • An error occurred in the communications path.			○			page 14-24

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
85D40000 hex	Packet Discarded Due to Full Reception Buffer	A packet drop occurred.	• Network congestion occurred.				○		page 14-25
85D50000 hex	Link OFF Detected	An Ethernet link OFF was detected.	• An Ethernet cable is broken, disconnected, or loose. • The Ethernet switch's power supply is turned OFF. • Communications speed mismatched. • Noise • The identity object was reset. • Settings for EtherNet/IP were downloaded from the Network Configurator or Sysmac Studio, or the Clear All Memory operation was performed. • EtherNet/IP was restarted.				○		page 14-26
96440000 hex	Link Detected	Establishment of an Ethernet link was detected.	• Establishment of an Ethernet link was detected.					○	page 14-27
96470000 hex	IP Address Fixed	The correct IP address has been determined and Ethernet communications can start.	• The correct IP address has been determined and Ethernet communications can start.					○	page 14-27
96480000 hex	BOOTP Client Started	The BOOTP client started requesting an IP address.	• The BOOTP client started requesting an IP address.					○	page 14-28
964B0000 hex	SNMP Started	The SNMP agent started normally.	• The SNMP agent started normally.					○	page 14-28
96500000 hex	IP Address Changed	The IP address was changed.	• The IP address was changed.					○	page 14-29
96510000 hex	SNMP Settings Changed	The SNMP settings were changed.	• The SNMP settings were changed.					○	page 14-30
96520000 hex	Subnet Mask Changed	The subnet mask setting was changed.	• The subnet mask setting was changed.					○	page 14-31

X Bus EtherNet/IP Function Module

This section provides the list of errors (events) related to the X Bus EtherNet/IP Function Module.

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
14210000 hex	Identity Error	The CIP identity information in non-volatile memory was not read correctly.	• Non-volatile memory failure			○			page 14-32
34200000 hex	Tag Data Link Setting Error	An error was detected in the communications settings for tag data links.	• Power was interrupted when a download was in progress for the tag data link settings. • Memory error			○			page 14-33
34270000 hex	Tag Name Resolution Error	Resolution of a tag used in a tag data link failed.	• The size of the network variable is different from the tag settings. • The I/O direction that is set in the tag data link settings does not agree with the I/O direction of the variable in the Controller. • There is no network variable in the Controller that corresponds to the tag settings. • A variable in the Controller that is set for a tag data link has the Network Publish attribute set to Input but also has the Constant attribute.			○			page 14-34
84070000 hex	Tag Data Link Connection Failed	Establishing a tag data link connection failed.	• The tag data link connection information is not the same for the originator and target. • Insufficient connections • CIP message communications at the target node are stopped. • Setting to use tag data link communications was made to the NX-series EtherNet/IP Unit that is included in the CIP Safety connection settings. • The NX-series EtherNet/IP Unit with tag data link communications was added to the CIP Safety connection settings.			○			page 14-35

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
84080000 hex	Tag Data Link Timeout	A timeout occurred in a tag data link.	• The power supply to the target node is OFF. • Communications with the target node stopped. • The Ethernet cable connector for EtherNet/IP is disconnected. • The Ethernet cable for EtherNet/IP is broken. • The link to the EtherNet/IP port is OFF. • CIP message communications at the target node are stopped. • When the Packet Filter function is enabled in the EtherNet/IP Port Settings, packets from the target are not allowed. • CIP communications are not allowed by the firewall function or Packet Filter function on the target node or the devices on the communication path. • The packet loss occurred on the path due to the network communications load. • Noise			○			page 14-36
84090000 hex	Tag Data Link Connection Timeout	A timeout occurred while trying to establish a tag data link connection.	• The power supply to the target node is OFF. • Communications with the target node stopped. • CIP message communications stopped at the target node or the EtherNet/IP port. • The Ethernet cable connector for EtherNet/IP is disconnected. • The Ethernet cable for EtherNet/IP is broken. • CIP communications are not allowed by the firewall function or Packet Filter function on the target node or the devices on the communication path. • An error occurred in the communications path.			○			page 14-38

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
840C0000 hex	Allowed Communications Bandwidth per Unit Exceeded	The total bandwidth for the connections that are set or established for all of the EtherNet/IP ports exceeded the allowed communications bandwidth of tag data links and CIP Safety communications per Unit.	• An attempt was made to establish a connection of communications bandwidth (PPS), which is the sum of the packet transmission rates of the tag data links and CIP Safety communications used for all EtherNet/IP ports, and it exceeded the allowable communications bandwidth of the Unit.			○			page 14-39
840E0000 hex	Number of Tag Sets for Tag Data Links Exceeded	The total number of tag sets for tag data links for all Ethernet/IP ports exceeds the upper limit.	• The total number of tag sets for all ports that are set for tag data links in each Ethernet/IP port exceeded the maximum number the product allows.			○			page 14-40
342C0000 hex	Unit Configuration Error, Combined Use of CIP Safety and Tag Data Link	Tag data link communications and CIP Safety communications cannot be used together in one NX-series EtherNet/IP Unit.	• Setting to use tag data link communications was made to the NX-series EtherNet/IP Unit that is included in the CIP Safety connection settings. • The NX-series EtherNet/IP Unit with tag data link communications was added to the CIP Safety connection settings.				○		page 14-41
54E00000 hex	Access Detected Outside Range of Variable	An access attempt to write a value out of range was detected for a tag variable that is used in a tag data link.	• An out-of-range value was written by an EtherNet/IP tag data link to a variable with range specification. A value that does not specify an enumerator was written by an EtherNet/IP tag data link to an enumeration variable.				○		page 14-42
94010000 hex	Tag Data Link Download Started	Changing the tag data link settings started.	• Changing the tag data link settings started.					○	page 14-42
94020000 hex	Tag Data Link Download Finished	Changing the tag data link settings finished.	• Changing the tag data link settings finished.					○	page 14-43
94030000 hex	Tag Data Link Stopped	Tag data links were stopped by the Network Configurator, Sysmac Studio, special instructions or manipulation of a system-defined variable. Or, the data link table was downloaded from Network Configurator or Sysmac Studio.	• Tag data links were stopped by the Network Configurator, Sysmac Studio, special instructions or manipulation of a system-defined variable.					○	page 14-43

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
94040000 hex	Tag Data Link Started	Tag data links were started by the Network Configurator, Sysmac Studio, special instructions or manipulation of a system-defined variable. Or, the data link table was downloaded from Network Configurator or Sysmac Studio.	• Tag data links were started by the Network Configurator, Sysmac Studio, special instructions or manipulation of a system-defined variable.					○	page 14-44
94070000 hex	Tag Data Link All Run	Tag data link connections to all nodes have been normally established.	• Tag data link connections to all target nodes have been normally established.					○	page 14-45
96450000 hex	Restarting Ethernet Port	The EtherNet/IP port was restarted.	• The EtherNet/IP port was restarted.					○	page 14-45

14-4-4 Error Details

This section provides detailed information on errors (events) that occur on the NX-series EtherNet/IP Unit.

Interpreting Error Descriptions

The items that are used to describe individual errors (events) are described in the following copy of an error table.

<table>
<tr><td><b>Event name</b></td><td colspan="3">Gives the name of the error.</td><td><b>Event code</b></td><td colspan="2">Gives the code of the error.</td></tr>
<tr><td><b>Meaning</b></td><td colspan="6">Gives a short description of the error.</td></tr>
<tr><td><b>Source</b></td><td colspan="2">Gives the source of the error.</td><td><b>Source details</b></td><td>Gives details on the source of the error.</td><td><b>Detection timing</b></td><td>Tells when the error is detected.</td></tr>
<tr><td><b>Error attributes</b></td><td><b>Level</b></td><td>Tells the level of influence on control. [1]</td><td><b>Recovery</b></td><td>Gives the method to return to normal state after eliminating the cause of the error.</td><td><b>Log category</b></td><td>Tells which log the error is saved in. [2]</td></tr>
<tr><td><b>Effects</b></td><td><b>User program</b></td><td>Tells what will happen to execution of the user program. [3]</td><td><b>Operation</b></td><td colspan="3">Provides special information on the operation that results from the error.</td></tr>
<tr><td><b>Indicators</b></td><td colspan="6">Gives the status you can check with the EtherNet/IP port indicators.</td></tr>
</table>

Device variable	**Variable**	**Data type**	**Name**
	Lists the variable names and data types for device variables that provide direct error notification, that are directly affected by the error, or that contain settings that cause the error.		
Cause and correction	**Assumed cause**	**Correction**	**Prevention**
	Lists the possible causes, corrections, and preventive measures for the error.		
Attached information	This is the attached information that is displayed by the Sysmac Studio or an HMI. [*4]		
Precautions/ Remarks	Provides precautions, restrictions, and supplemental information. If the user can set the event level, the event levels that can be set, the recovery method, operational information, and other information is also provided.		
User name in the access log	Provides the name of the user who performed the operation that generates the access log. This information is provided only for errors (events) for which the user name is recorded in the access log.		

*1. One of the following:
Minor fault: Minor fault level
Observation
Information

*2. One of the following:
System: System event log
Access: Access event log

*3. One of the following:
Continues: Execution of the user program will continue.
Stops: Execution of the user program stops.
Starts: Execution of the user program starts.

*4. Refer to *Applicable Range of the HMI Troubleshooter* of the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* for the applicable range of the HMI Troubleshooter.

X Bus Ethernet Function Module

This section provides detailed information on errors (events) related to the X Bus Ethernet Function Module.

Event name	Communications Controller Error			**Event code**	04310000 hex	
Meaning	A hardware error was detected in the Communications Controller of the Ethernet port.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *communications port 1/ communications port 2* are given in combination	**Detection timing**	Continuously
Error attributes	**Level**	Minor fault	**Recovery**	Cycle the power supply.	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Ethernet communications are not possible for the relevant communications port.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	OFF		Lights.		---	
Device variable	**Variable**		**Data type**		**Name**	
	ETN_Port1Status.LanHwErr		BOOL		Port1 Communications Controller Error	
	ETN_Port2Status.LanHwErr		BOOL		Port2 Communications Controller Error	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Hardware failure of Communications Controller		Replace the Unit.		None	
Attached information	None					
Precautions/ Remarks	Once the device variable ETN_Port1Status.LanHwErr or ETN_Port2Status.LanHwErr becomes TRUE, it will not become FALSE unless the Controller power is turned OFF and then ON.					

Event name	MAC Address Error			**Event code**	14310000 hex	
Meaning	MAC address in non-volatile memory could not be read correctly.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *communications port 1/ communications port 2* are given in combination	**Detection timing**	At power ON or Controller reset
Error attributes	**Level**	Minor fault	**Recovery**	Cycle the power supply.	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Ethernet communications are not possible for the relevant communications port.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	OFF		Lights.		---	
Device variable	**Variable**		**Data type**		**Name**	
	ETN_Port1Status.MacAdrErr		BOOL		Port1 MAC Address Error	
	ETN_Port2Status.MacAdrErr		BOOL		Port2 MAC Address Error	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Non-volatile memory failure		Replace the Unit.		None	
Attached information	None					
Precautions/ Remarks	Once the device variable ETN_Port1Status.MacAdrErr or ETN_Port2Status.MacAdrErr becomes TRUE, it will not become FALSE unless the Controller power is turned OFF and then ON.					

Event name	Ethernet Processing Error			**Event code**	14340000 hex	
Meaning	A fatal error was detected in the Ethernet Function Module.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *communications port* are given in combination	**Detection timing**	Continuously
Error attributes	**Level**	Minor fault	**Recovery**	Cycle the power supply.	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Ethernet communications are not possible.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	OFF		Lights.		---	
Device variable	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Hardware failure		Replace the Unit.		None	
Attached information	None					
Precautions/ Remarks	None					

Event name	Basic Ethernet Setting Error			**Event code**	36010000 hex	
Meaning	An Ethernet setting error was detected.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *communications port 1/ communications port 2* are given in combination	**Detection timing**	At power ON or Controller reset
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery, cycle the power supply, or Controller reset	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Ethernet communications are not possible for the relevant communications port.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	OFF		Flashes at 1-s intervals.		---	
Device variable	**Variable**		**Data type**		**Name**	
	ETN_Port1Status.EtnCfgErr		BOOL		Port1 Basic Ethernet Setting Error	
	ETN_Port2Status.EtnCfgErr		BOOL		Port2 Basic Ethernet Setting Error	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Parameter error		Identify the cause of the error from the attached information, correct the settings, and then download the settings again.		None	
	Power interruption while downloading Ethernet port settings		Please clear all memory or download the settings.		Do not turn OFF the power supply to the Controller while downloading the Ethernet port settings.	
	Memory error		If the above measures do not work, replace the Unit.		None	
Attached information	Attached information 1: Error type 01 hex: Non-volatile Memory Access Error, 02 hex: There is an inconsistency in the set values. Attached information 2: Error Details 00 hex: Non-volatile memory access error, 11 hex: Invalid communications speed setting, 12 hex: Unsupported communications speed					
Precautions/ Remarks	None					

Event name	IP Address Setting Error			**Event code**	36020000 hex	
Meaning	An IP address setting error was detected.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *communications port 1/ communications port 2* are given in combination	**Detection timing**	At power ON or Controller reset
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery (after downloading the settings), cycle the power supply, or Controller reset	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Ethernet communications are not possible for the relevant communications port.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	OFF		Flashes at 1-s intervals.		---	
Device variable	**Variable**		**Data type**		**Name**	
	ETN_Port1Status.IPAdrCfgErr		BOOL		Port1 IP Address Setting Error	
	ETN_Port2Status.IPAdrCfgErr		BOOL		Port2 IP Address Setting Error	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Parameter error		Identify the cause of the error from the attached information, correct the settings, and then download the settings again.		None	
	Power interruption while downloading Ethernet port settings		Clear all memory or download the settings again.		Do not turn OFF the power supply to the Controller while downloading the Ethernet port settings.	
	The IP address obtained from the BOOTP server is invalid.		Correct the IP address setting provided by the BOOTP server to this port within the range specified for the NX-series Controller.		Set the IP address provided by the BOOTP server to this port within the range specified for the NX-series Controller.	
	Memory error		If the above measures do not work, replace the Unit.		None	
Attached information	Attached information 1: Error type 01 hex: Non-volatile Memory Access Error, 02 hex: There is an inconsistency in the set values. Attached information 2: Error Details 00 hex: Non-volatile memory access error If there is an inconsistency in the set values: 11 hex: Illegal IP address, 12 hex: Illegal subnet mask, 13 hex: Invalid default gateway, 14 hex: Preferred DNS setting error, 15 hex: Alternate DNS setting error, 16 hex: Illegal domain name, 17 hex: Illegal X Bus network address					
Precautions/ Remarks	None					

Event name	IP Router Table Setting Error			**Event code**	36030000 hex	
Meaning	An error was detected in the IP routing function settings.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *communications port* are given in combination	**Detection timing**	At power ON or Controller reset
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery (after downloading the settings), cycle the power supply, or Controller reset	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Communications that use the relevant IP routing settings are not possible.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	---		Flashes at 1-s intervals.		---	
Device variable	**Variable**		**Data type**		**Name**	
	ETN_IPRTblErr		BOOL		IP Router Table Setting Error	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Parameter error		Identify the cause of the error from the attached information, correct the settings, and then download the settings again.		None	
	Power interruption while downloading EtherNet/IP port settings		Clear all memory or download the settings again.		Do not turn OFF the power supply to the Controller while downloading the EtherNet/IP port settings.	
	Memory error		If the above measures do not work, replace the Unit.		None	
Attached information	Attached information 1: Error type 01 hex: Non-volatile Memory Access Error, 02 hex: There is an inconsistency in the set values. Attached information 2: Error Details 00 hex: Non-volatile memory access error If there is an inconsistency in the set values: 11 hex: Illegal IP router table settings, 12 hex: Illegal hosts settings, 13 hex: Invalid default gateway, 14 hex: Illegal IP Forward settings, 15 hex: Illegal NAT settings, 16 hex: Illegal Packet Filter settings, 17 hex: Illegal TCP/UDP Port Transfer settings					
Precautions/ Remarks	None					

Event name	SNMP Setting Error			**Event code**	36060000 hex	
Meaning	A setting error in SNMP agent/trap was detected.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *SNMP* are given in combination	**Detection timing**	At power ON or Controller reset
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery (after downloading the SNMP settings), cycle the power supply, or Controller reset	**Log category**	System
Effects	**User program**	Continues.	**Operation**	SNMP operation stops.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	---		Flashes at 1-s intervals.		---	
Device variable	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Parameter error		Identify the cause of the error from the attached information, correct the settings, and then download the settings again.		None	
	Power interruption while downloading SNMP agent/trap settings		Clear all memory or download the settings again.		Do not turn OFF the power supply to the Controller while the SNMP agent/trap settings are being downloaded.	
	Memory error		If the above measures do not work, replace the Unit.		None	
Attached information	Attached information 1: Error type 01 hex: Non-volatile Memory Access Error, 02 hex: There is an inconsistency in the set values. Attached information 2: Error Location If there is an inconsistency in the set values: 01 hex: SNMP agent settings, 02 hex: SNMP trap settings					
Precautions/ Remarks	None					

Event name	DNS Setting Error			**Event code**	36080000 hex	
Meaning	Errors were detected in DNS setting and Hosts setting.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *communications port* are given in combination	**Detection timing**	At power ON or Controller reset
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery (after downloading the settings), cycle the power supply, or Controller reset	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Ethernet communications are not possible.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	OFF		Flashes at 1-s intervals.		---	
Device variable	**Variable**		**Data type**		**Name**	
	ETN_DNSCfgErr		BOOL		DNS Setting Error	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Parameter error		Identify the cause of the error from the attached information, correct the settings, and then download the settings again.		None	
	Power interruption while downloading Ethernet port settings		Clear all memory or download the settings again.		Do not turn OFF the power supply to the Controller while downloading the Ethernet port settings.	
	Memory error		If the above measures do not work, replace the Unit.		None	
Attached information	Attached information 1: Error type 01 hex: Non-volatile Memory Access Error, 02 hex: There is an inconsistency in the set values. Attached information 2: Error Details 00 hex: Non-volatile memory access error If there is an inconsistency in the set values: 14 hex: Preferred DNS setting error, 15 hex: Alternate DNS setting error, 16 hex: Illegal domain name, 17 hex: Illegal hosts settings					
Precautions/ Remarks	None					

Event name	IP Address Duplication Error			**Event code**	85D00000 hex	
Meaning	The same IP address is used more than once.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *communications port 1/ communications port 2* are given in combination	**Detection timing**	Continuously after link establishment
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery (after downloading the IP address settings), cycle the power supply, or Controller reset	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Ethernet communications are not possible for the relevant communications port. Packets addressed to the local IP address of the relevant communications port are discarded.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	OFF		Flashes at 1-s intervals.		---	
Device variable	**Variable**		**Data type**		**Name**	
	ETN_Port1Status.IPAdrDupErr		BOOL		Port1 IP Address Duplication Error	
	ETN_Port2Status.IPAdrDupErr		BOOL		Port2 IP Address Duplication Error	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The IP address of the Ethernet port is duplicated with the IP address of another node.		Perform either of the following corrections. • Check the IP addresses of other nodes and correct the IP address settings so that the same address is not used by more than one node. • Remove the other node that has the duplicate IP address from the network and then cycle the power supply to the Controller or reset the Controller.		Perform allocations so that IP addresses of nodes on the network are used for only one node.	
Attached information	Attached information 1: Duplicated IP address (example: C0A8FA01 hex = address 192.168.250.1)					
Precautions/ Remarks	A duplicated address error occurs if an ARP is sent with the set IP address and there is an ARP response.					

Event name	BOOTP Server Connection Error			**Event code**	85D10000 hex	
Meaning	Connection with the BOOTP server failed.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *communications port 1/ communications port 2* are given in combination	**Detection timing**	During BOOTP operation
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Ethernet communications are not possible for the relevant communications port. Requests to the BOOTP server will continue until there is a response from the BOOTP server. Data refreshing with the PLC Function Module will continue. An IP address was not set for the Ethernet port for which the BOOTP server attempted to set an IP address.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	OFF		Flashes at 1-s intervals.		---	
Device variable	**Variable**		**Data type**		**Name**	
	ETN_Port1Status.BootpErr		BOOL		Port1 BOOTP Server Error	
	ETN_Port2Status.BootpErr		BOOL		Port2 BOOTP Server Error	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The server is misconfigured.		Correct the server settings at the remote connection.		Check to make sure that the server settings at the remote connection are correct.	
	The server went down.		Check if the server at the remote connection is operating normally and set it to operate normally if it is not.		Check to make sure that the server at the remote connection is operating normally.	
	An error occurred in the communications path.		Check the communications path to the server and take corrective measures if there are any problems.		None	
Attached information	None					
Precautions/ Remarks	None					

Event name	Packet Discarded Due to Full Reception Buffer			**Event code**	85D40000 hex	
Meaning	A packet drop occurred.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *communications port 1/ communications port 2* are given in combination	**Detection timing**	After link is established
Error attributes	**Level**	Observation	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Not affected.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	---		---		---	
Device variable	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Network congestion occurred.		The load on the network is too high. Check whether there are nodes that send unnecessary broadcast frames on the network and remove them. After that, check that the received number of frames has reduced in the network statistical information.		Make sure that unnecessary broadcast frames are not sent on the network. Do not connect the Ethernet cable in a loop.	
Attached information	None					
Precautions/ Remarks	None					

Event name	Link OFF Detected			**Event code**	85D50000 hex	
Meaning	An Ethernet link OFF was detected.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *communications port 1*/*communications port 2* are given in combination	**Detection timing**	Continuously
Error attributes	**Level**	Observation	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Ethernet communications are not possible.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	---		---		OFF	
Device variable	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	An Ethernet cable is broken, disconnected, or loose.		Firmly connect the Ethernet cable. Replace the cable if it is broken.		Firmly connect the Ethernet cable. Also, make sure that the cable to be used is not disconnected.	
	The Ethernet switch's power supply is turned OFF.		Turn ON the power supply to the Ethernet switch. Replace the Ethernet switch if it fails.		Do not turn OFF the Ethernet switch.	
	Communications speed mismatched.		Please modify the setting so that the communication speed is the same as that of the remote node.		Set the same communication speed as that on the remote node.	
	Noise		Implement noise countermeasures if there is excessive noise.		Implement the noise countermeasures.	
	One of the following operations was performed. • The identity object was reset. • Settings for Ethernet were downloaded from the Network Configurator or Sysmac Studio, or the Clear All Memory operation was performed. • Ethernet port was restarted.		None. This error occurs when the operations on the left are performed.		None. This error occurs when the operations on the left are performed.	
Attached information	None					
Precautions/ Remarks	None					

Event name	Link Detected			**Event code**	96440000 hex	
Meaning	Establishment of an Ethernet link was detected.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *communications port 1/ communications port 2* are given in combination	**Detection timing**	When a link is established
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Not affected.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	---		---		Lights.	
Device variable	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Establishment of an Ethernet link was detected.		---		---	
Attached information	None					
Precautions/ Remarks	None					

Event name	IP Address Fixed			**Event code**	96470000 hex	
Meaning	The correct IP address has been determined and Ethernet communications can start.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *communications port 1/ communications port 2* are given in combination	**Detection timing**	At power ON or Controller reset
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Not affected.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	Lights.		---		---	
Device variable	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The correct IP address has been determined and Ethernet communications can start.		---		---	
Attached information	Attached information 1: IP address (example: C0A8FA01 hex = address 192.168.250.1)					
Precautions/ Remarks	None					

Event name	BOOTP Client Started			**Event code**	96480000 hex	
Meaning	The BOOTP client started requesting an IP address.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *communications port 1/communications port 2* are given in combination	**Detection timing**	At power ON or Controller reset
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Not affected.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	---		---		---	
Device variable	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The BOOTP client started requesting an IP address.		---		---	
Attached information	None					
Precautions/ Remarks	None					

Event name	SNMP Started			**Event code**	964B0000 hex	
Meaning	The SNMP agent started normally.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *SNMP* are given in combination	**Detection timing**	At power ON or Controller reset
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Not affected.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	---		---		---	
Device variable	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The SNMP agent started normally.		---		---	
Attached information	None					
Precautions/ Remarks	None					

Event name	IP Address Changed			**Event code**	96500000 hex	
Meaning	The IP address was changed.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *communications port 1/ communications port 2* are given in combination	**Detection timing**	When downloaded
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Not affected.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	---		---		---	
Device variable	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The IP address was changed.		---		---	
Attached information	Attached information 1: IP address after change, e.g. 192.168.250.1					
Precautions/ Remarks	None					

Event name	SNMP Settings Changed			**Event code**	96510000 hex	
Meaning	The SNMP settings were changed.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *SNMP* are given in combination	**Detection timing**	When downloaded
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Not affected.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	---		---		---	
Device variable	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The SNMP settings were changed.		---		---	
Attached information	Attached information 1: Changes in SNMP Service • 1: SNMP service enabled • 2: SNMP service disabled • 3: SNMP service settings changed • 4: No change (Not 1, 2, or 3) Attached information 2: Changes in Recognition 1 • 1: Recognition 1 enabled • 2: Recognition 1 disabled • 3: Recognition 1 settings changed • 4: No change (Not 1, 2, or 3) Attached information 3: Changes in Recognition 2 • 1: Recognition 2 enabled • 2: Recognition 2 disabled • 3: Recognition 2 settings changed • 4: No change (Not 1, 2, or 3)					
Precautions/ Remarks	None					

Event name	Subnet Mask Changed			**Event code**	96520000 hex	
Meaning	The subnet mask was changed.					
Source	X Bus Ethernet Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *communications port 1/ communications port 2* are given in combination	**Detection timing**	When downloaded
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Not affected.		
Indicators	**Ethernet NET RUN**		**Ethernet NET ERR**		**Ethernet LINK/ACT**	
	---		---		---	
Device variable	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The subnet mask was changed.		---		---	
Attached information	Attached information 1: Subnet mask after change, e.g. 255.255.255.0					
Precautions/ Remarks	None					

X Bus EtherNet/IP Function Module

This section provides detailed information on errors (events) related to the X Bus EtherNet/IP Function Module.

<table>
<tr><td><b>Event name</b></td><td colspan="3">Identity Error</td><td><b>Event code</b></td><td colspan="2">14210000 hex</td></tr>
<tr><td><b>Meaning</b></td><td colspan="6">The CIP identity information in non-volatile memory was not read correctly.</td></tr>
<tr><td><b>Source</b></td><td colspan="2">X Bus EtherNet/IP Function Module</td><td><b>Source details</b></td><td><i>1 to 4: Mounting position of the X Bus Unit (unit number)</i> and <i>CIP1/CIP2</i> are given in combination</td><td><b>Detection timing</b></td><td>At power ON or Controller reset</td></tr>
<tr><td><b>Error attributes</b></td><td><b>Level</b></td><td>Minor fault</td><td><b>Recovery</b></td><td>Cycle the power supply.</td><td><b>Log category</b></td><td>System</td></tr>
<tr><td><b>Effects</b></td><td><b>User program</b></td><td>Continues.</td><td><b>Operation</b></td><td colspan="3">EtherNet/IP communications are not possible for the relevant communications port.</td></tr>
<tr><td rowspan="2"><b>Indicators</b></td><td colspan="2"><b>EtherNet/IP NET RUN</b></td><td colspan="2"><b>EtherNet/IP NET ERR</b></td><td colspan="2"><b>EtherNet/IP LINK/ACT</b></td></tr>
<tr><td colspan="2">---</td><td colspan="2">Lights.</td><td colspan="2">---</td></tr>
<tr><td rowspan="3"><b>Device variable</b></td><td colspan="2"><b>Variable</b></td><td colspan="2"><b>Data type</b></td><td colspan="2"><b>Name</b></td></tr>
<tr><td colspan="2">EIP_Comm1Status.IdentityErr</td><td colspan="2">BOOL</td><td colspan="2">CIP Communications1 Identity Error</td></tr>
<tr><td colspan="2">EIP_Comm2Status.IdentityErr</td><td colspan="2">BOOL</td><td colspan="2">CIP Communications2 Identity Error</td></tr>
<tr><td rowspan="2"><b>Cause and correction</b></td><td colspan="2"><b>Assumed cause</b></td><td colspan="2"><b>Correction</b></td><td colspan="2"><b>Prevention</b></td></tr>
<tr><td colspan="2">Non-volatile memory failure</td><td colspan="2">Replace the CPU Unit.</td><td colspan="2">None</td></tr>
<tr><td><b>Attached information</b></td><td colspan="6">None</td></tr>
<tr><td><b>Precautions/ Remarks</b></td><td colspan="6">None</td></tr>
</table>

Event name	Tag Data Link Setting Error			**Event code**	34200000 hex	
Meaning	An error was detected in the communications settings for tag data links.					
Source	X Bus EtherNet/IP Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *CIP1/CIP2* are given in combination	**Detection timing**	At power ON or Controller reset
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery (after downloading the tag data link settings), cycle the power supply, or Controller reset	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Tag data link communications are not possible.		
Indicators	**EtherNet/IP NET RUN**		**EtherNet/IP NET ERR**		**EtherNet/IP LINK/ACT**	
	Flashes at 1-s intervals.		Flashes at 1-s intervals.		---	
Device variable	**Variable**		**Data type**		**Name**	
	EIP_Comm1Status.TDLinkCfgErr		BOOL		CIP Communications1 Tag Data Link Setting Error	
	EIP_Comm2Status.TDLinkCfgErr		BOOL		CIP Communications2 Tag Data Link Setting Error	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Power was interrupted when a download was in progress for the tag data link settings.		Please perform one of the following corrections. • Execute Clear All Memory operation. • Download the tag data link settings. • Clear the tag data link settings.		Do not turn OFF the power supply to the Controller while downloading the tag data link settings.	
	Memory error		If the above measures do not work, replace the CPU Unit.		None	
Attached information	Attached information 1: Error type 01 hex: Non-volatile Memory Access Error, 02 hex: There is an inconsistency in the set values.					
Precautions/ Remarks	None					

Event name	Tag Name Resolution Error			**Event code**	34270000 hex	
Meaning	Resolution of a tag used in a tag data link failed.					
Source	X Bus EtherNet/IP Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *CIP1/CIP2* are given in combination	**Detection timing**	At power ON, Controller reset, changing variable values from the Sysmac Studio, or changing data link table from the Network Configurator
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery (after downloading tag settings)	**Log category**	System
Effects	**User program**	Continues.	**Operation**	The data link does not operate for the tag whose errors were not resolved. Data links for other tags operate.		
Indicators	**EtherNet/IP NET RUN**		**EtherNet/IP NET ERR**		**EtherNet/IP LINK/ACT**	
	Flashes at 1-s intervals.		Flashes at 1-s intervals.		---	
Device variable	**Variable**		**Data type**		**Name**	
	EIP_Comm1Status.TagAdrErr		BOOL		CIP Communications1 Tag Name Resolution Error	
	EIP_Comm2Status.TagAdrErr		BOOL		CIP Communications2 Tag Name Resolution Error	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The size of the network variable is different from the tag settings.		Modify the size of the tag settings to match the network variable.		Set the size of the tag settings to match the network variable.	
	The I/O direction that is set in the tag data link settings does not agree with the I/O direction of the variable in the Controller.		Modify the tag settings or Controller variable settings so that the I/O direction of the tag data link settings and the Controller variable match.		Set the tag settings or Controller variable so that the I/O direction of the tag data link setting agree with the I/O direction of the Controller variable.	
	There is no network variable in the Controller that corresponds to the tag settings.		Modify the tag settings to specify existing network variable in the tag.		Set the tag to specify an existing network variable.	
	A variable in the Controller that is set for a tag data link has the Network Publish attribute set to **Input** but also has the Constant attribute.		Remove the Constant attribute of the Controller variable whose Network Publish attribute is set to **Input**.		Do not set the Constant attribute in the Controller variable whose Network Publish attribute is set to **Input**.	
Attached information	None					
Precautions/ Remarks	None					

<table>
<tr><td><b>Event name</b></td><td colspan="3">Tag Data Link Connection Failed</td><td><b>Event code</b></td><td colspan="2">84070000 hex</td></tr>
<tr><td><b>Meaning</b></td><td colspan="6">Establishing a tag data link connection failed.</td></tr>
<tr><td><b>Source</b></td><td colspan="2">X Bus EtherNet/IP Function Module</td><td><b>Source details</b></td><td><i>1 to 4: Mounting position of the X Bus Unit (unit number)</i> and <i>CIP1/CIP2</i> are given in combination</td><td><b>Detection timing</b></td><td>When establishing a tag data link connection</td></tr>
<tr><td><b>Error attributes</b></td><td><b>Level</b></td><td>Minor fault</td><td><b>Recovery</b></td><td>Automatic recovery</td><td><b>Log category</b></td><td>System</td></tr>
<tr><td><b>Effects</b></td><td><b>User program</b></td><td>Continues.</td><td><b>Operation</b></td><td colspan="3">The data link does not operate for a connection that failed to establish a connection. Data links on other connection operate.</td></tr>
<tr><td rowspan="2"><b>Indicators</b></td><td colspan="2"><b>EtherNet/IP NET RUN</b></td><td colspan="2"><b>EtherNet/IP NET ERR</b></td><td colspan="2"><b>EtherNet/IP LINK/ACT</b></td></tr>
<tr><td colspan="2">Flashes at 1-s intervals.</td><td colspan="2">Flashes at 1-s intervals.</td><td colspan="2">---</td></tr>
<tr><td rowspan="3"><b>Device variable</b></td><td colspan="2"><b>Variable</b></td><td colspan="2"><b>Data type</b></td><td colspan="2"><b>Name</b></td></tr>
<tr><td colspan="2">EIP_Comm1Status.TDLinkOpnErr</td><td colspan="2">BOOL</td><td colspan="2">CIP Communications1 Tag Data Link Connection Failed</td></tr>
<tr><td colspan="2">EIP_Comm2Status.TDLinkOpnErr</td><td colspan="2">BOOL</td><td colspan="2">CIP Communications2 Tag Data Link Connection Failed</td></tr>
<tr><td rowspan="6"><b>Cause and correction</b></td><td colspan="2"><b>Assumed cause</b></td><td colspan="2"><b>Correction</b></td><td colspan="2"><b>Prevention</b></td></tr>
<tr><td colspan="2">The tag data link connection information is not the same for the originator and target.</td><td colspan="2">Modify connection information of the tag data link and download the device parameter or connection settings from Network Configurator or Sysmac Studio.</td><td colspan="2">Before starting the tag data link, match the connection information for the tag data link in the originator and target.</td></tr>
<tr><td colspan="2">Insufficient connections</td><td colspan="2">Please reduce class-3 messages.</td><td colspan="2">Please reduce the number of data link and class-3 messages used.</td></tr>
<tr><td colspan="2">CIP message communications at the target node are stopped.</td><td colspan="2">Make the device start normal CIP message communications.</td><td colspan="2">Start CIP message communications successfully and then perform tag data links.</td></tr>
<tr><td colspan="2">Setting to use tag data link communications was made to the NX-series EtherNet/IP Unit that is included in the CIP Safety connection settings.</td><td colspan="2">Do not configure the NX-series EtherNet/IP Unit, which is included in the CIP Safety connection settings, to use tag data link communications.</td><td colspan="2">Do not configure the NX-series EtherNet/IP Unit, which is included in the CIP Safety connection settings, to use tag data link communications.</td></tr>
<tr><td colspan="2">The NX-series EtherNet/IP Unit with tag data link communications was added to the CIP Safety connection settings.</td><td colspan="2">Do not add the NX-series EtherNet/IP Unit, for which tag data link communications are set to use, to the CIP Safety connection settings.</td><td colspan="2">Do not add the NX-series EtherNet/IP Unit, for which tag data link communications are set to use, to the CIP Safety connection settings.</td></tr>
<tr><td><b>Attached information</b></td><td colspan="6">Attached information 1: IP address of the target node (example: C0A8FA01 hex for IP address of 192.168.250.1)
Attached information 2: Connection instance No. 0 to 255
Attached information 3: Connection status (example: 010000117 hex for General Status 01 and Additional Status 0117)</td></tr>
<tr><td><b>Precautions/ Remarks</b></td><td colspan="6">• You can know the detailed cause by checking the connection status. Refer to <i>14-6-2 Connection Status Codes and Troubleshooting</i> on page 14-55.
• If errors occur for multiple connections in one node, the event log is registered only for one connection where an error is occurring.</td></tr>
</table>

Event name	Tag Data Link Timeout			**Event code**	84080000 hex	
Meaning	A timeout occurred in a tag data link.					
Source	X Bus EtherNet/IP Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *CIP1/CIP2* are given in combination	**Detection timing**	Continuously after the start of tag data link communications
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery	**Log category**	System
Effects	**User program**	Continues.	**Operation**	The related data link connection stops. Reconnection process on a regular basis continues for the target node of the tag data link error.		
Indicators	**EtherNet/IP NET RUN**		**EtherNet/IP NET ERR**		**EtherNet/IP LINK/ACT**	
	Flashes at 1-s intervals.		Flashes at 1-s intervals.		---	
Device variable	**Variable**		**Data type**		**Name**	
	EIP_Comm1Status.TDLinkErr		BOOL		CIP Communications1 Tag Data Link Communications Error	
	EIP_Comm2Status.TDLinkErr		BOOL		CIP Communications2 Tag Data Link Communications Error	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The power supply to the target node is OFF.		Check the status of the target node and start it up normally.		Check that the target node is operating properly and start the tag data link.	
	Communications with the target node stopped.					
	The Ethernet cable connector for EtherNet/IP is disconnected.		Check that the connector is fitted correctly and reconnect the connector.		Connect the connector properly.	
	The Ethernet cable for EtherNet/IP is broken.		Replace the Ethernet cable.		None	
	The link to the EtherNet/IP port is OFF.		Refer to the Link OFF Detected error (85D50000Hex) for the assumed causes and other information on link OFF.		Refer to the Link OFF Detected error (85D50000Hex) for the assumed causes and other information on link OFF.	
	CIP message communications at the target node are stopped.		Make the device start normal CIP message communications.		Start CIP message communications successfully and then perform tag data links.	
	When the Packet Filter function is enabled in the EtherNet/IP Port Settings, packets from the target are not allowed.		Allow packets from the target in the Packet Filter settings of the EtherNet/IP Port Settings.		Make sure that packets from the target are allowed in the Packet Filter settings of the Ethernet/IP Port Settings and perform a tag data link.	
	CIP communications are not allowed by the firewall function or Packet Filter function on the target node or the devices on the communication path.		Allow CIP communications in the firewall function or Packet Filter functions on the target node and the devices on the communication path.		Make sure that CIP communications are allowed in the firewall function or Packet Filter functions on the target node or the devices on the communication path, and then perform a tag data link.	
	The packet loss occurred on the path due to the network communications load.		Increase the connection timeout value or RPI. Or, review the network environment and network devices.		Design the network so that there is not too much load on the network.	
	Noise		Implement noise countermeasures if there is excessive noise.		Implement noise countermeasures if there is excessive noise.	

Attached information	Attached information 1: Connection instance No. 0 to 255 Attached information 2: IP address of the target node (example: C0A8FA01 hex for IP address of 192.168.250.1)
Precautions/ Remarks	• This event des not occur for the following cases. The Controller is connected as a target. A connection timeout is occurring due to a Link OFF Error with an Ethernet switch. • If errors occur for multiple connections in one node, the event log is registered only for one connection where an error is occurring.

<table>
<tr><td><b>Event name</b></td><td colspan="3">Tag Data Link Connection Timeout</td><td><b>Event code</b></td><td colspan="2">84090000 hex</td></tr>
<tr><td><b>Meaning</b></td><td colspan="6">A timeout occurred while trying to establish a tag data link connection.</td></tr>
<tr><td><b>Source</b></td><td colspan="2">X Bus EtherNet/IP Function Module</td><td><b>Source details</b></td><td><i>1 to 4: Mounting position of the X Bus Unit (unit number)</i> and <i>CIP1/CIP2</i> are given in combination</td><td><b>Detection timing</b></td><td>When establishing a tag data link connection</td></tr>
<tr><td><b>Error attributes</b></td><td><b>Level</b></td><td>Minor fault</td><td><b>Recovery</b></td><td>Automatic recovery</td><td><b>Log category</b></td><td>System</td></tr>
<tr><td><b>Effects</b></td><td><b>User program</b></td><td>Continues.</td><td><b>Operation</b></td><td colspan="3">A data link where a timeout error occurred while trying to establish a connection does not operate. Reconnection process on a regular basis continues for the connection where a timeout error occurred.</td></tr>
<tr><td rowspan="2"><b>Indicators</b></td><td colspan="2"><b>EtherNet/IP NET RUN</b></td><td colspan="2"><b>EtherNet/IP NET ERR</b></td><td colspan="2"><b>EtherNet/IP LINK/ACT</b></td></tr>
<tr><td colspan="2">Flashes at 1-s intervals.</td><td colspan="2">Flashes at 1-s intervals.</td><td colspan="2">---</td></tr>
<tr><td rowspan="3"><b>Device variable</b></td><td colspan="2"><b>Variable</b></td><td colspan="2"><b>Data type</b></td><td colspan="2"><b>Name</b></td></tr>
<tr><td colspan="2">EIP_Comm1Status.TDLinkOpnErr</td><td colspan="2">BOOL</td><td colspan="2">CIP Communications1 Tag Data Link Connection Failed</td></tr>
<tr><td colspan="2">EIP_Comm2Status.TDLinkOpnErr</td><td colspan="2">BOOL</td><td colspan="2">CIP Communications2 Tag Data Link Connection Failed</td></tr>
<tr><td rowspan="8"><b>Cause and correction</b></td><td colspan="2"><b>Assumed cause</b></td><td colspan="2"><b>Correction</b></td><td colspan="2"><b>Prevention</b></td></tr>
<tr><td colspan="2">The power supply to the target node is OFF.</td><td colspan="2" rowspan="2">Check the status of the target node and start it up normally.</td><td colspan="2" rowspan="2">Check that the target node is operating properly and start the tag data link.</td></tr>
<tr><td colspan="2">Communications with the target node stopped.</td></tr>
<tr><td colspan="2">CIP message communications stopped at the target node or the EtherNet/IP port.</td><td colspan="2">Make the device start normal CIP message communications.</td><td colspan="2">Start CIP message communications successfully and then perform tag data links.</td></tr>
<tr><td colspan="2">The Ethernet cable connector for EtherNet/IP is disconnected.</td><td colspan="2">Check that the connector is fitted correctly and reconnect the connector.</td><td colspan="2">Connect the connector properly.</td></tr>
<tr><td colspan="2">The Ethernet cable for EtherNet/IP is broken.</td><td colspan="2">Replace the Ethernet cable.</td><td colspan="2">None</td></tr>
<tr><td colspan="2">CIP communications are not allowed by the firewall function or Packet Filter function on the target node or the devices on the communication path.</td><td colspan="2">Allow CIP communications in the firewall function or Packet Filter functions on the target node and the devices on the communication path.</td><td colspan="2">Make sure that CIP communications are allowed in the firewall function or Packet Filter functions on the target node or the devices on the communication path, and then perform a tag data link.</td></tr>
<tr><td colspan="2">An error occurred in the communications path.</td><td colspan="2">Check the communications path and take corrective measures if there are any problems.</td><td colspan="2">None</td></tr>
<tr><td><b>Attached information</b></td><td colspan="6">Attached information 1: IP address of the target node (example: C0A8FA01 hex for IP address of 192.168.250.1)</td></tr>
<tr><td><b>Precautions/ Remarks</b></td><td colspan="6">• This event des not occur for the following cases.
The Controller is connected as a target.
A connection timeout is occurring due to detection of a link OFF to an Ethernet switch.
• If errors occur for multiple connections in one node, the event log is registered only for one connection where an error is occurring.</td></tr>
</table>

<table>
<tr><td><b>Event name</b></td><td colspan="3">Allowed Communications Bandwidth per Unit Exceeded</td><td><b>Event code</b></td><td colspan="2">840C0000 hex</td></tr>
<tr><td><b>Meaning</b></td><td colspan="6">The total bandwidth for the connections that are set or established for all of the EtherNet/IP ports exceeded the allowed communications bandwidth of tag data links and CIP Safety communications per Unit.</td></tr>
<tr><td><b>Source</b></td><td colspan="2">X Bus EtherNet/IP Function Module</td><td><b>Source details</b></td><td><i>1 to 4: Mounting position of the X Bus Unit (unit number)</i> and <i>CIP1/CIP2</i> are given in combination</td><td><b>Detection timing</b></td><td>When establishing a tag data link connection or a CIP safety connection</td></tr>
<tr><td><b>Error attributes</b></td><td><b>Level</b></td><td>Minor fault</td><td><b>Recovery</b></td><td>Automatic recovery (after downloading the settings), cycle the power supply, or Controller reset</td><td><b>Log category</b></td><td>System</td></tr>
<tr><td><b>Effects</b></td><td><b>User program</b></td><td>Continues.</td><td><b>Operation</b></td><td colspan="3">Tag data links and CIP Safety communications that exceed the unit's allowable communication bandwidth do not operate.</td></tr>
<tr><td rowspan="2"><b>Indicators</b></td><td colspan="2"><b>EtherNet/IP NET RUN</b></td><td colspan="2"><b>EtherNet/IP NET ERR</b></td><td colspan="2"><b>EtherNet/IP LINK/ACT</b></td></tr>
<tr><td colspan="2">Flashes at 1-s intervals.</td><td colspan="2">Flashes at 1-s intervals.</td><td colspan="2">---</td></tr>
<tr><td rowspan="3"><b>Device variable</b></td><td colspan="2"><b>Variable</b></td><td colspan="2"><b>Data type</b></td><td colspan="2"><b>Name</b></td></tr>
<tr><td colspan="2">EIP_Comm1Status.TDLinkOpnErr</td><td colspan="2">BOOL</td><td colspan="2">CIP Communications1 Tag Data Link Connection Failed</td></tr>
<tr><td colspan="2">EIP_Comm2Status.TDLinkOpnErr</td><td colspan="2">BOOL</td><td colspan="2">CIP Communications2 Tag Data Link Connection Failed</td></tr>
<tr><td rowspan="2"><b>Cause and correction</b></td><td colspan="2"><b>Assumed cause</b></td><td colspan="2"><b>Correction</b></td><td colspan="2"><b>Prevention</b></td></tr>
<tr><td colspan="2">An attempt was made to establish a connection of communications bandwidth (PPS), which is the sum of the packet transmission rates of the tag data links and CIP Safety communications used for all EtherNet/IP ports, and it exceeded the allowable communications bandwidth of the Unit.</td><td colspan="2">Change the settings of the originator node for tag data links and CIP Safety communications so that PPS for all port of the Ethernet/IP port is within the allowable communications bandwidth per Unit, and cycle the power supply to the Controller or reset the Controller.</td><td colspan="2">Set tag data links and CIP Safety communications so that PPS for all ports of the Ethernet/IP port is smaller than the allowable communications bandwidth per Unit.</td></tr>
<tr><td><b>Attached information</b></td><td colspan="6">None</td></tr>
<tr><td><b>Precautions/ Remarks</b></td><td colspan="6">The bandwidth usage (PPS) for tag data links on the EtherNet/IP port is shown on the <b>Ethernet Information</b> tab page of the Network Configurator.
For the procedure to check the bandwidth usage (PPS), refer to the description on <b><i>Ethernet Information</i></b> <i>Tab Page</i> in <i>Checking Communications Status with the Sysmac Studio and Troubleshooting</i> on the <i>NJ/NX-series CPU Unit Built-in EtherNet/IP Port User’s Manual (Cat. No. W506)</i>.</td></tr>
</table>

Event name	Number of Tag Sets for Tag Data Links Exceeded			**Event code**	840E0000 hex	
Meaning	The total number of tag sets for tag data links for all Ethernet/IP ports exceeds the upper limit.					
Source	X Bus EtherNet/IP Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *CIP1/CIP2* are given in combination	**Detection timing**	At power ON, Controller reset, download from the Sysmac Studio, or download from the Network Configurator
Error attributes	**Level**	Minor fault	**Recovery**	Automatic recovery	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Tag data link communications for the relevant port were stopped.		
Indicators	**EtherNet/IP NET RUN**		**EtherNet/IP NET ERR**		**EtherNet/IP LINK/ACT**	
	Flashes at 1-s intervals.		Flashes at 1-s intervals.		---	
Device variable	**Variable**		**Data type**		**Name**	
	EIP_Comm1Status.TDLinkCfgErr		BOOL		CIP Communications1 Tag Data Link Setting Error	
	EIP_Comm2Status.TDLinkCfgErr		BOOL		CIP Communications2 Tag Data Link Setting Error	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The total number of tag sets for all ports that are set for tag data links in each Ethernet/IP port exceeded the maximum number the product allows.		Change the number of tag sets so that the total number of tag sets for all ports that are set for tag data links in each Ethernet/IP port does not exceed the maximum number the product allows.		When you change the number of tag sets for tag data links in each Ethernet/IP port, make sure that the total number of tag sets for all ports does not exceed the maximum number.	
Attached information	Attached information 1: The number of tag sets that are set for the port. Attached information 2: Total number of tag sets that are set for the product. Attached information 3: Maximum number of tag sets that the product allows.					
Precautions/ Remarks	None					

Event name	Unit Configuration Error, Combined Use of CIP Safety and Tag Data Link			**Event code**	342C0000 hex	
Meaning	Tag data link communications and CIP Safety communications cannot be used together in one NX-series EtherNet/IP Unit.					
Source	X Bus EtherNet/IP Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *CIP1/CIP2* are given in combination	**Detection timing**	Continuously
Error attributes	**Level**	Observation	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Not affected.		
Indicators	**EtherNet/IP NET RUN**		**EtherNet/IP NET ERR**		**EtherNet/IP LINK/ACT**	
	---		---		---	
Device variable	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Setting to use tag data link communications was made to the NX-series EtherNet/IP Unit that is included in the CIP Safety connection settings.		Do not configure the NX-series EtherNet/IP Unit, which is included in the CIP Safety connection settings, to use tag data link communications.		Do not configure the NX-series EtherNet/IP Unit, which is included in the CIP Safety connection settings, to use tag data link communications.	
	The NX-series EtherNet/IP Unit with tag data link communications was added to the CIP Safety connection settings.		Do not add the NX-series EtherNet/IP Unit, for which tag data link communications are set to use, to the CIP Safety connection settings.		Do not add the NX-series EtherNet/IP Unit, for which tag data link communications are set to use, to the CIP Safety connection settings.	
Attached information	None					
Precautions/ Remarks	None					

<table>
<tr><td><b>Event name</b></td><td colspan="3">Access Detected Outside Range of Variable</td><td><b>Event code</b></td><td colspan="2">54E00000 hex</td></tr>
<tr><td><b>Meaning</b></td><td colspan="6">An access attempt to write a value out of range was detected for a tag variable that is used in a tag data link.</td></tr>
<tr><td><b>Source</b></td><td colspan="2">X Bus EtherNet/IP Function Module</td><td><b>Source details</b></td><td>CIP1 or CIP2</td><td><b>Detection timing</b></td><td>When writing a value to a variable</td></tr>
<tr><td><b>Error attributes</b></td><td><b>Level</b></td><td>Observation</td><td><b>Recovery</b></td><td>---</td><td><b>Log category</b></td><td>System</td></tr>
<tr><td><b>Effects</b></td><td><b>User program</b></td><td>Continues.</td><td><b>Operation</b></td><td colspan="3">Not affected.</td></tr>
<tr><td rowspan="2"><b>Indicators</b></td><td colspan="2"><b>EtherNet/IP NET RUN</b></td><td colspan="2"><b>EtherNet/IP NET ERR</b></td><td colspan="2"><b>EtherNet/IP LINK/ACT</b></td></tr>
<tr><td colspan="2">---</td><td colspan="2">---</td><td colspan="2">---</td></tr>
<tr><td rowspan="2"><b>Device variable</b></td><td colspan="2"><b>Variable</b></td><td colspan="2"><b>Data type</b></td><td colspan="2"><b>Name</b></td></tr>
<tr><td colspan="2">None</td><td colspan="2">---</td><td colspan="2">---</td></tr>
<tr><td rowspan="2"><b>Cause and correction</b></td><td colspan="2"><b>Assumed cause</b></td><td colspan="2"><b>Correction</b></td><td colspan="2"><b>Prevention</b></td></tr>
<tr><td colspan="2">An out-of-range value was written by an EtherNet/IP tag data link to a variable with range specification.
A value that does not specify an enumerator was written by an EtherNet/IP tag data link to an enumeration variable.</td><td colspan="2">Correct the value that is written to the variable with range specification so that the value is in the range.
Correct the value that is written to the enumeration variable so that the value specifies an enumerator.</td><td colspan="2">Write values that are in range for variables with specified ranges.
Write values that specify enumerators to enumeration variables.</td></tr>
<tr><td><b>Attached information</b></td><td colspan="6">None</td></tr>
<tr><td><b>Precautions/ Remarks</b></td><td colspan="6">• Write operations for out-of-range values or values that do not specify enumerators do not end normally.
• Write operations for in-range values or values that specify enumerators end normally.</td></tr>
</table>

<table>
<tr><td><b>Event name</b></td><td colspan="3">Tag Data Link Download Started</td><td><b>Event code</b></td><td colspan="2">94010000 hex</td></tr>
<tr><td><b>Meaning</b></td><td colspan="6">Changing the tag data link settings started.</td></tr>
<tr><td><b>Source</b></td><td colspan="2">X Bus EtherNet/IP Function Module</td><td><b>Source details</b></td><td><i>1 to 4: Mounting position of the X Bus Unit (unit number)</i> and <i>CIP1/CIP2</i> are given in combination</td><td><b>Detection timing</b></td><td>At user operation</td></tr>
<tr><td><b>Error attributes</b></td><td><b>Level</b></td><td>Information</td><td><b>Recovery</b></td><td>---</td><td><b>Log category</b></td><td>Access</td></tr>
<tr><td><b>Effects</b></td><td><b>User program</b></td><td>Continues.</td><td><b>Operation</b></td><td colspan="3">Not affected.</td></tr>
<tr><td rowspan="2"><b>Indicators</b></td><td colspan="2"><b>EtherNet/IP NET RUN</b></td><td colspan="2"><b>EtherNet/IP NET ERR</b></td><td colspan="2"><b>EtherNet/IP LINK/ACT</b></td></tr>
<tr><td colspan="2">Flashes at 1-s intervals.</td><td colspan="2">---</td><td colspan="2">---</td></tr>
<tr><td rowspan="2"><b>Device variable</b></td><td colspan="2"><b>Variable</b></td><td colspan="2"><b>Data type</b></td><td colspan="2"><b>Name</b></td></tr>
<tr><td colspan="2">None</td><td colspan="2">---</td><td colspan="2">---</td></tr>
<tr><td rowspan="2"><b>Cause and correction</b></td><td colspan="2"><b>Assumed cause</b></td><td colspan="2"><b>Correction</b></td><td colspan="2"><b>Prevention</b></td></tr>
<tr><td colspan="2">Changing the tag data link settings started.</td><td colspan="2">---</td><td colspan="2">---</td></tr>
<tr><td><b>Attached information</b></td><td colspan="6">Attached information 1: Controller status (01 hex: PROGRAM mode, 02 hex: RUN mode)</td></tr>
<tr><td><b>Precautions/ Remarks</b></td><td colspan="6">None</td></tr>
</table>

Event name	Tag Data Link Download Finished			**Event code**	94020000 hex	
Meaning	Changing the tag data link settings finished.					
Source	X Bus EtherNet/IP Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *CIP1/CIP2* are given in combination	**Detection timing**	At user operation
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	Access
Effects	**User program**	Continues.	**Operation**	Not affected.		
Indicators	**EtherNet/IP NET RUN**		**EtherNet/IP NET ERR**		**EtherNet/IP LINK/ACT**	
	Flashes at 1-s intervals.		---		---	
Device variable	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Changing the tag data link settings finished.		---		---	
Attached information	Attached information 1: Controller status (01 hex: PROGRAM mode, 02 hex: RUN mode)					
Precautions/ Remarks	None					

Event name	Tag Data Link Stopped			**Event code**	94030000 hex	
Meaning	Tag data links were stopped by the Network Configurator, Sysmac Studio, special instructions or manipulation of a system-defined variable. Or, the data link table was downloaded from Network Configurator or Sysmac Studio.					
Source	X Bus EtherNet/IP Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *CIP1/CIP2* are given in combination	**Detection timing**	At user operation
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	Access
Effects	**User program**	Continues.	**Operation**	Not affected.		
Indicators	**EtherNet/IP NET RUN**		**EtherNet/IP NET ERR**		**EtherNet/IP LINK/ACT**	
	Flashes at 1-s intervals.		---		---	
Device variable	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Tag data links were stopped by the Network Configurator, Sysmac Studio, special instructions or manipulation of a system-defined variable.		---		---	
Attached information	Attached information 1: Controller status (01 hex: PROGRAM mode, 02 hex: RUN mode) Attached information 2: Operation method (01 hex: Operation by Network Configurator or Sysmac Studio, 02 hex: Manipulation by a device variable, 03 hex: Manipulation by special instructions) Attached information 3: • When attached information 2 is 03 hex: IP address of the target node • Other than the above: 0					
Precautions/ Remarks	None					

Event name	Tag Data Link Started			**Event code**	94040000 hex	
Meaning	Tag data links were started by the Network Configurator, Sysmac Studio, special instructions or manipulation of a system-defined variable. Or, the data link table was downloaded from Network Configurator or Sysmac Studio.					
Source	X Bus EtherNet/IP Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *CIP1/CIP2* are given in combination	**Detection timing**	At user operation
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	Access
Effects	**User program**	Continues.	**Operation**	Not affected.		
Indicators	**EtherNet/IP NET RUN**		**EtherNet/IP NET ERR**		**EtherNet/IP LINK/ACT**	
	Flashes at 1-s intervals.		---		---	
Device variable	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Tag data links were started by the Network Configurator, Sysmac Studio, special instructions or manipulation of a system-defined variable.		---		---	
Attached information	Attached information 1: Controller status (01 hex: PROGRAM mode, 02 hex: RUN mode) Attached information 2: Operation method (01 hex: Operation by Network Configurator or Sysmac Studio, 02 hex: Manipulation by a device variable, 03 hex: Manipulation by special instructions) Attached information 3: • When attached information 2 is 03 hex: IP address of the target node • Other than the above: 0					
Precautions/ Remarks	None					

Event name	Tag Data Link All Run			**Event code**	94070000 hex	
Meaning	Tag data link connections to all target nodes have been normally established.					
Source	X Bus EtherNet/IP Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *CIP1/CIP2* are given in combination	**Detection timing**	When establishing a tag data link connection
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	System
Effects	**User program**	Continues.	**Operation**	Not affected.		
Indicators	**EtherNet/IP NET RUN**		**EtherNet/IP NET ERR**		**EtherNet/IP LINK/ACT**	
	Lights.		---		---	
Device variable	**Variable**		**Data type**		**Name**	
	EIP_Comm1Status.TDLinkAllRunSta		BOOL		CIP Communications1 All Tag Data Link Communications Status	
	EIP_Comm2Status.TDLinkAllRunSta		BOOL		CIP Communications2 All Tag Data Link Communications Status	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	Tag data link connections to all target nodes have been normally established.		---		---	
Attached information	None					
Precautions/ Remarks	None					

Event name	Restarting Ethernet Port			**Event code**	96450000 hex	
Meaning	The EtherNet/IP port was restarted.					
Source	X Bus EtherNet/IP Function Module		**Source details**	*1 to 4: Mounting position of the X Bus Unit (unit number)* and *CIP1/CIP2* are given in combination	**Detection timing**	At user operation
Error attributes	**Level**	Information	**Recovery**	---	**Log category**	Access
Effects	**User program**	Continues.	**Operation**	Not affected.		
Indicators	**EtherNet/IP NET RUN**		**EtherNet/IP NET ERR**		**EtherNet/IP LINK/ACT**	
	---		---		---	
Device variable	**Variable**		**Data type**		**Name**	
	None		---		---	
Cause and correction	**Assumed cause**		**Correction**		**Prevention**	
	The EtherNet/IP port was restarted.		---		---	
Attached information	None					
Precautions/ Remarks	None					

14-5 Checking with Device Variables

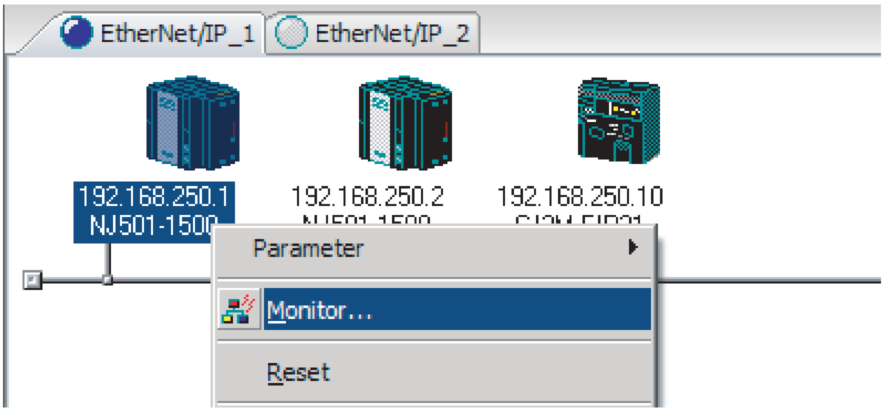
You can check the status of current Controller errors in the X Bus Ethernet Function Module, X Bus EtherNet/IP Function Module, and X Bus Unit Common Function Module with the device variables.
Refer to *Section 6 Device Variables Related to the NX-series EtherNet/IP Unit* on page 6-1 for details on the device variables of the X Bus Ethernet Function Module and X Bus EtherNet/IP Function Module.
Refer to *Specifications for Individual Device Variables* in the *NJ/NX-series CPU Unit Software User's Manual (Cat. No. W501)* for details on the device variables of the X Bus Unit Common Function Module.

14-6 Checking with the Network Configurator

You can check the communications status of each device on the EtherNet/IP network (e.g. tag data link connection status) with the Network Configurator.

14-6-1 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.

Precautions for Correct Use

Monitoring may not be performed if the following settings are configured on the NJ/NX-series Controller on the connection route or on the destination NJ/NX-series Controller. If monitoring is not performed, check the following settings. Refer to *CIP Message Server* on page 7-15, and*Packet Filter* on page 7-7 for details on the settings.

- The **Do not use** Option is selected for the CIP message server.
- The **Use** Option is selected for Packet Filter.

Additional Information

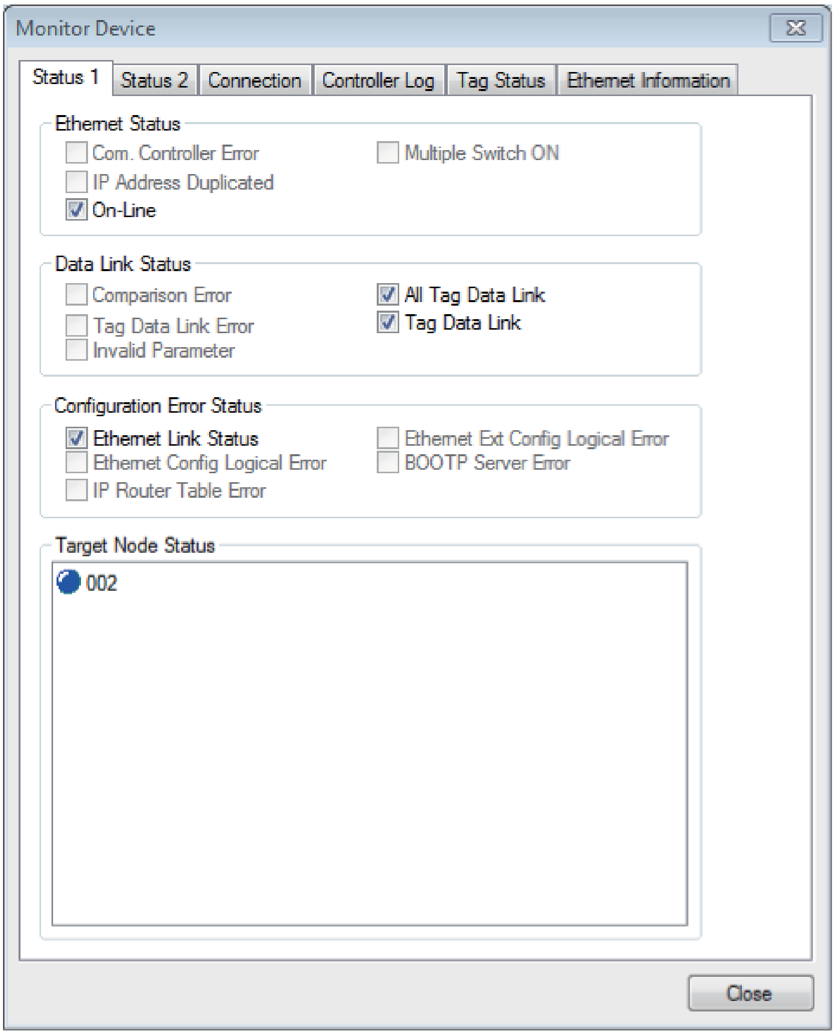
If a communications error occurs during monitoring, the dialog box will continue to show the last information that was collected.
To start monitoring again, close the **Monitor Device** Dialog Box, and then open the **Monitor Device** Dialog Box again.

● Status 1 Tab Page

The following check boxes are displayed for the status. If a check box is checked with ☑, the status is TRUE.

Classification	Item	TRUE status description
Ethernet Status	Com. Controller Error	An error occurred in the Communications Controller.
	IP Address Duplicated	The same IP address is assigned to more than one node.
	On-Line	The Unit is online. (The EtherNet/IP Unit can perform communications processing.)
	Multiple Switch ON	More than one data link start/stop switch changed to TRUE at the same time.
Data Link Status	Comparison Error	The remote node information in the tag data link parameters was different from the actual node information. Main causes: • The specified target does not exist. • The variable name does not match. • The connection size is different. • Connection resources are not sufficient.
Data Link Status	Tag Data Link Error	There were two or more errors in a connection as an originator.
	Invalid Parameter	An error was found in the parameters for tag data links that are saved in non-volatile memory.
	All Tag Data Link	Tag data links are communicating in all connections as the originator.
	Tag Data Link	Tag data links are communicating in one or more connections as the originator.
Configuration Error Status	Ethernet Link Status	A link is established with the Ethernet switch.
	Ethernet Basic Settings Logic Error	The following settings are incorrect: • TCP/IP settings (IP address, subnet mask, or link settings)
	IP Router Table Error	There is a mistake in the IP router table information.
	Ethernet Ext Config Logical Error	Always FALSE.
	BOOTP Server Error	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.

In the **Target Node Status**, information about the target node that acts as the originator is displayed.
If all tag data link connections to the node are established and normal, this information is displayed in blue. However, if any connection is broken it is displayed in red.



Monitor Device

Ethernet Status

☐ Com. Controller Error
☐ IP Address Duplicated
☑ On-Line
☐ Multiple Switch ON

Data Link Status

☐ Comparison Error
☐ Tag Data Link Error
☐ Invalid Parameter
☑ All Tag Data Link
☑ Tag Data Link

Configuration Error Status

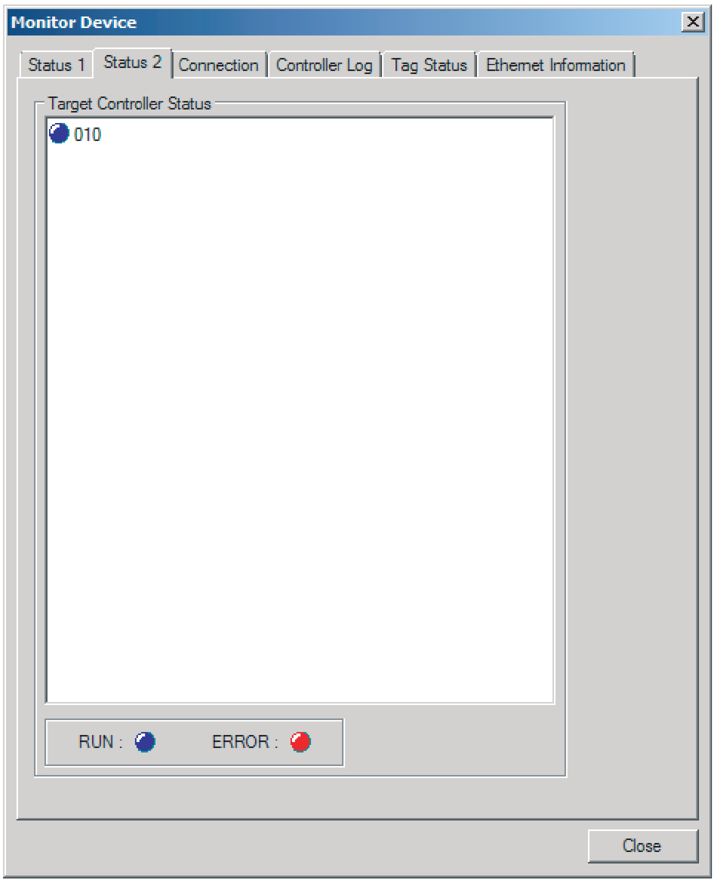
☑ Ethernet Link Status
☐ Ethernet Config Logical Error
☐ IP Router Table Error
☐ Ethernet Ext Config Logical Error
☐ BOOTP Server Error

Target Node Status

● 002

● Status 2 Tab Page

This tab page displays information on nodes with tag data link originator settings. This information is in blue if the connection is normal, or red if an error occurred.



Additional Information

The target Controller status can be used when the Controller status is set to **Included** for all the target sets for both originator and target connections.
If it is set to **Not included**, it is grayed out on the display.

● Connection Tab Page

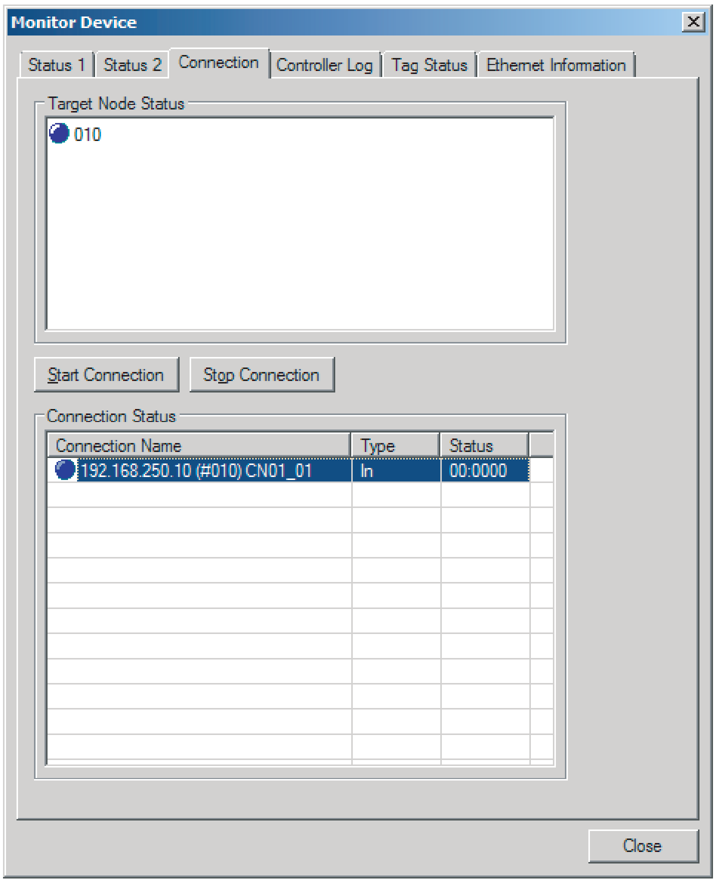
- Target Node Status

  Information about the target node that acts as the originator is displayed.

  If all tag data link connections to the node are established and normal, this information is displayed in blue. However, if any connection is broken it is displayed in red.

  However, this information is displayed in gray if the connection to the node is stopped.
- Connection Status

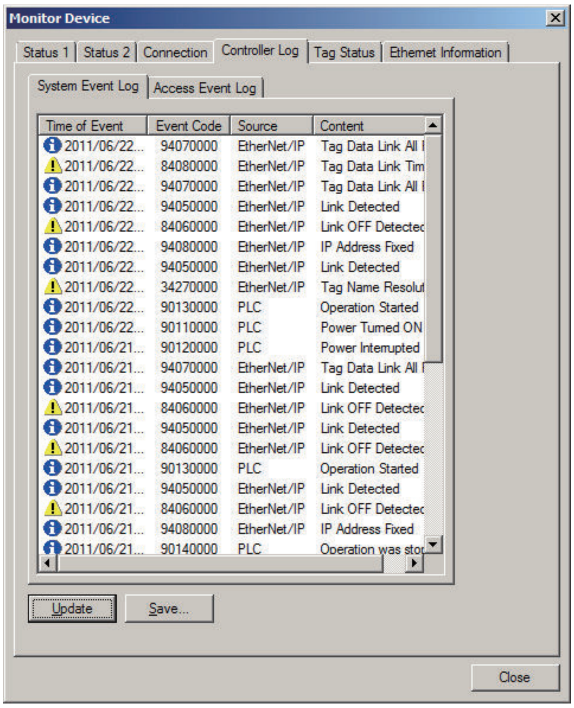
  The **Status** Column of the connection status shows the status of each connection that is set as the originator. The connection status can be used to identify the cause of tag data link errors. Refer to *14-6-2 Connection Status Codes and Troubleshooting* on page 14-55 for details on the connection status.



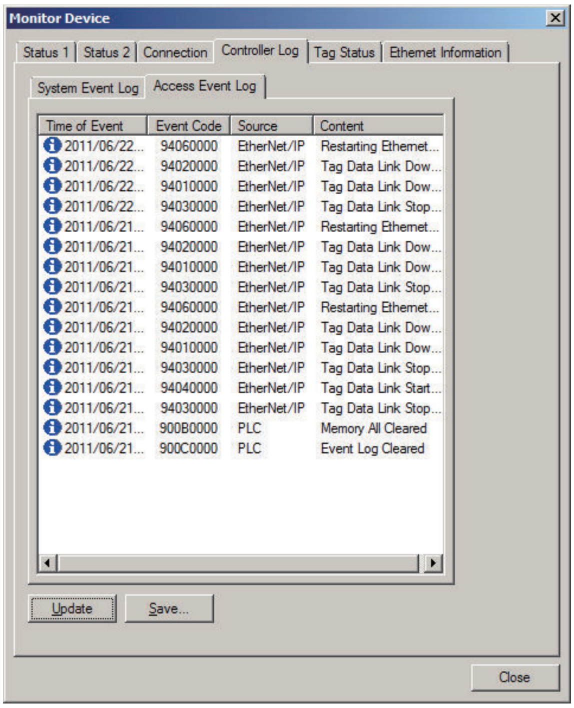
Connection Name	Type	Status
192.168.250.10 (#010) CN01_01	In	00:0000

● Controller Log Tab Page

This tab page displays the Controller event log that is stored in the NX-series EtherNet/IP Unit. The error history shows errors that have occurred. It can be saved in a file in the computer.



Time of Event	Event Code	Source	Content
ℹ 2011/06/22...	94070000	EtherNet/IP	Tag Data Link All I
⚠ 2011/06/22...	84080000	EtherNet/IP	Tag Data Link Tim
ℹ 2011/06/22...	94070000	EtherNet/IP	Tag Data Link All I
ℹ 2011/06/22...	94050000	EtherNet/IP	Link Detected
⚠ 2011/06/22...	84060000	EtherNet/IP	Link OFF Detectec
ℹ 2011/06/22...	94080000	EtherNet/IP	IP Address Fixed
ℹ 2011/06/22...	94050000	EtherNet/IP	Link Detected
⚠ 2011/06/22...	34270000	EtherNet/IP	Tag Name Resolut
ℹ 2011/06/22...	90130000	PLC	Operation Started
ℹ 2011/06/22...	90110000	PLC	Power Turned ON
ℹ 2011/06/21...	90120000	PLC	Power Interrupted
ℹ 2011/06/21...	94070000	EtherNet/IP	Tag Data Link All I
ℹ 2011/06/21...	94050000	EtherNet/IP	Link Detected
⚠ 2011/06/21...	84060000	EtherNet/IP	Link OFF Detectec
ℹ 2011/06/21...	94050000	EtherNet/IP	Link Detected
⚠ 2011/06/21...	84060000	EtherNet/IP	Link OFF Detectec
ℹ 2011/06/21...	90130000	PLC	Operation Started
ℹ 2011/06/21...	94050000	EtherNet/IP	Link Detected
⚠ 2011/06/21...	84060000	EtherNet/IP	Link OFF Detectec
ℹ 2011/06/21...	94080000	EtherNet/IP	IP Address Fixed
ℹ 2011/06/21...	90140000	PLC	Operation was sto



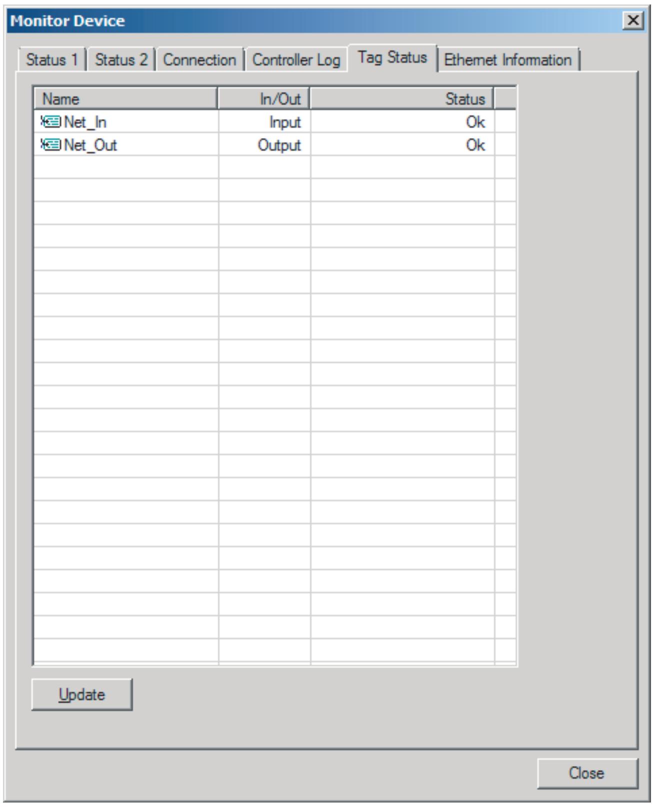
Time of Event	Event Code	Source	Content
ℹ 2011/06/22...	94060000	EtherNet/IP	Restarting Ethernet...
ℹ 2011/06/22...	94020000	EtherNet/IP	Tag Data Link Dow...
ℹ 2011/06/22...	94010000	EtherNet/IP	Tag Data Link Dow...
ℹ 2011/06/22...	94030000	EtherNet/IP	Tag Data Link Stop...
ℹ 2011/06/21...	94060000	EtherNet/IP	Restarting Ethernet...
ℹ 2011/06/21...	94020000	EtherNet/IP	Tag Data Link Dow...
ℹ 2011/06/21...	94010000	EtherNet/IP	Tag Data Link Dow...
ℹ 2011/06/21...	94030000	EtherNet/IP	Tag Data Link Stop...
ℹ 2011/06/21...	94060000	EtherNet/IP	Restarting Ethernet...
ℹ 2011/06/21...	94020000	EtherNet/IP	Tag Data Link Dow...
ℹ 2011/06/21...	94010000	EtherNet/IP	Tag Data Link Dow...
ℹ 2011/06/21...	94030000	EtherNet/IP	Tag Data Link Stop...
ℹ 2011/06/21...	94040000	EtherNet/IP	Tag Data Link Start...
ℹ 2011/06/21...	94030000	EtherNet/IP	Tag Data Link Stop...
ℹ 2011/06/21...	900B0000	PLC	Memory All Cleared
ℹ 2011/06/21...	900C0000	PLC	Event Log Cleared

● Tag Status Tab Page

This tab page displays if the tag settings for each tag for tag data links are set so that data can be exchanged with the NX-series EtherNet/IP Unit.
The following status is displayed depending on the status that is set.

Normally resolved:	Normal data exchange is possible.
Resolving:	The variables with tags are being resolved. When the resolution is completed normally, a connection will be established and the data exchange will start.
Different sizes:	Different sizes are set for the network variables and the tag settings. A connection will not be established for a tag for which this error occurs.
No tag:	A network variable is not set in the variable table in the NX-series EtherNet/IP Unit for the specified tag setting. Or, instead of a member of union variable, unions are specified. A connection will not be established for a tag for which this error occurs.
Attribute error:	1. Writing is not possible for Read Only and Constant attributes. 2. The I/O direction that is set in the tag data link settings does not agree with the I/O direction of the variable in the NX-series EtherNet/IP Unit. There is an error in the setting of a Network Publish attribute for a NX-series EtherNet/IP Unit variable. A connection will not be established for a tag for which this error occurs.

If the status is not "Normally resolved", check the tag data link settings or the network variable settings in the variable table in the NX-series EtherNet/IP Unit.



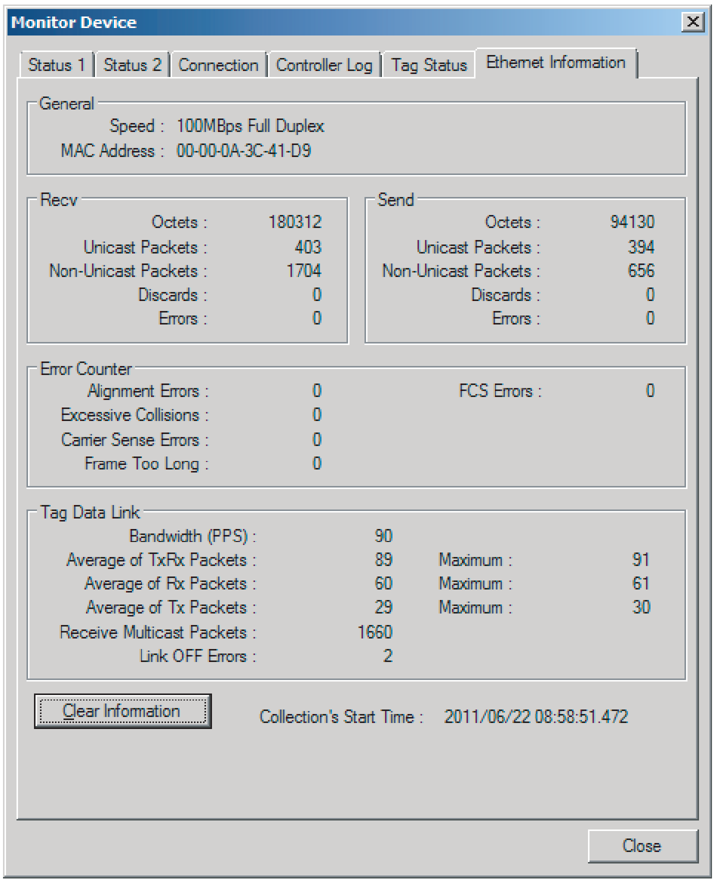
Name	In/Out	Status
Net_In	Input	Ok
Net_Out	Output	Ok

● Ethernet Information Tab Page

This tab page displays the communications status at the communications driver level of the EtherNet/IP port.

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 (pps).



General

Speed : 100MBps Full Duplex

MAC Address : 00-00-0A-3C-41-D9

Recv		Send	
Octets :	180312	Octets :	94130
Unicast Packets :	403	Unicast Packets :	394
Non-Unicast Packets :	1704	Non-Unicast Packets :	656
Discards :	0	Discards :	0
Errors :	0	Errors :	0

Error Counter

Alignment Errors :	0	FCS Errors :	0
Excessive Collisions :	0		
Carrier Sense Errors :	0		
Frame Too Long :	0		

Tag Data Link

Bandwidth (PPS) :	90		
Average of TxRx Packets :	89	Maximum :	91
Average of Rx Packets :	60	Maximum :	61
Average of Tx Packets :	29	Maximum :	30
Receive Multicast Packets :	1660		
Link OFF Errors :	2		

Collection's Start Time : 2011/06/22 08:58:51.472

14-6-2 Connection Status Codes and Troubleshooting

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 Monitor Device Window with the Network Configurator. Refer to *14-6-1 The Network Configurator's Device Monitor Function* on page 14-47 for details.

Additional Information

The connection status has the same meaning as the Connection Manager's General and Additional error response codes, as defined in the CIP specifications.

The following table shows the likely causes of the errors causes for each configuration and connection status (code).

	Originator	Target
Configuration 1		
Configuration 2		Products from other manufacturers
Configuration 3	Products from other manufacturers	

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 for the same connection.	This error does not occur.	Depends on the target's specifications. (This error should not occur. If it does, contact the target device's manufacturer.)	Depends on the originator's specifications. (This error should not occur. If it does, contact the originator device's manufacturer.)
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.
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.

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
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 connections can be set.	Check which connection types can be used by the originator. (An error will occur if a connection other than a multicast or point-to-point connection 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 software switch.)	Depends on the target's specifications. (Contact the target device's manufacturer.)	Check whether the tag data link is stopped at the target. (Restart the tag data link communications with the software switch.)
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.

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
01	0113	Error code generated by originator or returned from target: Attempted to open more connections than allowed by the specifications. Connections of tag data link communications and CIP Safety communications are used together.	Check the connection settings (number of connections) at the originator and target. Check whether a *Unit Configuration Error, Combined Use of CIP Safety and Tag Data Link* (342C0000 hex) observation level event occurred in the NX-series EtherNet/IP Unit which is on the path of tag data link communications.	Check the connection settings (number of connections) at the originator and target. Check the connection specifications for devices from other manufacturers. Check whether a *Unit Configuration Error, Combined Use of CIP Safety and Tag Data Link* (342C0000 hex) observation level event occurred in the NX-series EtherNet/IP Unit which is on the path of tag data link communications.	Check the connection settings (number of connections) at the originator and target. Check the connection specifications for devices from other manufacturers. Check whether a *Unit Configuration Error, Combined Use of CIP Safety and Tag Data Link* (342C0000 hex) observation level event occurred in the NX-series EtherNet/IP Unit which is on the path of tag data link communications.
01	0114	Error code returned from target: The Vendor ID and Product Code did not match when opening connection.	This error does not occur.	Depends on the target's specifications. (Contact the target device's manufacturer.) Check 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.) Check that the target device's EDS file is correct.	Check the originator's connection settings.

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
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 most recent EDS file and set it again.	Depends on the target's specifications. (Contact the target device's manufacturer.) Check 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.	Depends on the target's specifications. (Contact the target device's manufacturer.)	Check the originator's connection settings. Check whether the target tag sets and tags are set correctly.
01	011A	Error code generated by originator: Connection could not be established because the buffer was full due to high traffic.	Unexpected network traffic may have been received. If there are places where broadcast storms occur, such as loop connections in the network connection format, then correct them.	Unexpected network traffic may have been received. If there are places where broadcast storms occur, such as loop connections in the network connection format, then correct them.	Depends on the target's specifications. (Contact the target device's 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 1 ms or greater.
01	0203	Error code generated by originator: 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 traffic, change the performance settings. For example, increase the timeout time or RPI setting. Also, check whether the CIP message communications of the target are stopped and whether the CIP communications are permitted by Packet Filter function of the originator or the device on the route.		

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
01	0204	Error code generated by originator: The connection open 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. Also, check whether the CIP message communications of the target or originator are stopped and whether the CIP communications are permitted by Packet Filter function of the target device or the device on the route.		
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	0301	Error code generated by originator or returned from target: Total number of tag sets that are set to the product was exceeded.	Check the total number of the tag sets that are set to the product and set the tag sets so that the total number does not exceed the maximum of the allowable number.	Check the total number of the tag sets that are set to the product and set the tag sets so that the total number does not exceed the maximum of the allowable number.	Check the total number of the tag sets that are set to the product and set the tag sets so that the total number does not exceed the maximum of the allowable number.
01	0302	Error code generated by originator or returned from target: The tag data link's allowable bandwidth (pps) was exceeded.	Check the connection settings (number of connections and RPI) at the originator and target.	Check the target's connection settings (number of connections and RPI). Check the connection settings (number of connections and RPI) at the originator and target.	Check the connection settings (number of connections and RPI) at the originator and target.
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.)

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
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.)
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 by 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 an open 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.)

Connection status		Source of error	Handling		
General Status (hex)	Additional Status (hex)		Configuration 1	Configuration 2	Configuration 3
D0	0001	Error code generated by 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 Switch, or wait until the settings data has been downloaded. This code includes fatal Controller errors and Unit failure. To handle these errors, refer to the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)*.	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 by 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
OMRON error code					
01	0810	Error code returned from target:		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 by originator:	The error will be recovered automatically.	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.)

15

Maintenance and Inspection

This section describes cleaning and inspection methods and maintenance procedures.

15-1 Maintenance and Inspection

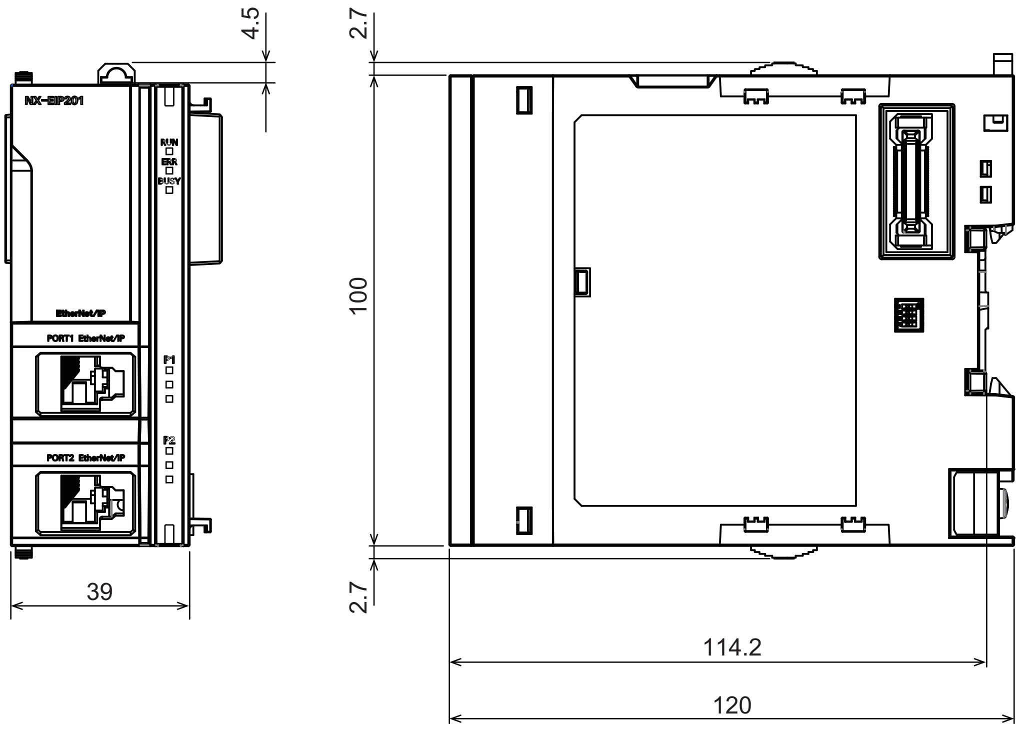
Refer to *Maintenance and Inspection* in the *NX-series NX502 CPU Unit Hardware User's Manual (Cat. No. W629)* for information on cleaning and inspection methods and maintenance procedures of the NX-series EtherNet/IP Unit.

A

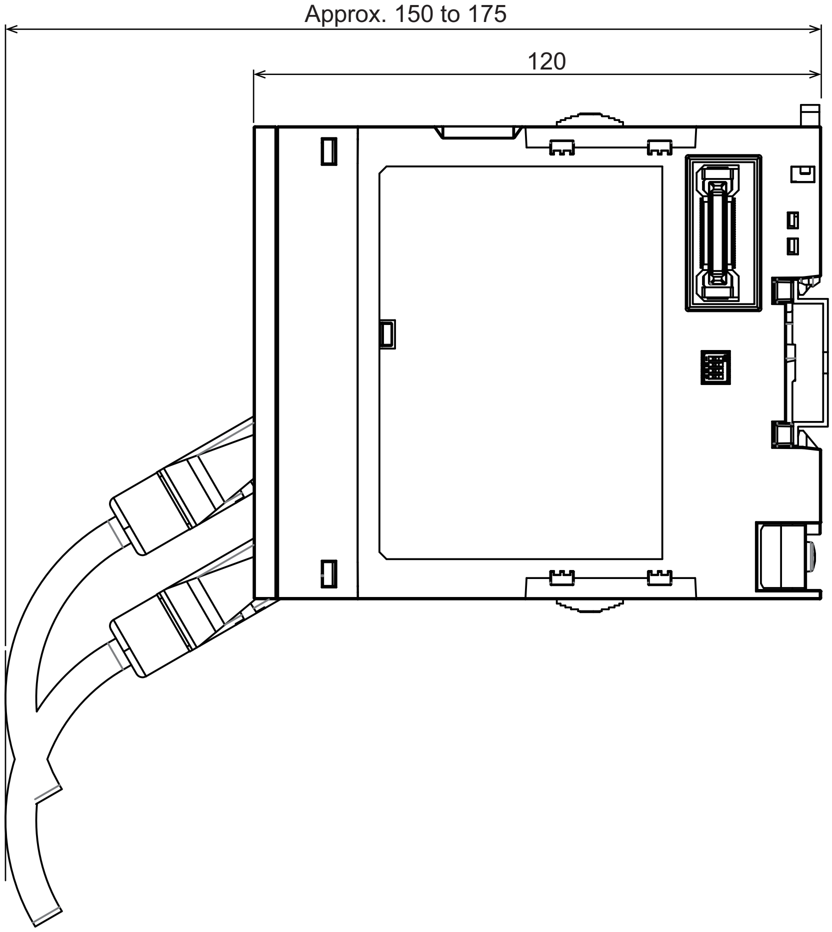
Appendices

The appendices provide datasheets for the NX-series EtherNet/IP Unit, dimensions, and other information.

A-1 Dimensions



Installation Height



(Unit: mm)

The dimension from the back of the Unit to the communications cable varies depending on the cable connector. Use the following dimensions as a guide.

Cable connector		Dimension from the back of the Unit to the cable
Manufacturer	**Model**	
Panduit Corporation	MPS588-C	Approx. 150 mm
OMRON	XS6G-T421-1	Approx. 175 mm

A-2 Functional Comparison of EtherNet/IP Ports on NJ/NX-series CPU Units and Other Series

OK: Supported, ---: Not supported

Item	Built-in EtherNet/IP port on NX701 CPU Unit	Built-in EtherNet/IP port on NX502 CPU Unit	Built-in EtherNet/IP port on NX102 CPU Unit	Built-in EtherNet/IP port on NX1P2 CPU Unit	Built-in EtherNet/IP port on NJ-series CPU Unit	NX-series EtherNet/IP Unit	CJ-series Ethernet Unit	EtherNet/IP Unit (built-in port on CJ2 CPU Unit)		
								Unit version 1.0	Unit version 2.0	Unit version 2.1
Tag data link communications service	OK	OK	OK	OK	OK	OK	---	OK	OK	OK
CIP message communications service	OK	OK	OK	OK	OK	OK	---	OK	OK	OK
IP routing	OK	OK	OK	---	---	OK	---	---	---	---
Socket service	OK	OK	OK	OK	OK	---	OK	---	---	---
FTP server	OK	OK	OK	OK	OK	---	OK	---	OK	OK
FTP client	OK	OK	OK	OK	OK	---	---	---	---	---
Mail send/receive	---	---	---	---	---	---	OK	---	---	---
Web functions	---	---	---	---	---	---	OK	---	---	---
Automatic adjustment of PLC/Controller’s internal clock	OK	OK	OK	OK	OK	---	OK	---	OK	OK
Error history	OK[*1]	OK[*1]	OK[*1]	OK[*1]	OK[*1]	OK[*1]	OK	OK	OK	OK
Response to PING command	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
SNMP/SNMP trap	OK	OK	OK	OK	OK	OK	---	---	OK	OK
CIDR function for IP addresses	OK	OK	OK	OK	OK	OK	---	---	OK	OK
DHCP client	---	OK	---	---	---	---	---	---	---	---
Online connection via EtherNet/IP using CX-One	---	---	---	---	---	---	OK	---	OK	OK
Online connection via EtherNet/IP using Network Configurator	OK	OK	OK	OK	OK	OK	---	OK	OK	OK
Mounting in an NJ-series CPU Unit	---	---	---	---	---	---	---	---	---	OK[*2]

Item	Built-in EtherNet/IP port on NX701 CPU Unit	Built-in EtherNet/IP port on NX502 CPU Unit	Built-in EtherNet/IP port on NX102 CPU Unit	Built-in EtherNet/IP port on NX1P2 CPU Unit	Built-in EtherNet/IP port on NJ-series CPU Unit	NX-series EtherNet/IP Unit	CJ-series Ethernet Unit	EtherNet/IP Unit (built-in port on CJ2 CPU Unit)		
								Unit version 1.0	Unit version 2.0	Unit version 2.1
Connection settings using the Sysmac Studio	OK	OK	OK	OK	OK	OK	---	---	---	OK

*1. This is equivalent to the event log in the EtherNet/IP of an NJ-series Controller.

*2. You cannot use the following functions if you connect to the CPU Unit through an EtherNet/IP Unit.

- Placing the Sysmac Studio online with the CPU Unit (However, you can place the Network Configurator online)
- Using the Troubleshooter of an NS-series PT

A-3 Use the Sysmac Studio to Set the Tag Data Links (EtherNet/IP Connections)

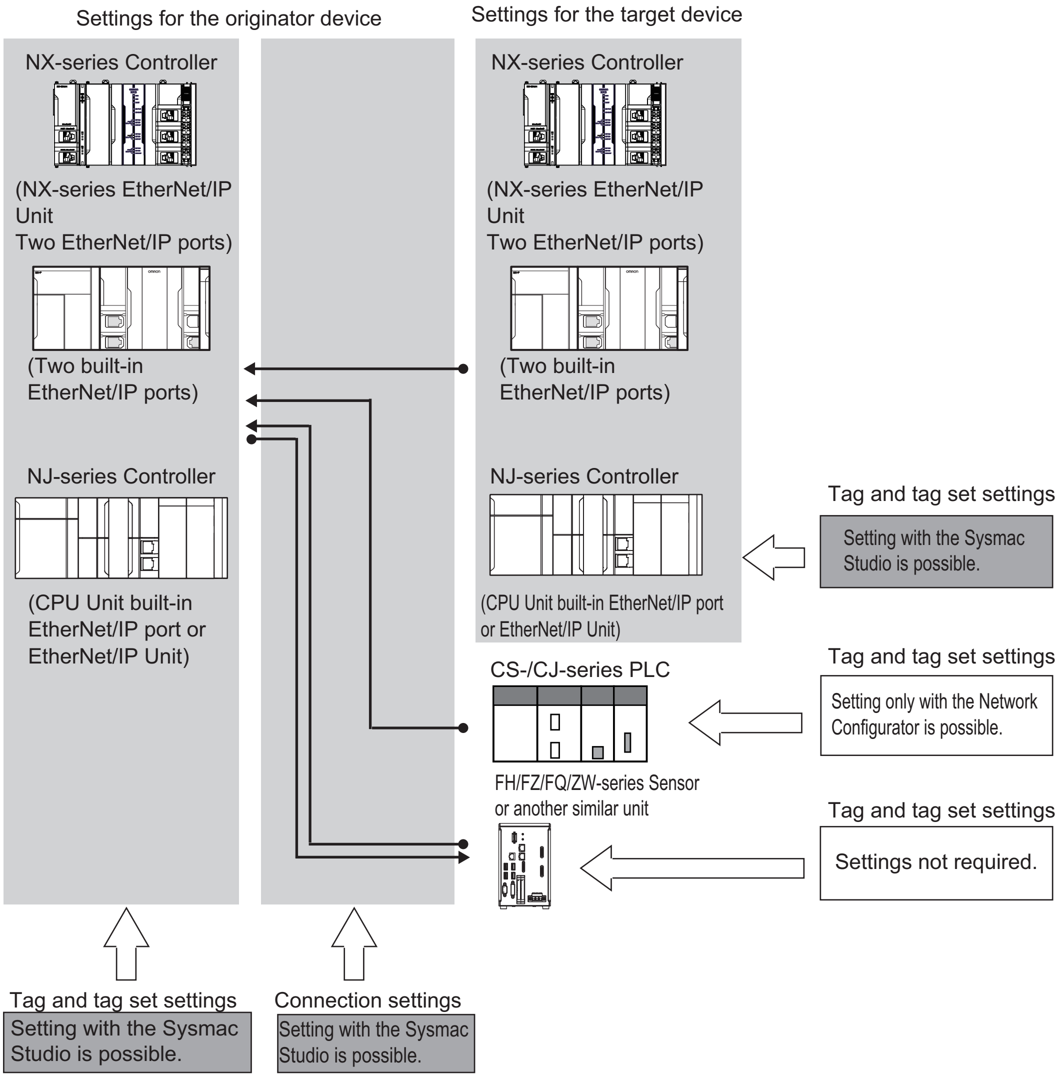
A-3-1 Overview of the Tag Data Links (EtherNet/IP Connections) Settings with the Sysmac Studio

You can use the Sysmac Studio to set the settings required for creating tag data links (EtherNet/IP connections)*1 on the NX-series EtherNet/IP Units.

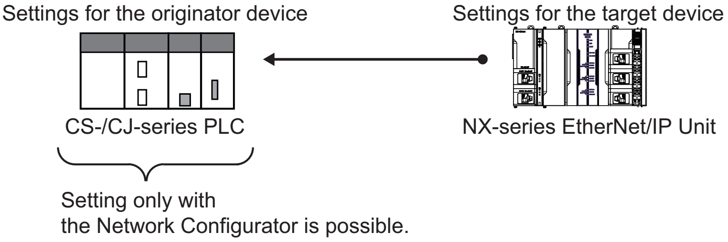
*1. The tag data links and EtherNet/IP connections enable cyclic tag data exchanges on an EtherNet/IP network between Controllers or between Controllers and other devices. Here, "EtherNet/IP connection" refers to both the tag data links and the EtherNet/IP connections.

Acceptable System Configuration Conditions for Setting the EtherNet/IP Connection Settings on the Sysmac Studio

If an NX-series EtherNet/IP Unit operates as the originator device, you can use the Sysmac Studio to set the originator device settings for the EtherNet/IP connections.
Similarly, if an NX-series EtherNet/IP Unit operates as the target device, you can use the Sysmac Studio to set the tags and tag sets of the target device.


Settings for the originator device
Settings for the target device
NX-series Controller
(NX-series EtherNet/IP Unit
Two EtherNet/IP ports)
(Two built-in EtherNet/IP ports)
NJ-series Controller
(CPU Unit built-in EtherNet/IP port or EtherNet/IP Unit)
NX-series Controller
(NX-series EtherNet/IP Unit
Two EtherNet/IP ports)
(Two built-in EtherNet/IP ports)
NJ-series Controller
(CPU Unit built-in EtherNet/IP port or EtherNet/IP Unit)
CS-/CJ-series PLC
FH/FZ/FQ/ZW-series Sensor or another similar unit
Tag and tag set settings
Setting with the Sysmac Studio is possible.
Tag and tag set settings
Setting only with the Network Configurator is possible.
Tag and tag set settings
Settings not required.
Tag and tag set settings
Setting with the Sysmac Studio is possible.
Connection settings
Setting with the Sysmac Studio is possible.

Use the Network Configurator if a CS/CJ-series PLC operates as the originator device.


Settings for the originator device
Settings for the target device
CS-/CJ-series PLC
NX-series EtherNet/IP Unit
Setting only with the Network Configurator is possible.

A-3-2 Procedure to Make the EtherNet/IP Connection Settings with the Sysmac Studio

1 Registering devices		• Main Window
↓	Register devices with which the EtherNet/IP connections are established to the project.	
2 Creating network variables[*1]	--- Refer to *Registering the Network Variable for the Originator Device* on page A-13.	Setup Window Global Variable Table on the Sysmac Studio

↓			
3 Registering tags and tag sets	---	Refer to *Registering the Tag and Tag Set* on page A-14.	EtherNet/IP Connection Settings (Tag Set Display)
↓	Register the network variables that are set in step 2 as tags and tag sets.		
4 Setting connections	---	Refer to *Setting Connections for the Originator Device* on page A-17.	EtherNet/IP Connection Settings (Connection Display)
↓	Specify devices (i.e., target devices and originator devices) and tag sets to communicate with using the EtherNet/IP connections.		
5 Going online from the Sysmac Studio	---	Refer to *Transferring the Connection Settings Data* on page A-28.	• Main Window
↓			
6 Downloading EtherNet/IP connection settings Note Connections automatically start after the download.	---	Refer to *Transferring the Connection Settings Data* on page A-28.	• Synchronization Window/ Transfer to Controller Dialog Box • EtherNet/IP Connection Settings
↓			
7 Checking operation Stopping and starting connections	---	Refer to *A-3-5 Checking Communications Status with the Sysmac Studio and Troubleshooting* on page A-32.	EtherNet/IP Connection Monitor Tab Page

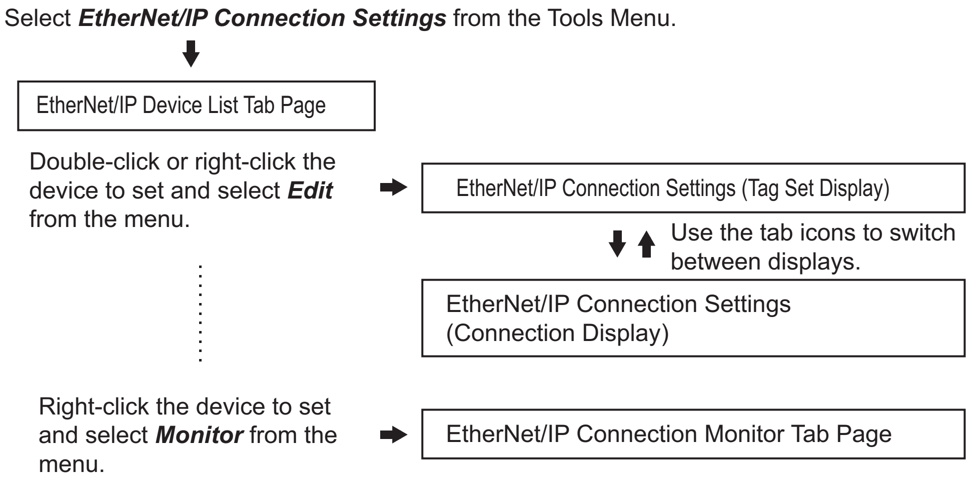
*1. Variables with its Network Publish attribute set to **Output** or **Input** in the Global Variable Table are called network variables.

A-3-3 EtherNet/IP Connection Settings

This section describes the screen configuration for EtherNet/IP connection settings.

Screen Transitions in the EtherNet/IP Connection Settings

- Connection Settings


Select ***EtherNet/IP Connection Settings*** from the Tools Menu.
EtherNet/IP Device List Tab Page
Double-click or right-click the device to set and select ***Edit*** from the menu.
EtherNet/IP Connection Settings (Tag Set Display)
Use the tab icons to switch between displays.
EtherNet/IP Connection Settings (Connection Display)
Right-click the device to set and select ***Monitor*** from the menu.
EtherNet/IP Connection Monitor Tab Page

- Transferring connection settings to the Controller from the computer

Select ***Synchronization*** from the Controller Menu.
↓
Synchronization Window

Select ***Transfer - To Controller*** from the Controller Menu.
↓
Transfer to Controller Dialog Box

Select ***EtherNet/IP Connection Settings*** from the Tools Menu to display the device list.
Right-click the device and select ***Edit*** from the menu.
↓
EtherNet/IP Connection Settings Tab Page

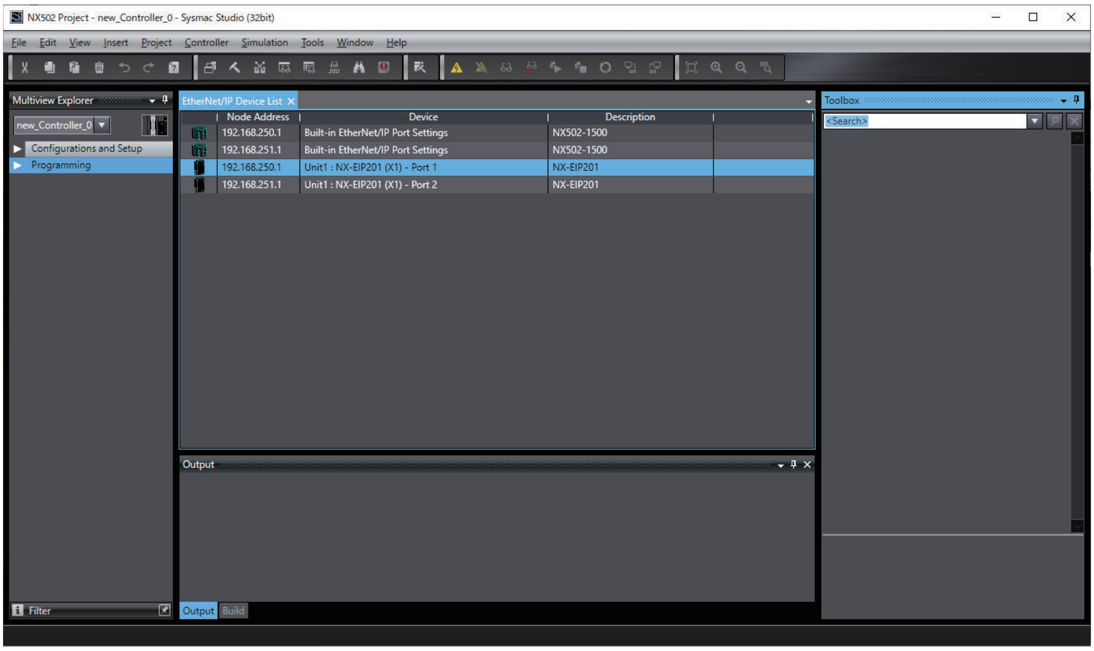
Precautions for Correct Use

To transfer only the connection settings, execute Transfer from the EtherNet/IP Connection Setting Tab Page.
Even if you clear the **Do not transfer the connection setting** Check Box, the connection settings are not transferred from the Synchronization Window, the **Transfer to the Controller** Dialog Box, or the **Transfer from the Controller** Dialog Box as long as the data in the computer is synchronized with the data in the Controller.

EtherNet/IP Device List Tab Page

The list indicates the devices to which EtherNet/IP connections can be set.

For information on how to access this tab page, refer to *Registering the Tag and Tag Set* on page A-14.



Node Address	Device	Description
192.168.250.1	Built-in EtherNet/IP Port Settings	NX502-1500
192.168.251.1	Built-in EtherNet/IP Port Settings	NX502-1500
192.168.250.1	Unit1 : NX-EIP201 (X1) - Port 1	NX-EIP201
192.168.251.1	Unit1 : NX-EIP201 (X1) - Port 2	NX-EIP201

EtherNet/IP Connection Settings (Tag Set Display)

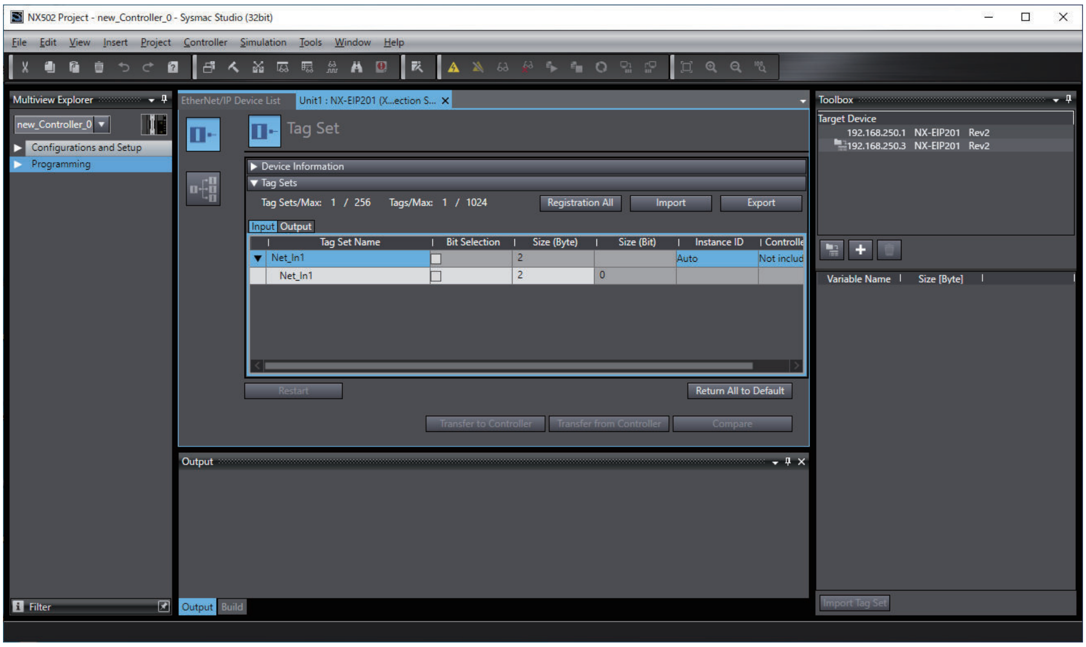
Register tag sets required to create connections.

Each tag set represents the data that is sent and received through a connection. You can register up to eight tags in one tag set.

The name and size of the tag must be the same as those of the network variable [*1]. Set whether to include the Controller status information in tags for the tag sets. You can also set the data output operation at a fatal error occurrence for output tags.

Refer to *Registering the Tag and Tag Set* on page A-14 for information on how to register tags and tag sets.

[*1] A variable with its **Network Publish attribute** set to **Output** or **Input** in the Global Variable Table is called a network variable.



Tag Sets/Max: 1 / 256 Tags/Max: 1 / 1024

	Tag Set Name	Bit Selection	Size (Byte)	Size (Bit)	Instance ID	Controlle
▼	Net_In1	☐	2		Auto	Not includ
	Net_In1	☐	2	0		

EtherNet/IP Connection Settings (Connection Display)

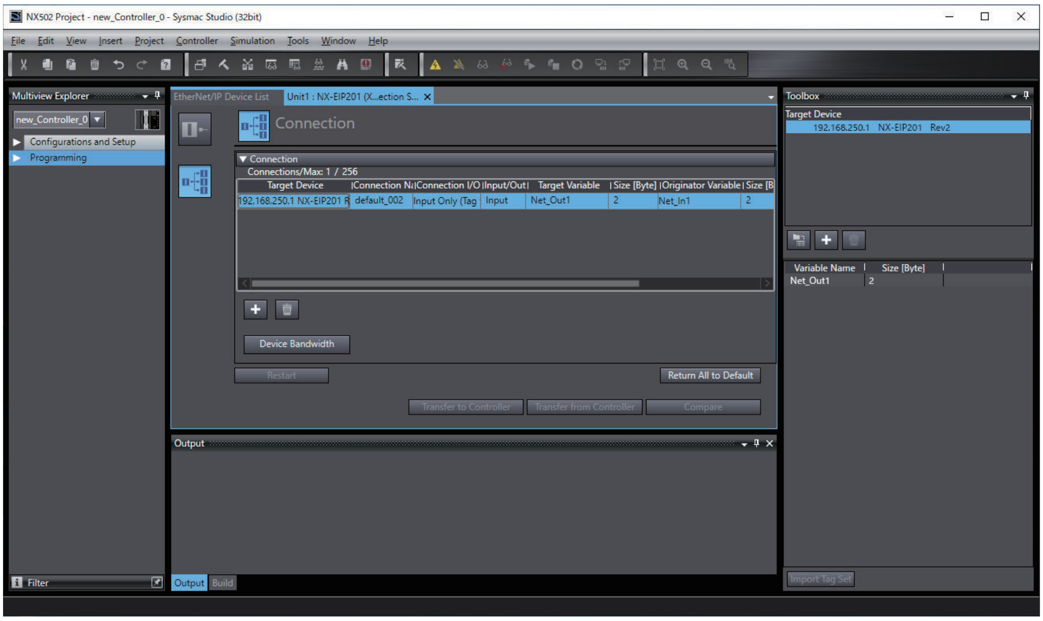
Specify the target devices and set their connections.

For each connection, set the following information: Connection Name, Connection I/O Type, I/O, target device tag set (target variable), originator device tag set (originator variable), Packet Interval (RPI), and Timeout Value.

Refer to *Setting Connections for the Originator Device* on page A-17 for information on how to make connection settings.

Precautions for Correct Use

If you changed the IP address, model, or revision of the target device after making the connection settings, change the connection settings entirely.



Connection
Connections/Max: 1 / 256

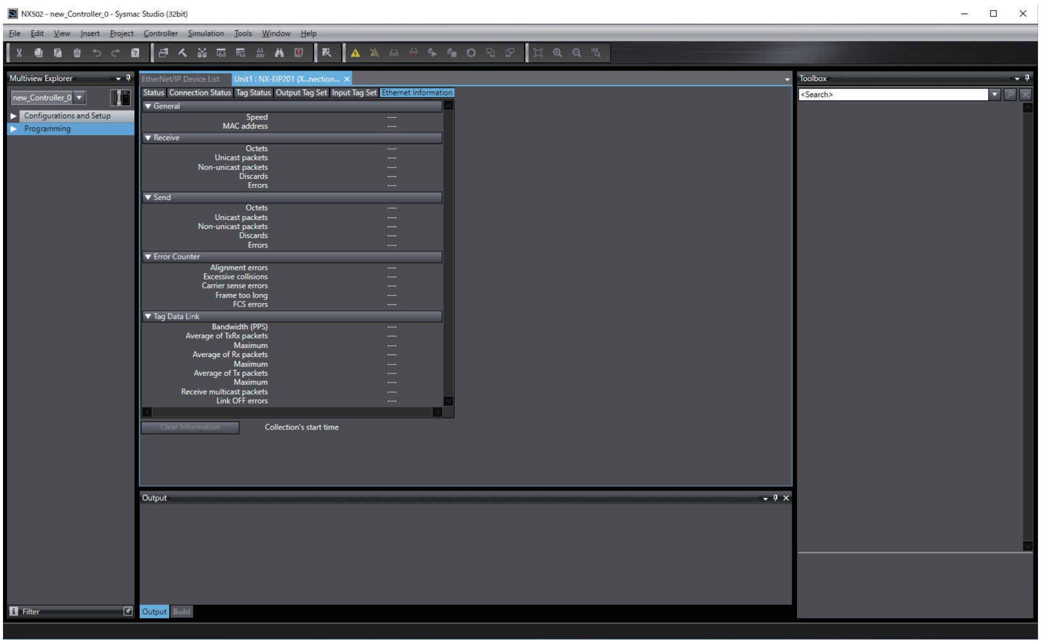
Target Device	Connection Na	Connection I/O	Input/Out	Target Variable	Size [Byte]	Originator Variable	Size [B
192.168.250.1 NX-EIP201 R	default_002	Input Only (Tag	Input	Net_Out1	2	Net_In1	2

Variable Name	Size [Byte]
Net_Out1	2

EtherNet/IP Connection Monitor Tab Page

You can check the EtherNet/IP connection setting status offline and communications status online. When online, you can start and stop connections.

Refer to *A-3-5 Checking Communications Status with the Sysmac Studio and Troubleshooting* on page A-32 for information on how to check the EtherNet/IP connection setting status and communications status.



General
Speed ---
MAC address ---

Receive
Octets ---
Unicast packets ---
Non-unicast packets ---
Discards ---
Errors ---

Send
Octets ---
Unicast packets ---
Non-unicast packets ---
Discards ---
Errors ---

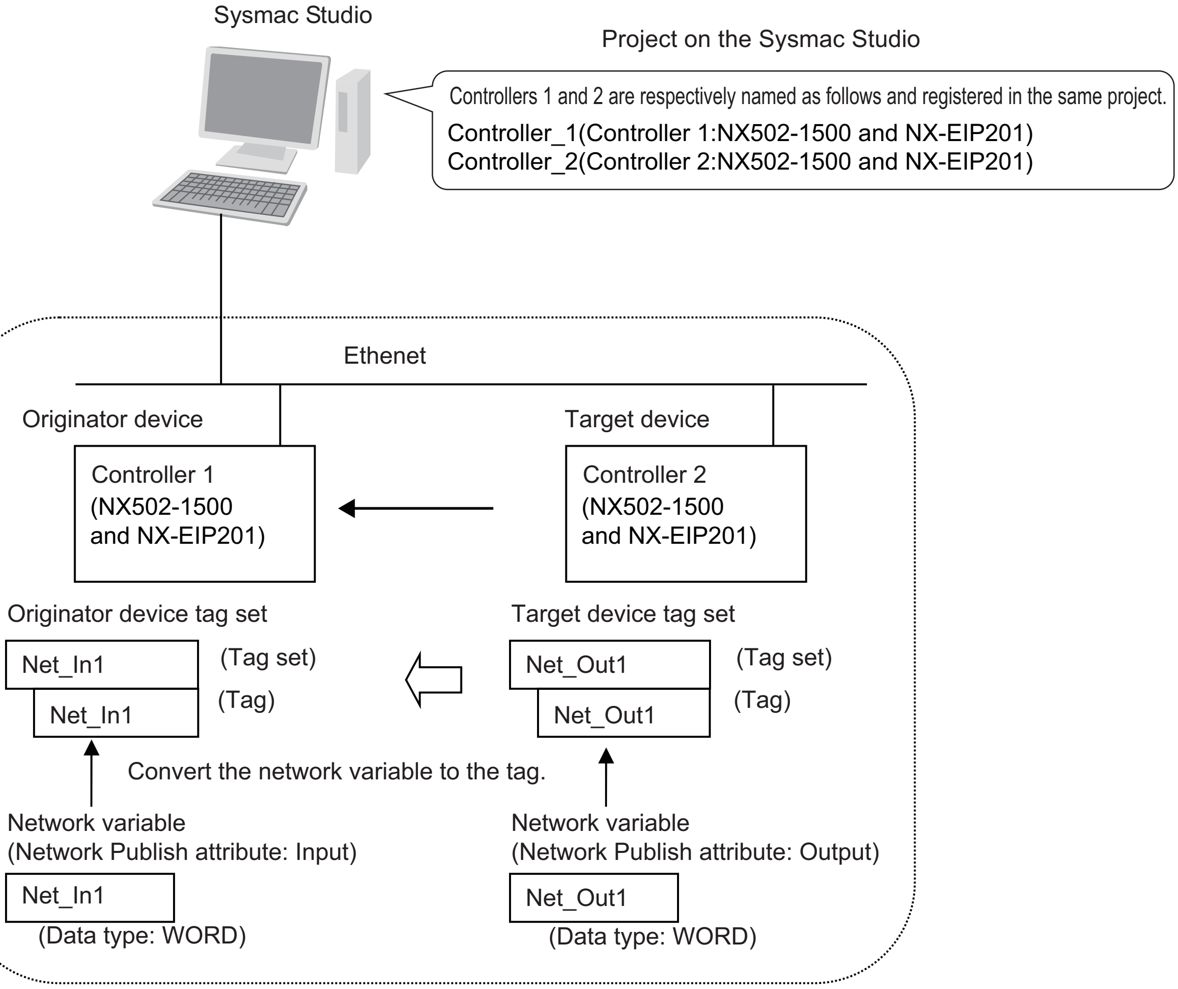
Error Counter
Alignment errors ---
Excessive collisions ---
Carrier sense errors ---
Frame too long ---
FCS errors ---

Tag Data Link
Bandwidth (PPS) ---
Average of TxRx packets ---
Maximum ---
Average of Rx packets ---
Maximum ---
Average of Tx packets ---
Maximum ---
Receive multicast packets ---
Link OFF errors ---

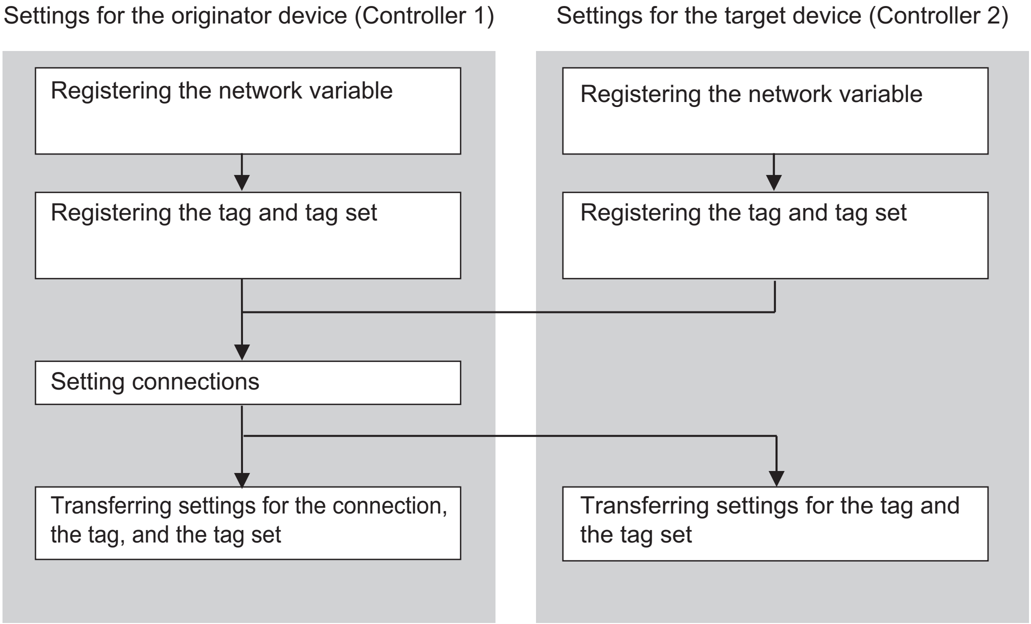
A-3-4 Making the EtherNet/IP Connection Settings with the Sysmac Studio

This section describes the procedure to make the EtherNet/IP connection settings with the Sysmac Studio.
Here, we take the following system configuration as an example to describe how to set the EtherNet/IP connection settings.
Example: System that connects the EtherNet/IP port on Controller 1 and the EtherNet/IP port on Controller 2 via Ethernet

- Set the settings so that values in the network variable Net_Out1 allocated for Controller 2 are sent to the network variable Net_In1 allocated for Controller 1 at the set RPI of 50 ms cycle.
- This example assumes the programs for both Controllers 1 and 2 are registered in the same project.


Sysmac Studio
Project on the Sysmac Studio
Controllers 1 and 2 are respectively named as follows and registered in the same project.
Controller_1(Controller 1:NX502-1500 and NX-EIP201)
Controller_2(Controller 2:NX502-1500 and NX-EIP201)
Ethenet
Originator device
Target device
Controller 1 (NX502-1500 and NX-EIP201)
Controller 2 (NX502-1500 and NX-EIP201)
Originator device tag set
Target device tag set
Net_In1
(Tag set)
Net_In1
(Tag)
Net_Out1
(Tag set)
Net_Out1
(Tag)
Convert the network variable to the tag.
Network variable
(Network Publish attribute: Input)
Net_In1
(Data type: WORD)
Network variable
(Network Publish attribute: Output)
Net_Out1
(Data type: WORD)

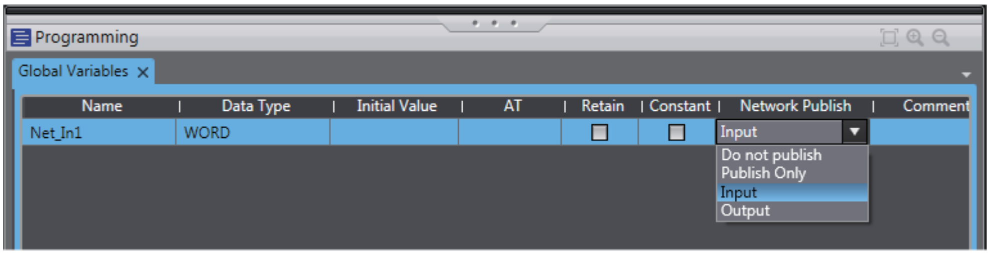
Follow the flow below to set the settings to Controllers 1 and 2 for which to establish EtherNet/IP connections.
The required settings for the originator device and the target device are shown below.


Settings for the originator device (Controller 1)
Settings for the target device (Controller 2)
Registering the network variable
Registering the tag and tag set
Setting connections
Transferring settings for the connection, the tag, and the tag set
Registering the network variable
Registering the tag and tag set
Transferring settings for the tag and the tag set

Registering the Network Variable for the Originator Device

Register the network variable that is sent and received using the EtherNet/IP connections.
Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for the operations for registering variables.

1 Assign the network variable to the tag used for the EtherNet/IP connection for Controller 1 (originator device).
This network variable receives data from Controller 2 (target device).
Select **Input** or **Output** for **Network Publish** of a variable in the Global Variable Table so that the variable can serve as a network variable, i.e. the variable can be used for the EtherNet/IP connections.
In this example, set the network variable for Controller 1 as shown below.



Name	Data Type	Initial Value	AT	Retain	Constant	Network Publish	Comment
Net_In1	WORD			☐	☐	Input	

- Variable name: Net_In1
- Data type: WORD
- Network Publish attribute: Input

● Network Variables Used for EtherNet/IP Connections

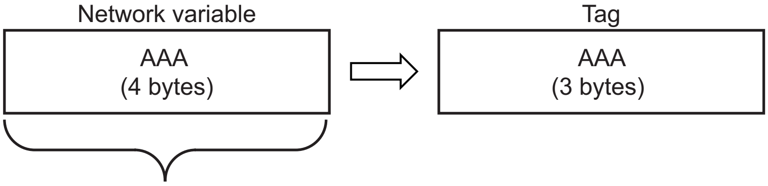
- Network variable name

You cannot specify an I/O memory address for a tag name in the EtherNet/IP connection settings. Thus, do not specify an I/O memory address for the network variable name that is to be assigned to a tag.
The following text strings are recognized as the I/O memory address names.

1. Variable names that contain only single-byte numerals from 0000 to 6143
2. Variable names with the following single-byte letters (uppercase or lowercase) followed by single-byte numerals
   - H (H000 to H511)
   - W (W000 to W511)
   - D (D00000 to D32767)
   - E0_ to E18_(E0_00000 ... E0_32767 to E18_00000 ... E18_32767)

To specify an I/O memory address for tag, do not specify I/O memory the address directly. Instead, create a variable with an AT specification of the I/O memory address on the Sysmac Studio, and then specify the variable for the tag.

- Size of variables
  To use an EtherNet/IP Unit as an EtherNet/IP device, set an even number of bytes for the size of the network variable used for the EtherNet/IP connections regardless of an odd number of bytes for the tag size.



The CPU Unit memory is consumed in units of two bytes. To assign tags of odd numbers of bytes to network variables, specify even byte numbers (i.e., sizes of the tags + 1) to the network variables.

- Data concurrency
  To maintain concurrency in the values of network variables that are assigned to tags, you must set refreshing tasks.
  Refer to *9-1-7 Concurrency of Tag Data Link Data* on page 9-12 for details.

Registering the Tag and Tag Set

Register the required tag and tag set for the EtherNet/IP connections.
You can register tags and tag sets in the EtherNet/IP Connection Setting Tab Page.

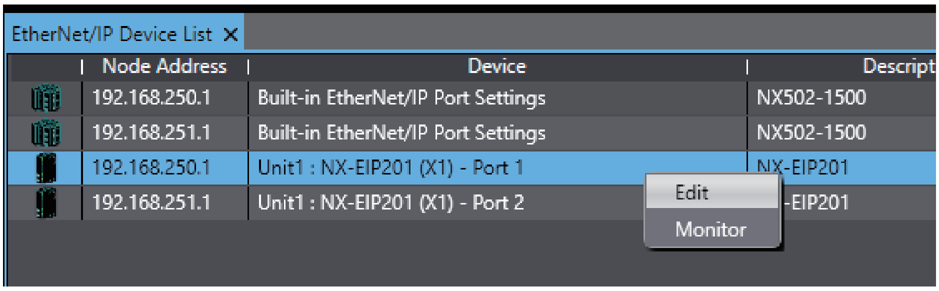
Precautions for Correct Use

Make the following settings to refresh all of the tag data in the same tag set at the same time.
- Use the Sysmac Studio, in advance, to specify the same refreshing task for all of the variables that are assigned to tags in the tag set.
- Do not place tag variables that have AT specifications in I/O memory and tag variables that do not have AT specifications in the same tag set.

1 Select **EtherNet/IP Connection Settings** from the **Tools** Menu.

The EtherNet/IP Device List Tab Page is displayed.

2 In this example, right-click **EtherNet/IP Port Settings** for the originator device and select **Edit** from the menu to open the EtherNet/IP Connection Setting Tab Page.



EtherNet/IP Device List

	Node Address	Device	Descript
	192.168.250.1	Built-in EtherNet/IP Port Settings	NX502-1500
	192.168.251.1	Built-in EtherNet/IP Port Settings	NX502-1500
	192.168.250.1	Unit1 : NX-EIP201 (X1) - Port 1	NX-EIP201
	192.168.251.1	Unit1 : NX-EIP201 (X1) - Port 2	NX-EIP201

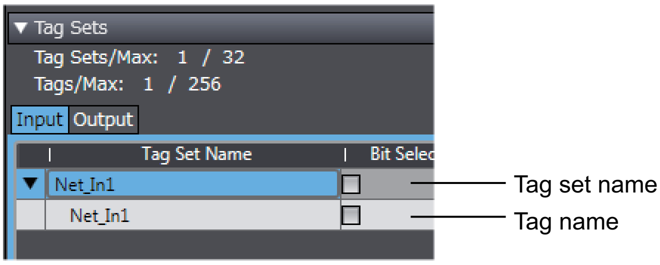
3 Click the (Show Tag Set Display) icon in the EtherNet/IP Connection Setting Tab Page.

4 Click the **Input** tab to switch to the **Input** Tab Page. Register the tag set and the tag. Use one of the following methods to register the tag set and the tag.

- Independent registration : Manually registers network variables in the Controller as tags.
- Batch registration : Registers all network variables in the Controller as tags at the same time.

5 Register tags and tag sets independently.

1) Right-click anywhere in the Input Tab Page of the EtherNet/IP Connection Setting Tab Page and select **Create New Tag Set** from the menu.
2) Enter the tag set name, *Net_In1*, directly into the list in the **Input** Tab Page.
3) Right-click anywhere in the Input Tab Page and select **Create New Tag** from the menu.
4) Enter tag name *Net_In1*.



▼ Tag Sets
Tag Sets/Max: 1 / 32
Tags/Max: 1 / 256

	Tag Set Name	Bit Selec
▼	Net_In1	☐
	Net_In1	☐

Precautions for Correct Use

Any name can be specified for the tag set if the name matches one of the registered network variable names in the Controller.
As you enter characters (or immediately after you press the Ctrl + Space Keys), the Sysmac Studio Entry Assistance provides a list of variable names registered in the Controller. Select the variable name from the list.

Additional Information

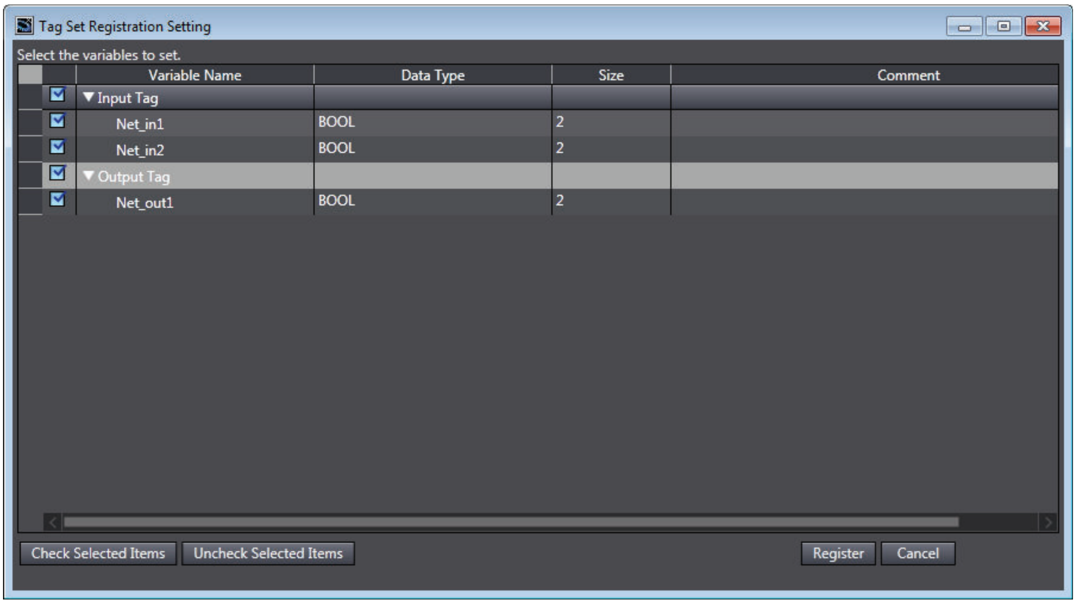
You can register up to 8 tags in a tag set.
Set as shown below to register multiple tags.
Examples:

	Tag set name	
▼	Network_Input_Value	.... (Tag set name)
	Net_In1	.... (Tag name)
	Net_In2	.... (Tag name)

6 Register all tags and tag sets at the same time.

1) Right-click anywhere on the Input Tab Page of the EtherNet/IP Connection Settings Tab Page and select **Register All Tag Sets** or click the **Registration All** Button to display the **Tag Set Registration Setting** Dialog Box.

   This dialog box lists the variables that are registered in the Global Variable Table and also have the **Network Publish** attribute set to **Input** or **Output**.



Tag Set Registration Setting

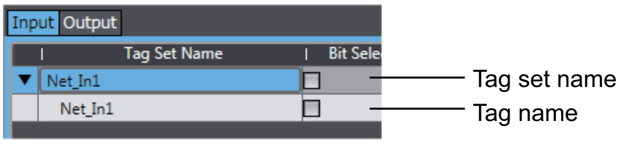
Select the variables to set.

	Variable Name	Data Type	Size	Comment
☑	▼ Input Tag			
☑	Net_in1	BOOL	2	
☑	Net_in2	BOOL	2	
☑	▼ Output Tag			
☑	Net_out1	BOOL	2	

2) Select the variable to register as a tag, and then click the **Register** Button.

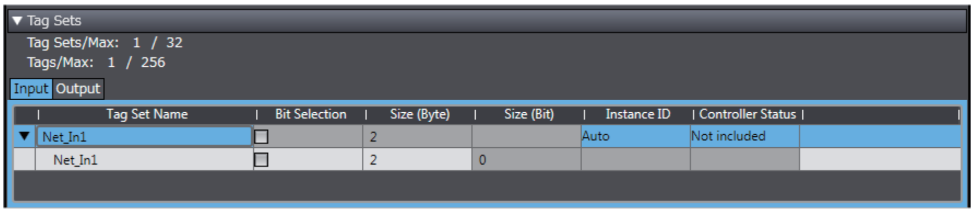
3) The automatically registered tag is added to the list in the EtherNet/IP Connection Setting Tab Page.

   With automatic registration, the tag is registered under a tag set having the same name as the tag, i.e., a single tag is registered in a single tag set.



	Tag Set Name	Bit Sele
▼	Net_In1	☐
	Net_In1	☐

7 Set the following settings for the registered tag and tag set.



▼ Tag Sets
Tag Sets/Max: 1 / 32
Tags/Max: 1 / 256

	Tag Set Name	Bit Selection	Size (Byte)	Size (Bit)	Instance ID	Controller Status
▼	Net_In1	☐	2		Auto	Not included
	Net_In1	☐	2	0		

- Setting for Tag Sets

Name	Item
Tag Set Name	Enter the tag set name. You can change the names as required.
Size (Byte)	Gives the total size of the tag in bytes.
Instance ID	Gives the instance ID. • Auto • IN_{min}...IN_{max} {min} represents the minimum number of Produced Assembly identification numbers recorded in the EDS files for the relevant devices. {max} represents the maximum number of Produced Assembly identification numbers recorded in the EDS files for the relevant devices.
Controller Status	Specify whether to include the Controller status in the tag set.

- Setting for Tags

Name	Item
Tag Name	Enter the tag name. Specify the tag name that matches one of the registered network variable names in the Controller.
Bit Selection	Specify whether to set the tag data size in bits. Selected: Set the size in bits. Not selected: Set the size in bytes.
Size (Byte)	Gives the size of the tag in bytes.
Size (Bit)	Gives the size of the tag in bits.
Output at Fatal Error	Specify whether to clear the output data or continue to send it when a major fault level Controller error occurs in the Controller. • Retained • Cleared

Setting Connections for the Originator Device

After the tag set registration, set the connection settings for transferring data using the EtherNet/IP connections.
Make the connection settings in the originator device (i.e., Controller 1 in this example) only.

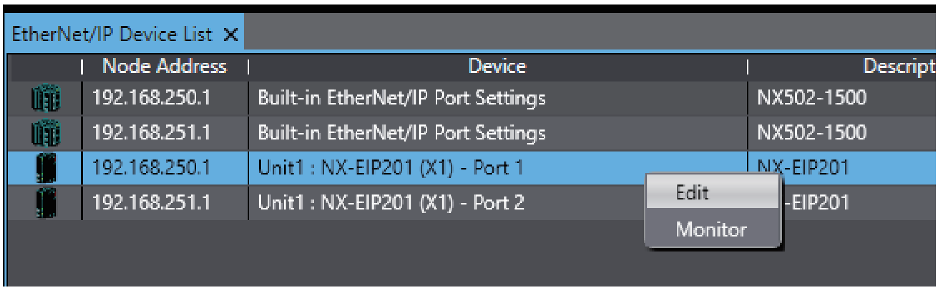
Register the tag and tag set for Controller 2 (Target device) before setting the connection settings as described in this example.
Refer to *Registering the Tag and Tag Set for the Target Device* on page A-25 for the operations for registering tags and tag sets.

Precautions for Correct Use

If you change the IP address, model, or revision of the target device after making the connection settings, you must also change the target device settings that are included in the connection settings.
For information on how to change the target device settings in the connection settings, refer to *Changing the Target Device Settings after Making Connection Settings* on page A-23.

1 Select **EtherNet/IP Connection Settings** from the **Tools** Menu to display the EtherNet/IP Device List Tab Page.

2 Right-click **EtherNet/IP Port Settings** for Controller 1 (originator device in this example), and select **Edit** from the menu.
The EtherNet/IP Connection Settings Tab Page is displayed.



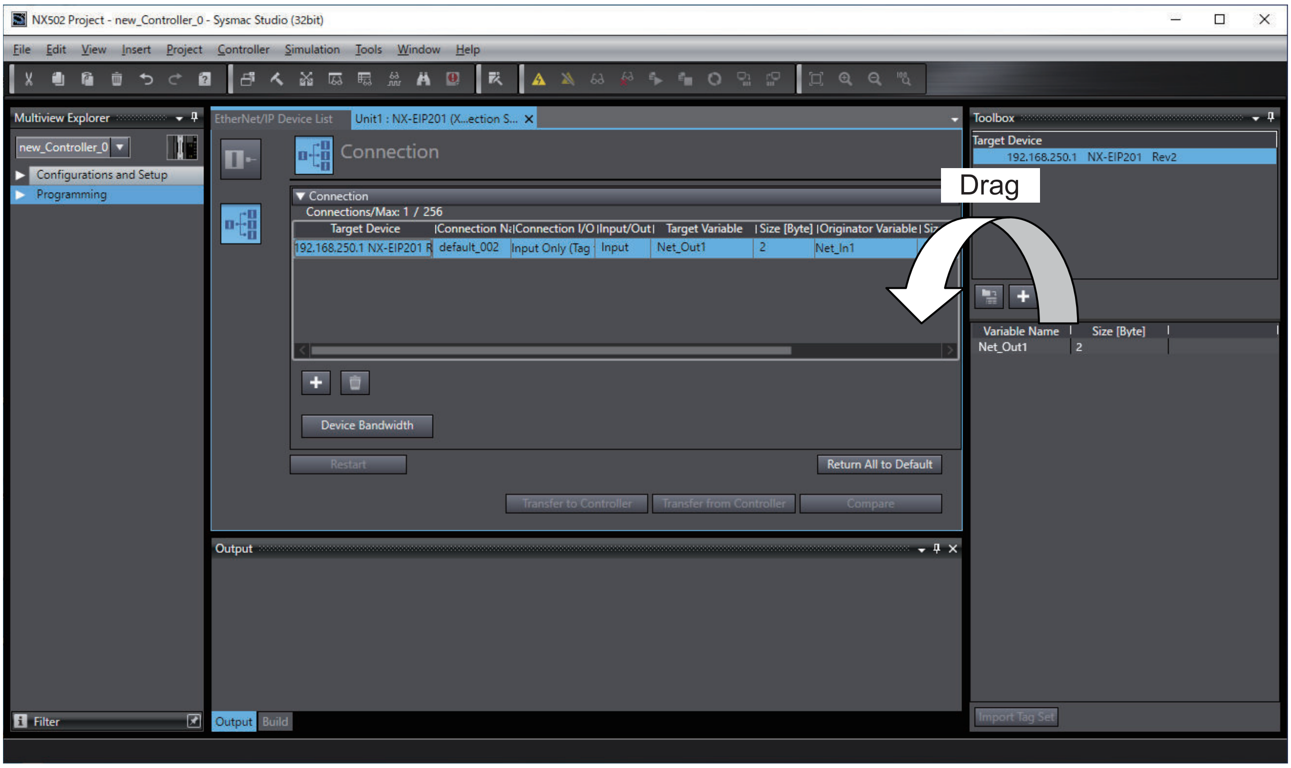
EtherNet/IP Device List

Node Address	Device	Descript
192.168.250.1	Built-in EtherNet/IP Port Settings	NX502-1500
192.168.251.1	Built-in EtherNet/IP Port Settings	NX502-1500
192.168.250.1	Unit1 : NX-EIP201 (X1) - Port 1	NX-EIP201
192.168.251.1	Unit1 : NX-EIP201 (X1) - Port 2	-EIP201

3 Click the (Show Connection Display) icon in the EtherNet/IP Connection Setting Tab Page.

4 Select **NX-EIP201** from **Target Device** in the Toolbox on the right side of the EtherNet/IP Connection Settings Tab Page.
When you select **NX-EIP201**, the target device tag set (Net_Out1) for Controller 2 is displayed in the **Variable Name** column in the Toolbox.

5 Drag the target device tag set Net_Out1 from the **Variable Name** column in the Toolbox to the Connection List.
As you enter characters (or immediately after you press the Ctrl + Space Keys), a list of target device variables that can be set for the connection is provided. Select the value from the list.



Connection
Connections/Max: 1 / 256

Target Device	Connection Na	Connection I/O	Input/Out	Target Variable	Size [Byte]	Originator Variable	Siz
192.168.250.1 NX-EIP201 R	default_002	Input Only (Tag	Input	Net_Out1	2	Net_In1	

Variable Name	Size [Byte]
Net_Out1	2

6 Specify **Originator Variable** and its **Size [Byte]** for the tag set Net_Out1 added in step 5.
Here, specify *Net_In1* for **Originator Variable** and *2* for its **Size [Byte]**.
Change the other settings as required.
You can set the following items in the connection settings.

Name	Setting Methods
Target Device	Select the target device.
Connection Name	Any name can be given to the connection (32 single-byte characters max.).
Connection I/O Type	Input Only (Tag type) is selected if the EtherNet/IP connection is established on an NX-EIP201, CS1W-EIP21, CJ1W-EIP21, CJ2B-EIP21, CJ2M-EIP21, CJ1W-EIP21(CJ2), CJ1W-EIP21(NJ), NX701, NX102-□□□□, NX1P2, NJ501-□□□□, NJ301-□□□□, or NJ101. When you create EtherNet/IP connection for another target device, select the connection I/O type specified in the device's EDS file. Use the **Input Only (ID type)** setting when the originator is a node from another manufacturer and does not support connection settings with a Tag type setting.
Input/Output	The connection's input/output is automatically displayed based on the selected connection. Input Only: Just Input is displayed.
Target Variable	Select the target node's tag set to assign it. • Input is specified for **Input/Output**: Select the target's output (produce) tag set. • Output is specified for **Input/Output**: Select the target's input (consume) tag set.
Size [Byte]	The data sizes of the target variables are displayed.

Name	Setting Methods
Originator Variable	Select the originator node's tag set to assign it. • Input is specified for **Input/Output**: Select the originator's input (consume) tag set. • Output is specified for **Input/Output**: Select the originator's output (produce) tag set.
Size [Byte]	Enter the data sizes of the originator variables.
Connection Type	Select whether the data is to be sent in the multicast or unicast (point-to-point) form. The default setting is multicast. • Multi-cast connection: Select when the same data is to be shared by multiple nodes. This setting is usually used. • Point-to-point connection: Select when the same data is not to be shared by multiple nodes. Since the data is sent in unicast transmission, other nodes are not burdened with unnecessary load. **Note** Refer to *9-1-4 Overview of Operation* on page 9-7 for details on how to use multi-cast and unicast connections, and how to count the number of connections.
RPI [ms]	Set the data update cycle (i.e., the packet interval) of each connection between the originator and target. The default setting is 50 ms (i.e., data is updated once every 50 ms).
Timeout Value	Set the time until a connection timeout is detected. 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 RPI x 4. The timeout value must be at least 10 ms.

7 The Toolbox displays the target devices if the devices are registered in the same Sysmac Studio project as where the originator devices are registered.

You can use one of the following methods to add unregistered devices in the same Sysmac Studio project as where the originator devices are registered to the Target Device List.

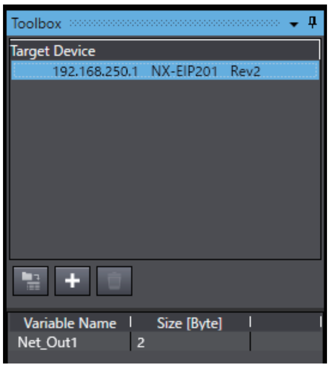
- Importing devices that are registered in another project
  You can import NJ/NX-series Controllers registered in another project data and add them to the Device List.
- Registering devices using user-specified settings
  You can manually add target devices to the device list.

Additional Information

You can add target devices to the Device List by installing EDS files that include connection information for the devices in the Sysmac Studio and register the devices to the project.
Refer to *Adding EDS Files* on page A-22 for details.

8 Import devices that are registered in another project.

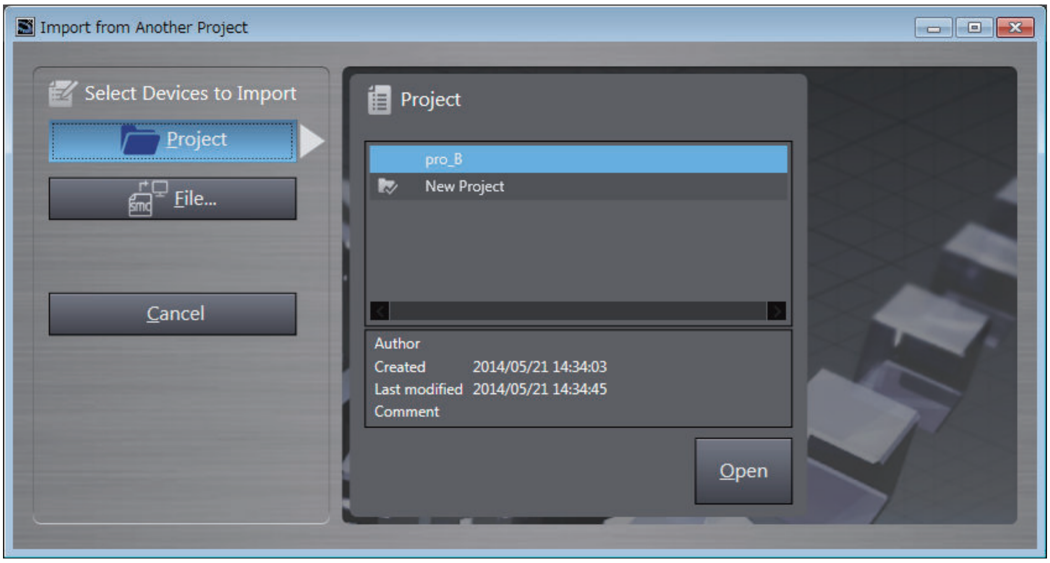
1) Click the (Import a device from another project) Button in the Toolbox on the right of the EtherNet/IP Connection Setting Tab Page.



192.168.250.1 NX-EIP201 Rev2

Variable Name	Size [Byte]
Net_Out1	2

2) The Import from Another Project Dialog Box is displayed. Click the **Project** Button, select a project to import and click the **Open** Button.



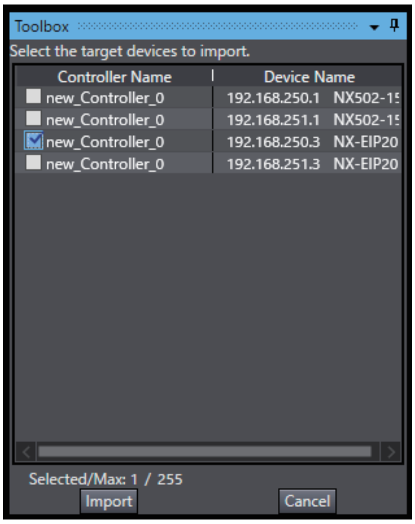
pro_B
New Project

Author
Created 2014/05/21 14:34:03
Last modified 2014/05/21 14:34:45
Comment

3) The list of EtherNet/IP devices registered in the selected project will be displayed. Select the target devices to import, and click the **Import** Button.

Note Only the project for which the EtherNet/IP connection settings are set will be displayed.

The imported EtherNet/IP devices are added to the Target Device List in the Toolbox.



Select the target devices to import.

Controller Name	Device Name
☐ new_Controller_0	192.168.250.1 NX502-1
☐ new_Controller_0	192.168.251.1 NX502-1
☑ new_Controller_0	192.168.250.3 NX-EIP20
☐ new_Controller_0	192.168.251.3 NX-EIP20

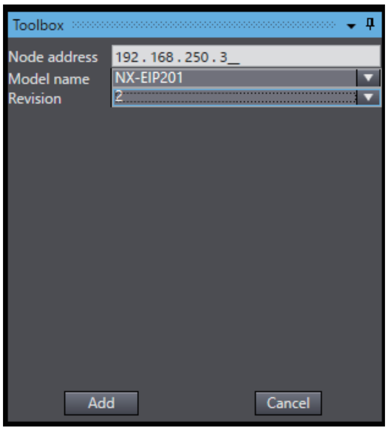
Selected/Max: 1 / 255

9 Register devices as required.

1) Click the + Button under the Target Device List in the Toolbox.

   The Add Target Device Pane is displayed.

2) Enter relevant items for the target devices to add.



Node address: 192 . 168 . 250 . 3_
Model name: NX-EIP201
Revision: 2

Menu	Description
Node address	Enter the target device IP address.
Model name	Select the target device model.
Revision	Select the revision of the target device.

3) Here, set the following items for Controller 3 and click the **Add** Button.

   The target device is added to the Target Device List in the Toolbox.

   Node address: 192.168.250.3

   Model name: NX-EIP201

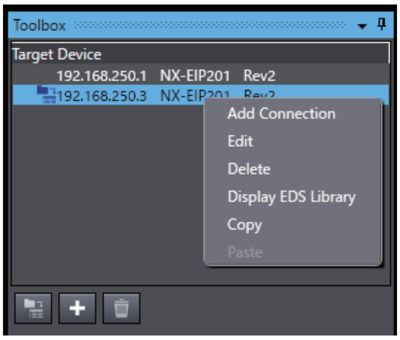
   Revision: 2

4) You can click the **Import Tag Set** Button to import the tag sets that are set in the Network Configurator to the target devices.

   Select **To/From File - Export to File** in the **Tag Sets** Tab Page of the **Edit Device Parameters** Dialog Box, and generate CSV files to import.

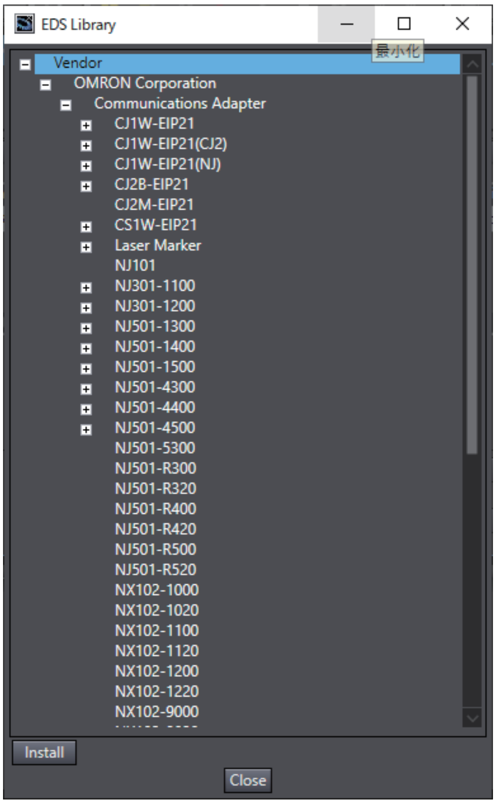
● Adding EDS Files

1 Right-click anywhere in the Target Device List in the Toolbox of the EtherNet/IP Connection Setting Tab Page and select **Display EDS Library** from the menu.



192.168.250.1 NX-EIP201 Rev2
192.168.250.3 NX-EIP201 Rev2

2 The EDS Library Dialog Box is displayed. Click the **Install** Button.



3 Select the EDS file to add, and then click the **Open** Button.
The EDS file is added.

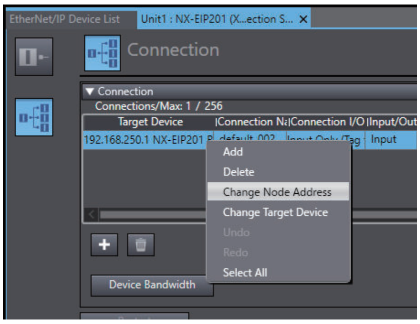
4 The EtherNet/IP device with the EDS file installed is added to the EDS Library.
Devices listed in the EDS Library are used as a candidate device list when adding devices to the Target Device List in the Toolbox of the EtherNet/IP Connection Setting Tab Page.

Changing the Target Device Settings after Making Connection Settings

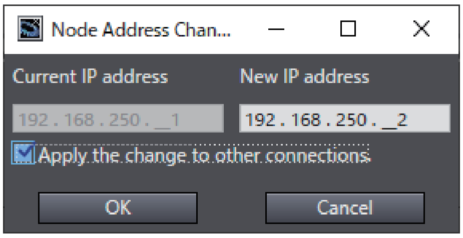
If you change the IP address, model, or revision of the target device after making the connection settings, you must also change the target device settings that are included in the connection settings. You can change the target device settings entirely.

● Changing the IP Addresses for All Target Devices

1 Right-click one of the connection lines and select **Change Node Address** from the menu.



2 The **Node Address Change** Dialog Box is displayed. Enter a new IP address in **New IP address**.
To apply the same change to other connections, select the **Apply the change to other connections** Check Box.



Current IP address: 192 . 168 . 250 . _1
New IP address: 192 . 168 . 250 . _2
☑ Apply the change to other connections

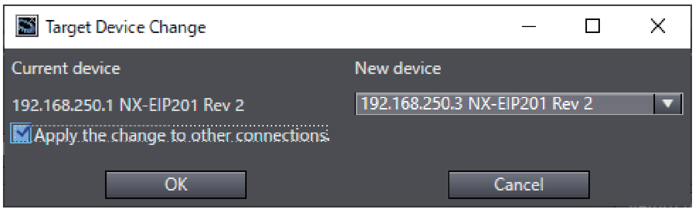
3 To apply the same change to other connections, select the **Apply the change to other connections** Check Box.

4 Click the **OK** Button.

● Changing All Target Device Information including Model Names and Revisions

1 Right-click one of the connection lines and select **Change Target Device** from the menu.

2 The **Target Device Change** Dialog Box is displayed. Select a target device from **New device**.



Current device: 192.168.250.1 NX-EIP201 Rev 2
New device: 192.168.250.3 NX-EIP201 Rev 2
☑ Apply the change to other connections

Precautions for Correct Use

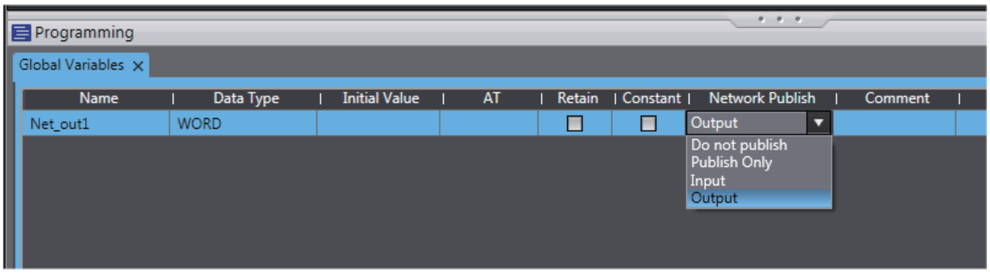
- Changeable target devices are limited to ones that have "OMRON" in the Vendor ID and is an EDS device of the Communications Adapter in the Device Type.
- To display a device in the list of selectable new target devices, the device must be registered as the target device in the Toolbox.

3 To apply the same change to other connections, select the **Apply the change to other connections** Check Box.

4 Click the **OK** Button.

Registering the Network Variable for the Target Device

1 Assign the network variable to the tag used for the EtherNet/IP connection for Controller 2 (target device).
This network variable stores data to send to Controller 1 (originator device).
Set the **Network Publish** attribute to **Input** or **Output** in the Global Variable Table for the variable so that the variable serves as a network variable, i.e., the variable can be used for the EtherNet/IP connections. In this example, set the network variable for Controller 1 as shown below.



Name	Data Type	Initial Value	AT	Retain	Constant	Network Publish	Comment
Net_out1	WORD			☐	☐	Output	

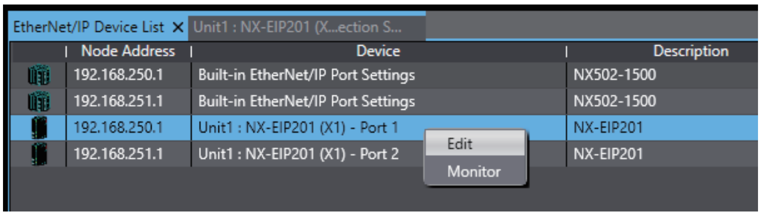
- Name: Net_Out1
- Data type: WORD
- Network Publish attribute: Output

Registering the Tag and Tag Set for the Target Device

Set the tag and tag set for the target device.

1 Select **EtherNet/IP Connection Settings** from the Tools Menu.
The EtherNet/IP Device List Tab Page is displayed.

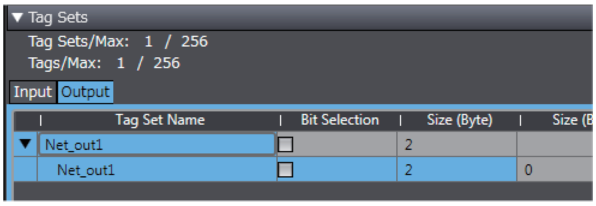
2 Right-click **NX-EIP201**, the NX-series EtherNet/IP Unit connected to the Controller 2 (originator device in this example), and select **Edit** from the menu.
The EtherNet/IP Connection Settings Tab Page is displayed.



Node Address	Device	Description
192.168.250.1	Built-in EtherNet/IP Port Settings	NX502-1500
192.168.251.1	Built-in EtherNet/IP Port Settings	NX502-1500
192.168.250.1	Unit1 : NX-EIP201 (X1) - Port 1	NX-EIP201
192.168.251.1	Unit1 : NX-EIP201 (X1) - Port 2	NX-EIP201

3 Click the (Show Tag Set Display) icon in the EtherNet/IP Connection Setting Tab Page.

4 Click the **Output** tab to switch to the **Output** Tab Page. Register the following tag and tag set. The tag and tag set can be registered in the same way as for the target device. (Refer to *Registering the Tag and Tag Set* on page A-14.)



Tag Sets/Max: 1 / 256
Tags/Max: 1 / 256

Tag Set Name	Bit Selection	Size (Byte)	Size (B
▼ Net_out1	☐	2	
Net_out1	☐	2	0

Checking the Device Bandwidth Usage

The bandwidth usage for the device can be displayed from the EtherNet/IP Connection Setting Tab Page.

This value is for when multicast filtering is used.

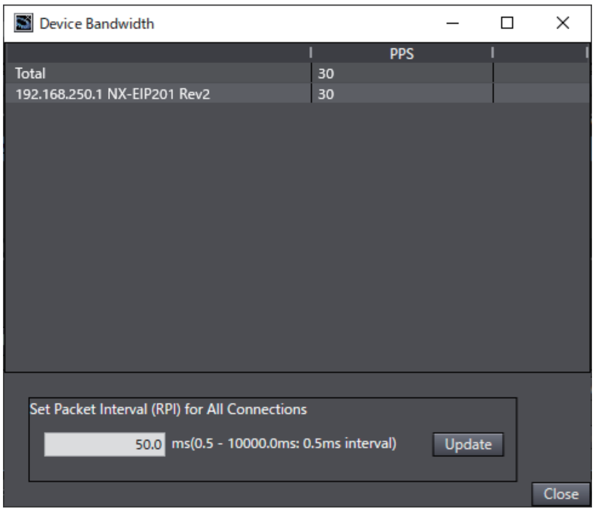
Precautions for Correct Use

In the Device Bandwidth Dialog Box, you can only check the bandwidth being used for the EtherNet/IP connections from one originator device to its target devices.

The actual bandwidth used for the EtherNet/IP network must be calculated by taking into account of all bandwidths used on the EtherNet/IP network (i.e., bandwidths used for connections for the other devices in the EtherNet/IP network than the one given on the dialog box must be included into the calculation).

● Procedure

Click the **Device Bandwidth** Button in the EtherNet/IP Connection Setting Tab Page for the target device.



	PPS
Total	30
192.168.250.1 NX-EIP201 Rev2	30

Set Packet Interval (RPI) for All Connections

50.0 ms(0.5 - 10000.0ms: 0.5ms interval)

Menu	Description
PPS	Gives the bandwidth used for each target device and total bandwidth used for all target devices.
Set Packet Interval (RPI) for All Connections	Changes all Packet Interval (RPI) values for all target devices.

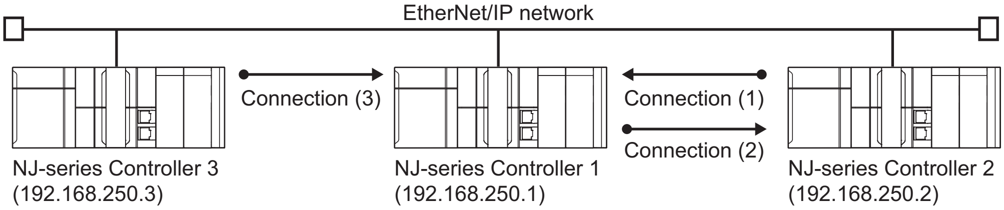
Additional Information

You can specify a value in **Set Packet Interval (RPI) for All Connections** and click the **Update** Button to change packet interval (RPI) values set in the connection settings for all target devices to the specified value.

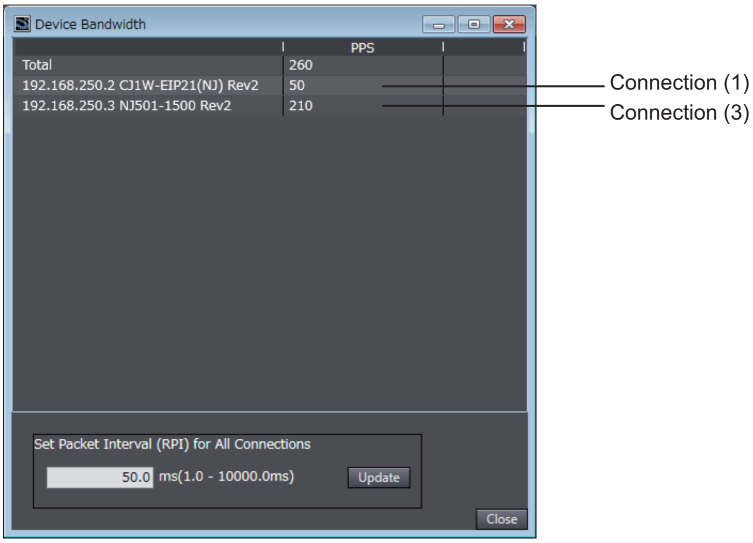
● Calculation Example for Bandwidth Used (PPS) for Each Device by the EtherNet/IP Connections

This section describes the case where the following three EtherNet/IP connections are established between NJ-series Controller 1 to 3, as an example of calculating the bandwidth used for each device by the EtherNet/IP connections.

Connection type	Relevant devices in the EtherNet/IP connections	Device bandwidth usage (PPS)
Connection (1)	NJ-series Controller 2 (target device) to NJ-series Controller 1 (originator device)	50 pps
Connection (2)	NJ-series Controller 1 (target device) to NJ-series Controller 2 (originator device)	10 pps
Connection (3)	NJ-series Controller 3 (target device) to NJ-series Controller 1 (originator device)	210 pps



Bandwidth used (PPS) for each EtherNet/IP device is as given below.

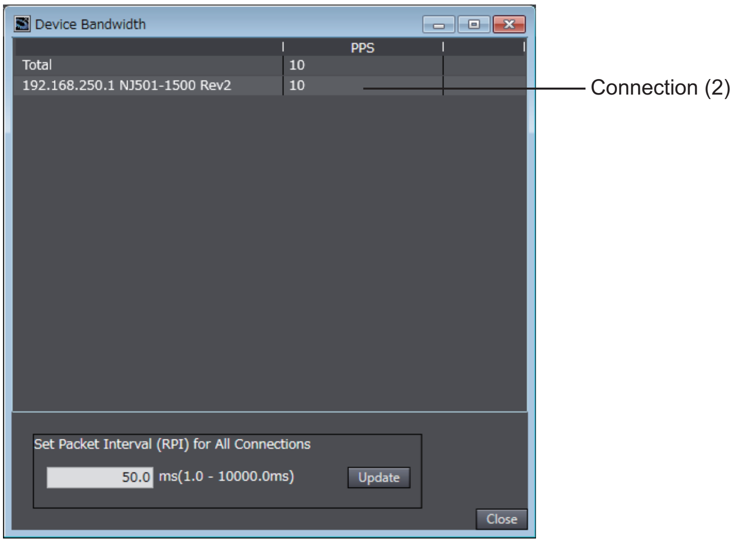


	PPS
Total	260
192.168.250.2 CJ1W-EIP21(NJ) Rev2	50
192.168.250.3 NJ501-1500 Rev2	210

Set Packet Interval (RPI) for All Connections

50.0 ms(1.0 - 10000.0ms)

EtherNet/IP connection settings for Controller 1



	PPS
Total	10
192.168.250.1 NJ501-1500 Rev2	10

Set Packet Interval (RPI) for All Connections

50.0 ms(1.0 - 10000.0ms)

EtherNet/IP connection settings for Controller 2

In this example, the PPS for Connection (1) is 50 pps, the PPS for Connection (2) is 10 pps, and the PPS for Connection (3) is 210 pps. Therefore, bandwidth used (PPS) for each EtherNet/IP device is as given below.
192.168.250.1: 270 pps = 50 pps (for Connection (1)) + 10 pps (for Connection (2)) + 210 pps (for Connection (3))
192.168.250.2: 60 pps = 50 pps (for Connection (1)) + 10 pps (for Connection (2))
192.168.250.3: 210 pps = 210 pps (for Connection (3))

● Adjusting Method

If the calculation result value exceeds the values in the specifications of the devices used in the EtherNet/IP connections, re-evaluate the overall network configuration and correct it by taking steps such as selecting a different Ethernet switch or splitting the network.
If the RPI is made longer, the PPS for the EtherNet/IP connections will decrease.
You can change the RPI values in the connection settings for all the target devices by specifying a value in **Set Packet Interval (RPI) for All Connections** in this dialog box.
Refer to *12-2-2 Tag Data Link Bandwidth Usage and RPI* on page 12-9 for the relationship between the PPS for the device and the RPI.

Transferring the Connection Settings Data

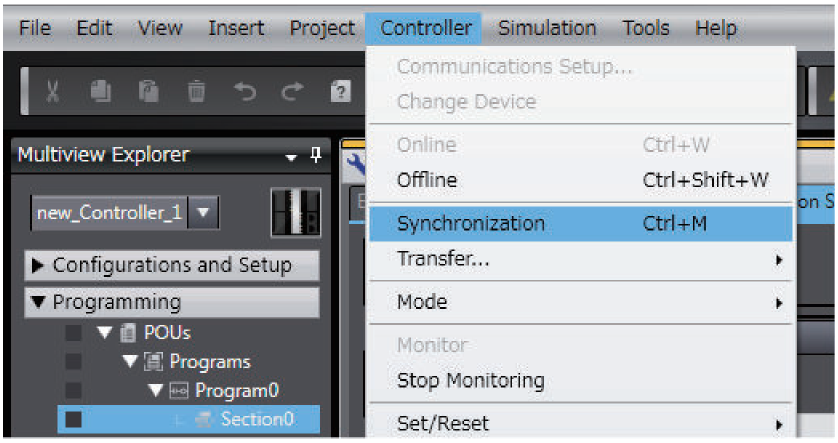
You can synchronize and transfer EtherNet/IP connection settings along with the program data. You can also transfer all the EtherNet/IP connection settings along with the program data.

Precautions for Correct Use

- If the node addresses (IP addresses) are not set correctly, you may connect to the wrong Controller and set incorrect device parameters. Download data only after you confirm that you are connected to the correct Controller.
- If incorrect connection settings are set, it may cause equipment to operate unpredictably. Even when the correct connection settings are set, make sure that there will be no effect on equipment before you transfer the data.
- A connection error will result if the network variables that are used in the tag settings are not set in the Controller. Before downloading the connection settings, check to confirm that the network variables used in the tag settings are set in the Controller.
- If a communications error occurs, the output status depends on the specifications of the device being used. When a communications error occurs for a device that is used along with output devices, check the operating specifications and implement safety countermeasures.
- The EtherNet/IP port and the port on the EtherNet/IP Unit are automatically restarted after the parameters are downloaded. This restart is required to enable the tag set and connection information. Before you download the parameters, check to confirm that problems will not occur with the equipment when the port is restarted.
- Do not disconnect the Ethernet cable or reset or turn OFF the power to the EtherNet/IP Unit during the parameter download.
- The EtherNet/IP connections between relevant nodes is stopped during a download. Before you download data in RUN mode, make sure that it will not affect the controlled system. Also implement interlocks on data processing in ladder programming that uses EtherNet/IP connections when the connections are stopped or a connection error occurs.
- In the EtherNet/IP network, if the device bandwidth usage (PPS) exceeds the unit's allowable bandwidth (PPS), the EtherNet/IP connection operations may not agree with the settings. If you increase the RPI value in such a case, there are cases when the problem can be resolved (i.e., the operations agree the settings).

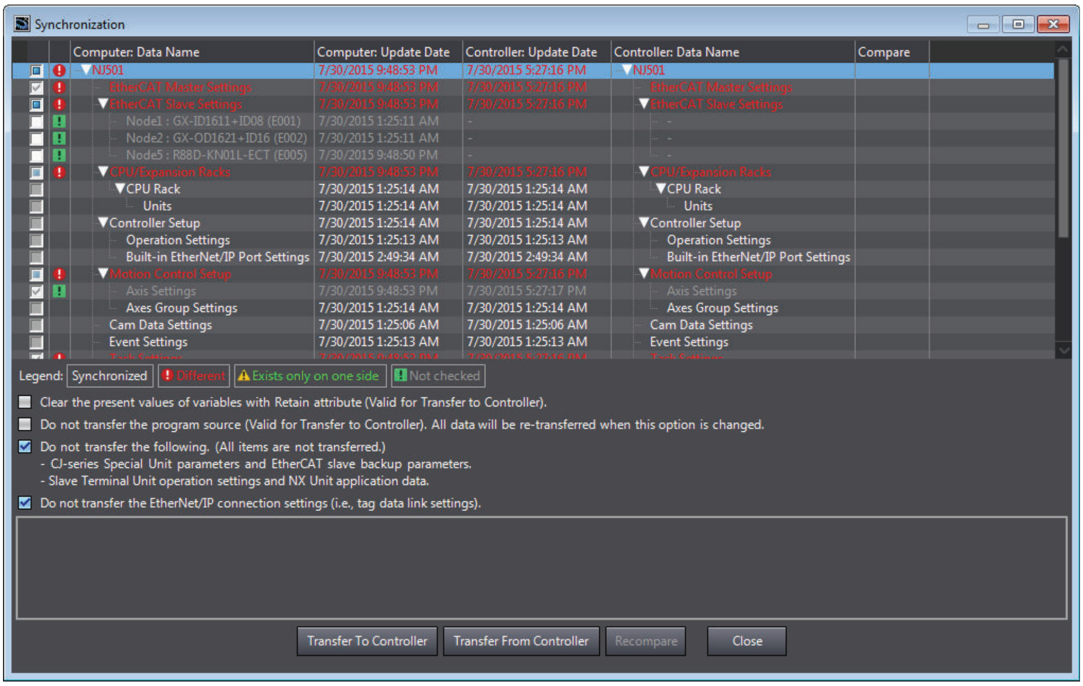
● Synchronizing/Transferring a Whole Project

1 Establish an online connection between the computer and the Controller, and then select **Synchronization** from the **Controller** Menu. (Or, click the Button on the Toolbar.)



The Synchronization Window is displayed, and comparison of the user program and parameter settings between the Sysmac Studio and the Controller is started.

2 The following Uploading and Downloading Data Window is displayed after the automatic comparison.



		Computer: Data Name	Computer: Update Date	Controller: Update Date	Controller: Data Name	Compare
▣	!	▼NJ501	7/30/2015 9:48:53 PM	7/30/2015 5:27:16 PM	▼NJ501	
☑	!	EtherCAT Master Settings	7/30/2015 9:48:53 PM	7/30/2015 5:27:16 PM	EtherCAT Master Settings	
▣	!	▼EtherCAT Slave Settings	7/30/2015 9:48:53 PM	7/30/2015 5:27:16 PM	▼EtherCAT Slave Settings	
☐	!	Node1 : GX-ID1611+ID08 (E001)	7/30/2015 1:25:11 AM	-	-	
☐	!	Node2 : GX-OD1621+ID16 (E002)	7/30/2015 1:25:11 AM	-	-	
☐	!	Node5 : R88D-KN01L-ECT (E005)	7/30/2015 9:48:50 PM	-	-	
▣	!	▼CPU/Expansion Racks	7/30/2015 9:48:53 PM	7/30/2015 5:27:16 PM	▼CPU/Expansion Racks	
☐		▼CPU Rack	7/30/2015 1:25:14 AM	7/30/2015 1:25:14 AM	▼CPU Rack	
☐		Units	7/30/2015 1:25:14 AM	7/30/2015 1:25:14 AM	Units	
☐		▼Controller Setup	7/30/2015 1:25:14 AM	7/30/2015 1:25:14 AM	▼Controller Setup	
☐		Operation Settings	7/30/2015 1:25:13 AM	7/30/2015 1:25:13 AM	Operation Settings	
☐		Built-in EtherNet/IP Port Settings	7/30/2015 2:49:34 AM	7/30/2015 2:49:34 AM	Built-in EtherNet/IP Port Settings	
▣	!	▼Motion Control Setup	7/30/2015 9:48:53 PM	7/30/2015 5:27:16 PM	▼Motion Control Setup	
☑	!	Axis Settings	7/30/2015 9:48:53 PM	7/30/2015 5:27:17 PM	Axis Settings	
☐		Axes Group Settings	7/30/2015 1:25:14 AM	7/30/2015 1:25:14 AM	Axes Group Settings	
☐		Cam Data Settings	7/30/2015 1:25:06 AM	7/30/2015 1:25:06 AM	Cam Data Settings	
☐		Event Settings	7/30/2015 1:25:13 AM	7/30/2015 1:25:13 AM	Event Settings	

Legend: Synchronized | ! Different | ⚠ Exists only on one side | ! Not checked

☐ Clear the present values of variables with Retain attribute (Valid for Transfer to Controller).

☐ Do not transfer the program source (Valid for Transfer to Controller). All data will be re-transferred when this option is changed.

☑ Do not transfer the following. (All items are not transferred.)
- CJ-series Special Unit parameters and EtherCAT slave backup parameters.
- Slave Terminal Unit operation settings and NX Unit application data.

☑ Do not transfer the EtherNet/IP connection settings (i.e., tag data link settings).

3 Clear the **Do not transfer the EtherNet/IP connection settings (i.e., tag data link settings)** Check Box and then click the **Transfer To Controller** Button.
Then the EtherNet/IP connection settings are transferred along with the not-synchronized data.
If no EtherNet/IP connection settings are set in the Sysmac Studio, no data will be sent.

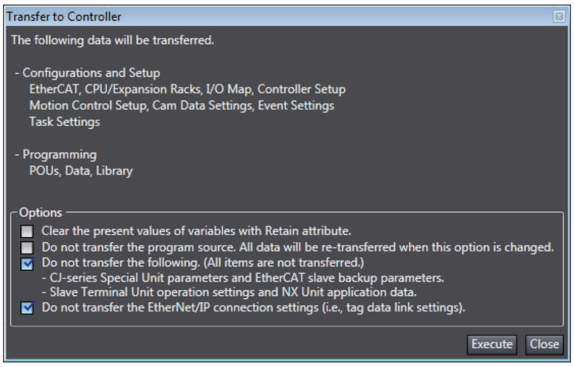
● Transferring all data

1 Establish an online connection between the computer and the Controller and then select **Transfer - To Controller** from the **Controller** Menu. (Or, click the Button on the Toolbar.)

2 The **Transfer to Controller** Dialog Box is displayed.
Clear the selection of the **Do not transfer the EtherNet/IP connection settings (i.e., tag data link settings)** Check Box, and then click the **Execute** Button.

Precautions for Correct Use

To transfer only the connection settings, execute Transfer from the EtherNet/IP Connection Setting Tab Page.
Even if you clear the **Do not transfer the connection setting** Check Box, the connection settings are not transferred from the Synchronization Window, the **Transfer to Controller** Dialog Box, or the **Transfer from Controller** Dialog Box as long as the data in the computer is synchronized with the data in the Controller.



Transfer to Controller

The following data will be transferred.

- Configurations and Setup
  EtherCAT, CPU/Expansion Racks, I/O Map, Controller Setup
  Motion Control Setup, Cam Data Settings, Event Settings
  Task Settings

- Programming
  POUs, Data, Library

Options
☐ Clear the present values of variables with Retain attribute.
☐ Do not transfer the program source. All data will be re-transferred when this option is changed.
☑ Do not transfer the following. (All items are not transferred.)
 - CJ-series Special Unit parameters and EtherCAT slave backup parameters.
 - Slave Terminal Unit operation settings and NX Unit application data.
☑ Do not transfer the EtherNet/IP connection settings (i.e., tag data link settings).

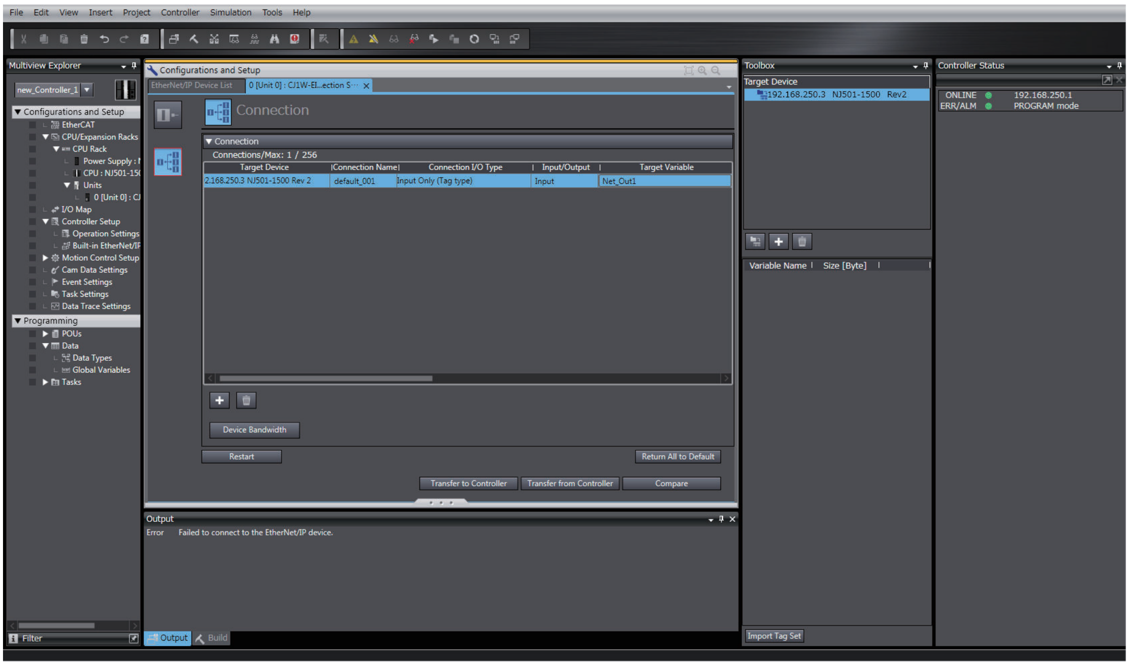
● Transferring Only the EtherNet/IP Connection Settings

You can transfer tag sets and connections to the EtherNet/IP devices.

1 Establish an online connection with the Controller.

2 Click the **Transfer to Controller** or **Transfer from Controller** Button in the EtherNet/IP Connection Setting Tab Page.
The tag settings and connection settings set at that time are transferred to the Controller connected online.

3 If the Controller connected online is in RUN mode, the dialog box to confirm whether to switch to PROGRAM mode before transferring the settings is displayed.



Connections/Max: 1 / 256

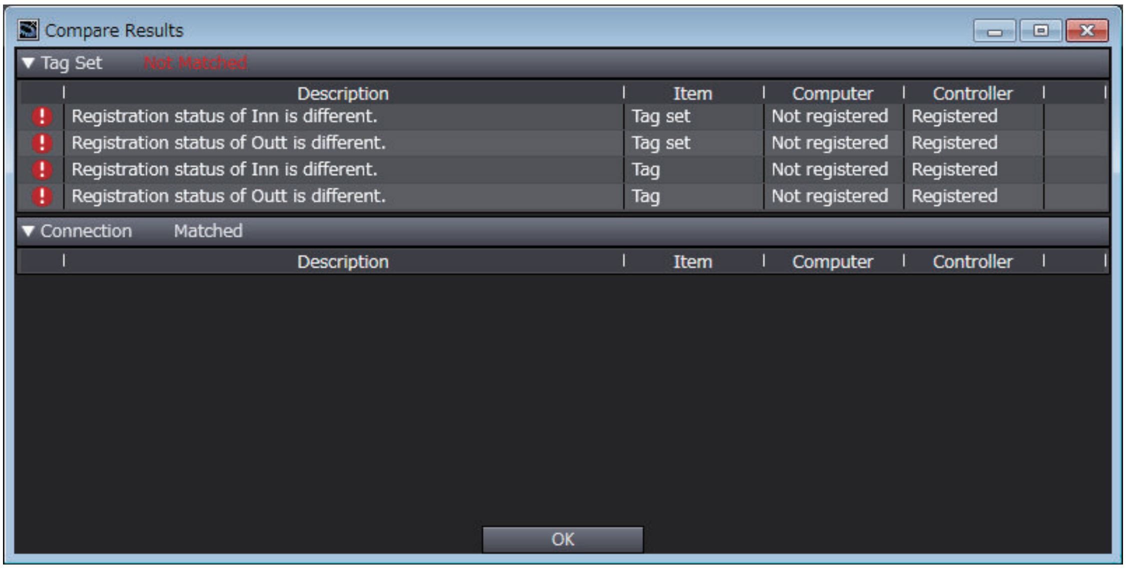
Target Device	Connection Name	Connection I/O Type	Input/Output	Target Variable
2.168.250.3 NJ501-1500 Rev 2	default_001	Input Only (Tag type)	Input	Net_Out1

Error Failed to connect to the EtherNet/IP device.

● Comparison

The differences in the tag set and connection settings between the project and the EtherNet/IP devices can be displayed.

1 Click the **Compare** Button in the EtherNet/IP Connection Setting Tab Page.



Tag Set Not Matched

	Description	Item	Computer	Controller
!	Registration status of Inn is different.	Tag set	Not registered	Registered
!	Registration status of Outt is different.	Tag set	Not registered	Registered
!	Registration status of Inn is different.	Tag	Not registered	Registered
!	Registration status of Outt is different.	Tag	Not registered	Registered

Connection Matched

	Description	Item	Computer	Controller

Starting and Stopping EtherNet/IP Connections

● Automatically Starting EtherNet/IP Connections

The EtherNet/IP device is automatically restarted and EtherNet/IP connections are automatically started immediately after the connection settings are downloaded from the Sysmac Studio.

Precautions for Correct Use

Connections are adversely cut off if any of the following errors occurs in the CPU Unit that is the originator while EtherNet/IP connections are active.

- Major fault level Controller error
- Partial fault level Controller error

● Starting and Stopping the EtherNet/IP Connections for the Entire Network

You can start and stop EtherNet/IP connections from the user program or from the Sysmac Studio.

Precautions for Correct Use

Use the same method (i.e., either the user program or the tool software) to both start and stop EtherNet/IP connections.
For example, if you use the *_EIP_TDLinkStopCmd* (Tag Data Link Communications Stop Switch) system-defined variable to stop EtherNet/IP connections, you cannot start them from the Sysmac Studio and the Network Configurator.

A-3-5 Checking Communications Status with the Sysmac Studio and Troubleshooting

You can monitor the communications status of the EtherNet/IP connections after their settings are set. You can also check errors.

Precautions for Correct Use

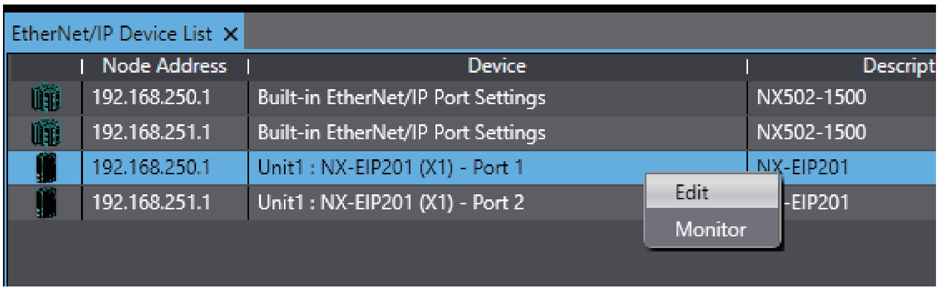
Make sure that the connection settings in both the Sysmac Studio and the Controller are consistent before using the monitor functions. You can use the *Comparison* on page A-31 to see if they are the same.

Checking Communications Status with the Sysmac Studio

You can check the communications status on the EtherNet/IP connections in the EtherNet/IP Connection Monitor Tab Page.

1. Select **EtherNet/IP Connection Settings** from the **Tools** Menu to display the EtherNet/IP Device List Tab Page.

2. Right-click the Controller for which you want to check the communications status, and select **Monitor** from the menu.
   The EtherNet/IP Connection Monitor Tab Page is displayed. In the EtherNet/IP Connection Monitor Tab Page, each communications status is displayed in six tabs.

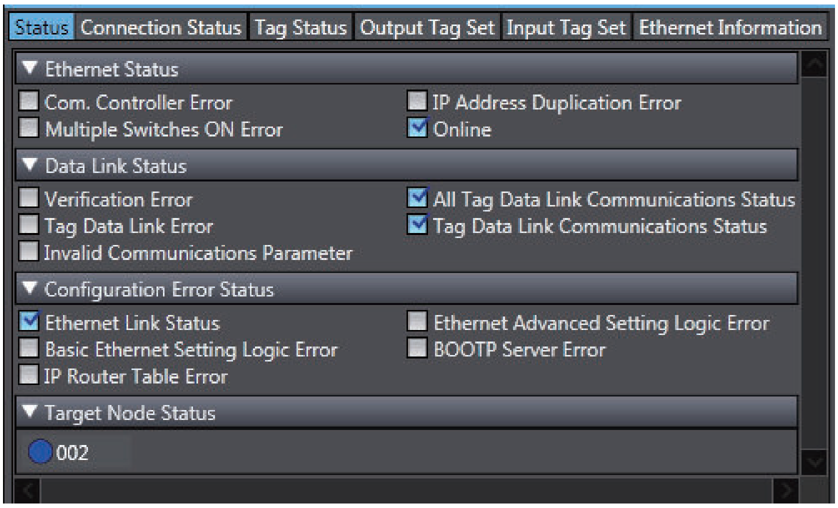


Node Address	Device	Descript
192.168.250.1	Built-in EtherNet/IP Port Settings	NX502-1500
192.168.251.1	Built-in EtherNet/IP Port Settings	NX502-1500
192.168.250.1	Unit1 : NX-EIP201 (X1) - Port 1	NX-EIP201
192.168.251.1	Unit1 : NX-EIP201 (X1) - Port 2	-EIP201

3. Select one of the six tabs for which you want to confirm the communications status.

- **Status** Tab Page
  This tab page gives the TRUE/FALSE status of the system-defined variables that monitors the tag data link status and communication status for errors. If any of the variables is TRUE, its checkbox is marked with ☑.

  Refer to *14-6-1 The Network Configurator's Device Monitor Function* on page 14-47 for details on each status item.



▼ Ethernet Status

☐ Com. Controller Error
☐ Multiple Switches ON Error
☐ IP Address Duplication Error
☑ Online

▼ Data Link Status

☐ Verification Error
☐ Tag Data Link Error
☐ Invalid Communications Parameter
☑ All Tag Data Link Communications Status
☑ Tag Data Link Communications Status

▼ Configuration Error Status

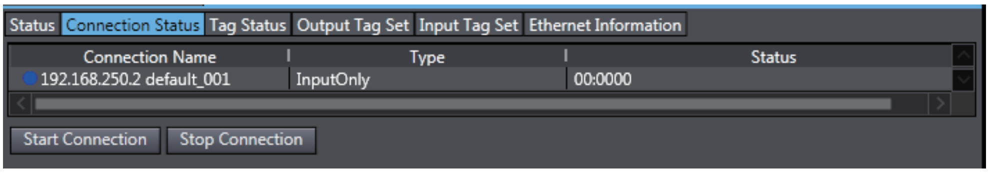
☑ Ethernet Link Status
☐ Basic Ethernet Setting Logic Error
☐ IP Router Table Error
☐ Ethernet Advanced Setting Logic Error
☐ BOOTP Server Error

▼ Target Node Status

● 002

- **Connection Status** Tab Page

Current status of each connection is given.

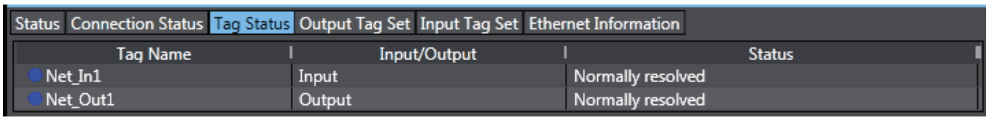


Connection Name	Type	Status
● 192.168.250.2 default_001	InputOnly	00:0000

Name	Description
Connection Name	Gives the current status of each connection with the following text colors. Blue: Normal Red: There is at least one connection that has not been established. Gray: There are no connections or the connection operation is stopped.
Type	Gives the connection type.
Status	Gives the current status on each connection with codes. • Normal operation: 00:0000 • Abnormal operation: Gives an error code. This information can be used to identify the cause of EtherNet/IP connection errors. Refer to *14-6-2 Connection Status Codes and Troubleshooting* on page 14-55 for details on the connection status.

- **Tag Status** Tab Page

This tab page gives if the tag settings for each tag for EtherNet/IP connections are set so that data can be exchanged with target devices.



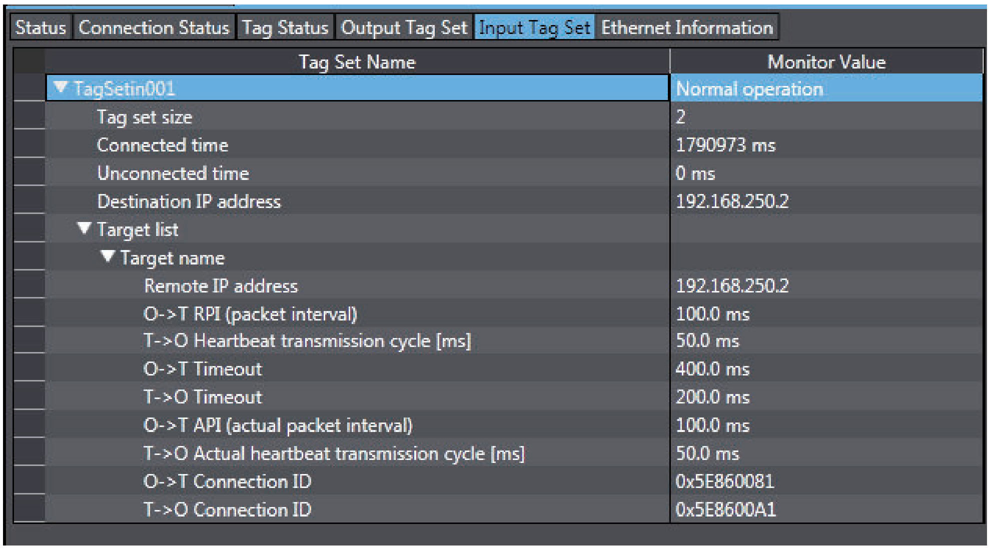
Tag Name	Input/Output	Status
● Net_In1	Input	Normally resolved
● Net_Out1	Output	Normally resolved

Name	Description
Tag Name	The current status of each tag is indicated by its color. Red: Tag name resolution error Blue: Tag name resolution normal Gray: Not yet transferred (no information in device).

Name	Description
Input/Output	Gives the type of the tag.
Status	The following status is displayed depending on the status that is set. • Normally resolved: Normal data exchange is possible. • Different sizes: Different sizes are set for the network variables and the tag settings. A connection will not be established for a tag for which this error occurs. • No tag: A network variable is not set in the variable table in the CPU Unit for the specified tag setting. Or, instead of a member of union variable, unions are specified. A connection will not be established for a tag for which this error occurs. • Attribute error: The following two factors cause this error. 1. Writing is not possible for constant attributes. 2. The I/O direction that is set in the tag data link settings does not agree with the I/O direction of the variable in the CPU Unit. There is an error in the setting of a Network Publish attribute for a CPU Unit variable. A connection will not be established for a tag for which this error occurs.

- **Output Tag Set** and **Input Tag Set** Tab Pages

  You can monitor the status of each input/output tag set that is used for the EtherNet/IP connections. Click ▼ of each tag to display its detailed information.

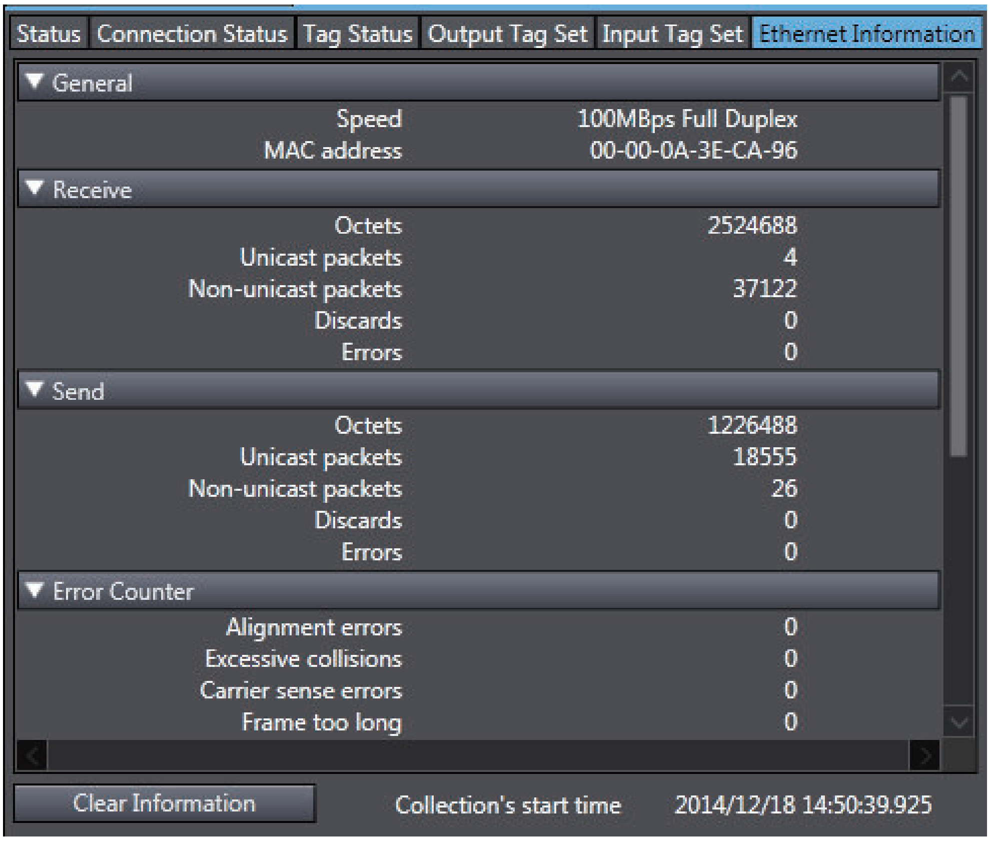


Tag Set Name	Monitor Value
▼ TagSetin001	Normal operation
Tag set size	2
Connected time	1790973 ms
Unconnected time	0 ms
Destination IP address	192.168.250.2
▼ Target list	
▼ Target name	
Remote IP address	192.168.250.2
O->T RPI (packet interval)	100.0 ms
T->O Heartbeat transmission cycle [ms]	50.0 ms
O->T Timeout	400.0 ms
T->O Timeout	200.0 ms
O->T API (actual packet interval)	100.0 ms
T->O Actual heartbeat transmission cycle [ms]	50.0 ms
O->T Connection ID	0x5E860081
T->O Connection ID	0x5E8600A1

Name	Description
Tag Set Name	Gives the connection status. If there is a connection error, "Not connected or error" is given.
Tag set size	Gives the size of the tag set in bytes.
Connected time	Gives the total connection duration in milliseconds.
Unconnected time	Gives the total disconnection duration in milliseconds.
Number of connections (in the **Output Tag Set** Tab Page)	Gives the number of connections.
Number of connected originators (in the **Output Tag Set** Tab Page)	Gives the number of the connected originator devices.

Name	Description
Originator list (in the **Output Tag Set** Tab Page), Target list (in the **Input Tag Set** Tab Page)	Gives the detailed information of the connected originators.
Originator name (in the **Output Tag Set** Tab Page), or Target name (in the **Input Tag Set** Tab Page)	Gives no information.
IP address (in the **Output Tag Set** Tab Page), or Remote IP address (in the **Input Tag Set** Tab Page)	Gives the IP addresses allocated for the originators.
Connected time (in the **Output Tag Set** Tab Page)	Gives the total duration of connection with the originator in milliseconds.
Unconnected time (in the **Output Tag Set** Tab Page)	Gives the total duration of disconnection with the originator in milliseconds.
Destination IP address (in the **Output Tag Set** Tab Page)	Gives the destination IP addresses. If the multi-cast connections are used, its own multi-cast address is displayed.
O->T RPI (packet interval)	Gives the RPI of connection from the originator to the target in milliseconds.
T->O Heartbeat transmission cycle (ms)	Gives the heartbeat transmission period of the connections from the target to the originator in milliseconds.
O->T Timeout	Gives the timeout time for the connections from the originator to the target in milliseconds.
T->O Timeout	Gives the timeout time for the connections from the target to the originator in milliseconds.
O -> T API (actual packet interval)	Gives the RPI of connection from the originator to the target in milliseconds.
T->O Actual heartbeat transmission cycle (ms)	Gives the actual heartbeat transmission period of the connections from the target to the originator in milliseconds.
O->T Connection ID	Gives the connection identification for the connections from the originator to the target in hexadecimal.
T->O Connection ID	Gives the connection identification for the connections from the target to the originator in hexadecimal.

- **Ethernet Information** Tab Page
  This tab page displays the communications status at the communications driver level of the Ether-net/IP port.
  The error counter information can be used to confirm whether communications problems have occurred.
  Under the Tag Data Link, you can confirm characteristics such as the bandwidth usage (PPS).



General

Speed	100MBps Full Duplex
MAC address	00-00-0A-3E-CA-96

Receive

Octets	2524688
Unicast packets	4
Non-unicast packets	37122
Discards	0
Errors	0

Send

Octets	1226488
Unicast packets	18555
Non-unicast packets	26
Discards	0
Errors	0

Error Counter

Alignment errors	0
Excessive collisions	0
Carrier sense errors	0
Frame too long	0

Collection's start time 2014/12/18 14:50:39.925

Display example for an NJ-series CPU Unit

A-3-6 Troubleshooting

In the case that there is a setting error or a communications error in the EtherNet/IP networks, the Sysmac Studio displays the error in the Troubleshooting Dialog Box.
Refer to the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* for how to identify errors and details on errors.

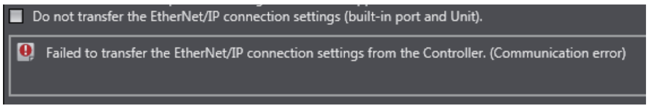
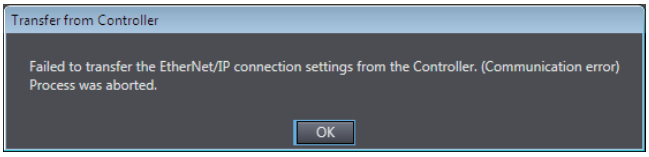
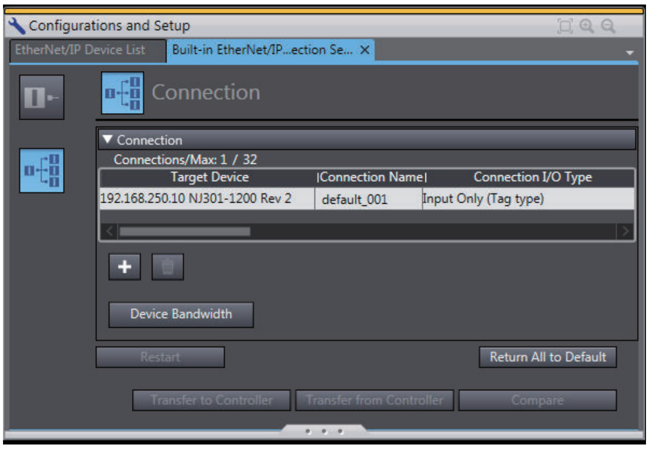
Troubleshooting When Transferring and Monitoring the EtherNet/IP Connection Settings Fail

The first time you establish an online connection between the Controller and the computer that runs the Sysmac Studio with Windows Firewall on the computer enabled, a dialog box may be displayed to confirm the connection. If that occurs, select **Allow access**.

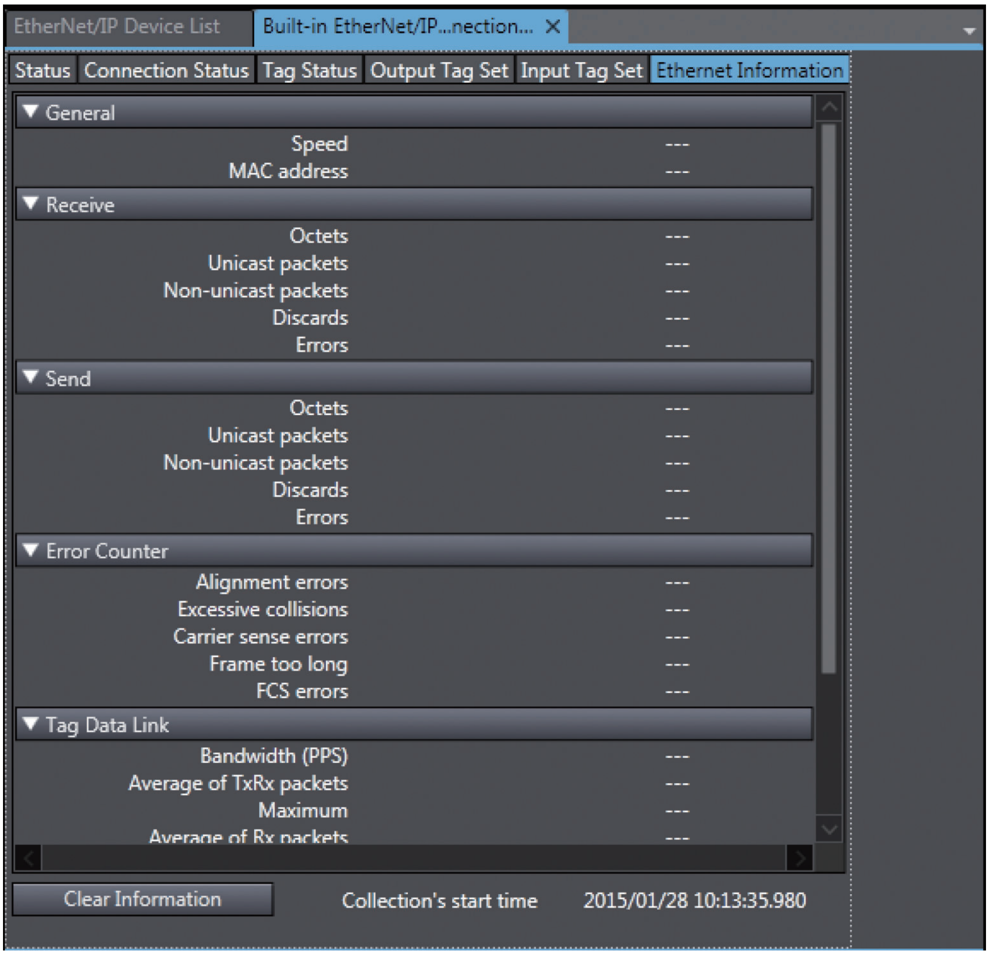
If you select other than **Allow access**, transferring and monitoring the EtherNet/IP connection settings may not be properly performed even if the online connection is successfully established between the Sysmac Studio and the Controller.
If the above problem occurs, take the following corrective method 1 or 2.

● Problems

- The connection setting data cannot be transferred.

Data Transmission Screen	Problem
Synchronization Window	The Sysmac Studio displays the following error message and the data will not be transferred.  ☐ Do not transfer the EtherNet/IP connection settings (built-in port and Unit). Failed to transfer the EtherNet/IP connection settings from the Controller. (Communication error)
Transfer to Controller Dialog Box	The Sysmac Studio displays the following error dialog box and the data will not be transferred.  Transfer from Controller Failed to transfer the EtherNet/IP connection settings from the Controller. (Communication error) Process was aborted.
EtherNet/IP Connection Setting Tab Page	The **Transfer to Controller** and **Transfer from Controller** Buttons are grayed out and the data cannot be transferred/compared.  Configurations and Setup EtherNet/IP Device List Built-in EtherNet/IP...ection Se... Connection Connection Connections/Max: 1 / 32 Target Device: 192.168.250.10 NJ301-1200 Rev 2 Connection Name: default_001 Connection I/O Type: Input Only (Tag type) Device Bandwidth Restart Return All to Default Transfer to Controller Transfer from Controller Compare

- Monitoring cannot be performed
  Monitor results in the EtherNet/IP Connection Monitor Tab Page remain as "---".



General
Speed ---
MAC address ---

Receive
Octets ---
Unicast packets ---
Non-unicast packets ---
Discards ---
Errors ---

Send
Octets ---
Unicast packets ---
Non-unicast packets ---
Discards ---
Errors ---

Error Counter
Alignment errors ---
Excessive collisions ---
Carrier sense errors ---
Frame too long ---
FCS errors ---

Tag Data Link
Bandwidth (PPS) ---
Average of TxRx packets ---
Maximum ---
Average of Rx packets ---

Collection's start time 2015/01/28 10:13:35.980

Method 1: Disabling Windows Firewall Settings

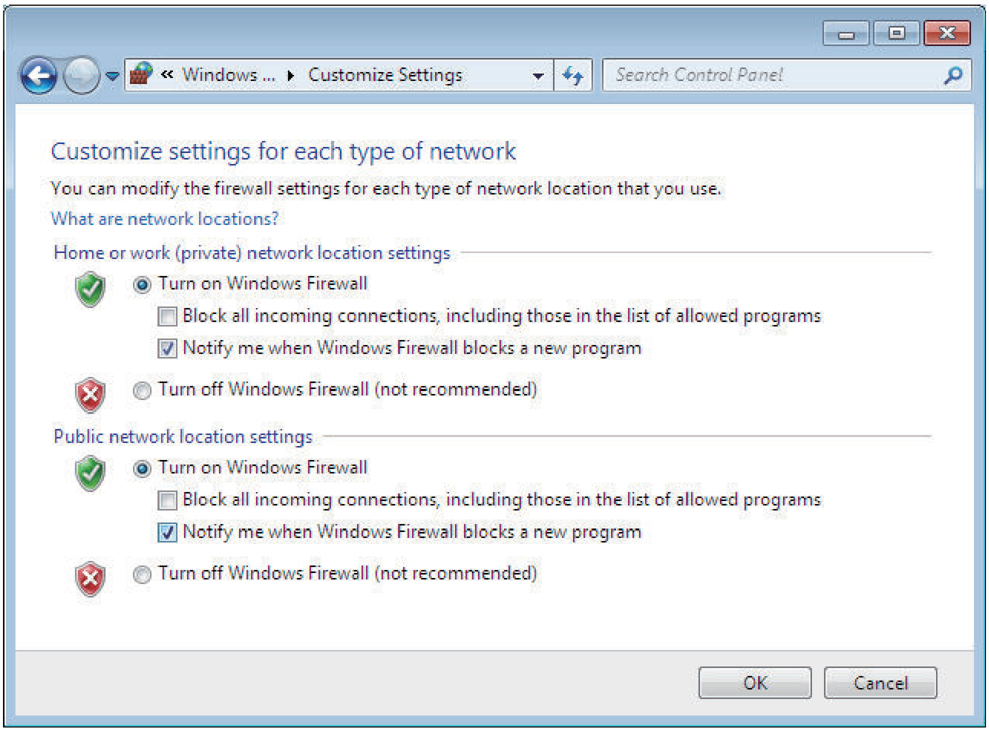
1. Open the **Control Panel** from the **Windows Start Menu** and then select **Windows Firewall** icon.

   The **Windows Firewall** Dialog Box is displayed.

2. Select **Turn Windows Firewall On or Off**.

   The **Customize Settings** Dialog box is displayed.

3. Clear the **Block all incoming connections, including those in the list of allowed programs** Check Box and click the **OK** Button.



Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

● Turn on Windows Firewall

☐ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Public network location settings

● Turn on Windows Firewall

☐ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

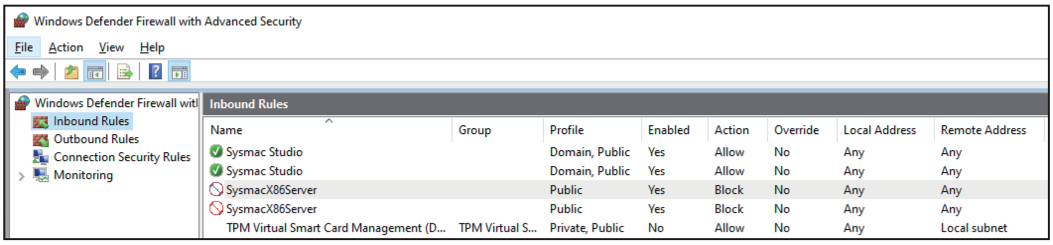
○ Turn off Windows Firewall (not recommended)

4 Select the **Advanced** Tab in the Windows Firewall Dialog Box.

The **Windows Firewall with Advanced Security** Dialog Box is displayed.

5 Click **Inbound Rules** in the left pane and then double-click **SysmacX86Server** in the **Inbound Rules** list for Sysmac Studio version 1.31 or higher. For Sysmac Studio lower than version 1.31, double-click **Sysmac Studio**.

If you double-click **SysmacX86Server**, the **SysmacX86Server Properties** Dialog Box appears. If you double-click **Sysmac Studio**, the **Sysmac Studio Properties** Dialog Box is displayed.


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Local Address	Remote Address
Sysmac Studio		Domain, Public	Yes	Allow	No	Any	Any
Sysmac Studio		Domain, Public	Yes	Allow	No	Any	Any
SysmacX86Server		Public	Yes	Block	No	Any	Any
SysmacX86Server		Public	Yes	Block	No	Any	Any
TPM Virtual Smart Card Management (D...	TPM Virtual S...	Private, Public	No	Allow	No	Any	Local subnet

6 For Sysmac Studio version 1.31 or higher, make the following settings in the **SyamacX86Server Properties** Dialog Box. If Sysmac Studio version is lower than 1.31, make the following settings in the **Syamac Studio Properties** Dialog Box.

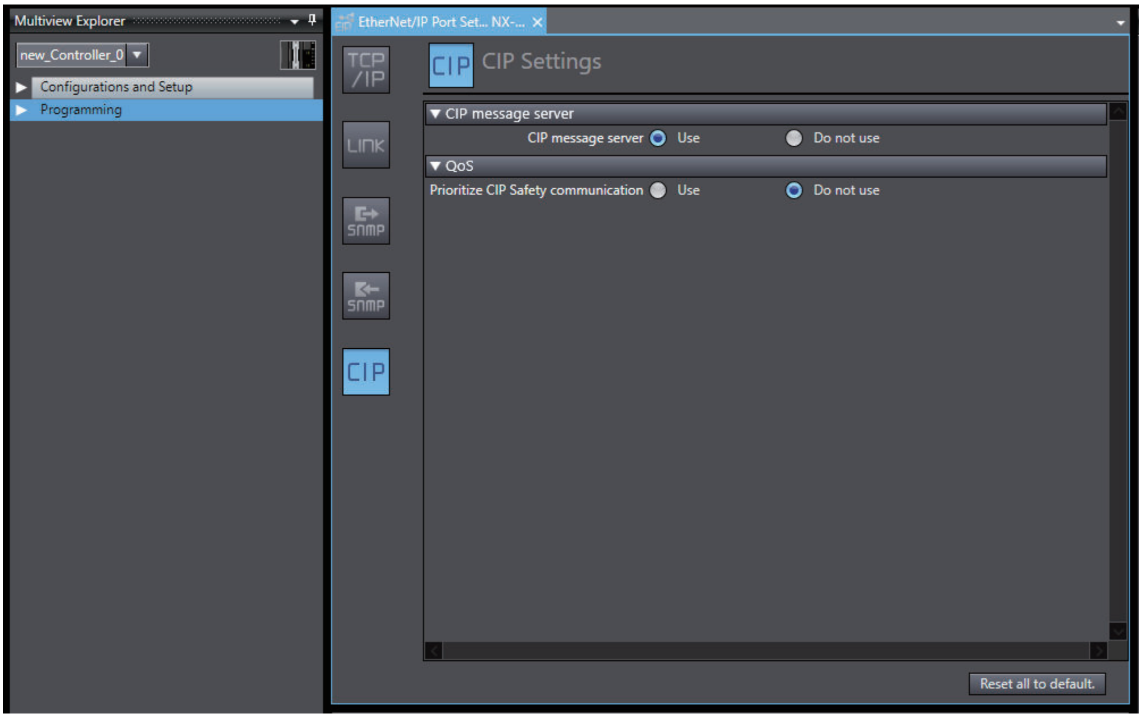
- If the **Public** Check Box under **Profiles** is not selected in the **Advanced** Tab Page, select it.
- If the **Enabled** Check Box under **General** is not selected in the **General** Tab Page, select it.
- Select **Allow the connection** under **Action** in the **General** Tab Page.

Precautions for Correct Use

The main function of the firewall is to prevent illegal access from external sources (e.g., the Internet).
The purpose of changing the firewall settings through this procedure is to connect the Sysmac Studio to an NJ/NX-series Controller. If your computer is connected to an in-house network, make such changes only after confirming that they have no security impact on the network.

Method 2: Selecting the Use Option for the CIP Message Server

1. Connect the Sysmac Studio to the Controller.
2. Select **Configurations and Setup - CPU/Expansion Racks - CPU Rack: X Bus - Unit No.: NX-EIP201 () - EtherNet/IP Port Settings - CIP Settings**.
3. Change the setting to select the **Use** Option for **CIP Message Server**.



▼ CIP message server

CIP message server ● Use ○ Do not use

▼ QoS

Prioritize CIP Safety communication ○ Use ● Do not use

Method 3: Configuring Packet Filter Settings to Allow Packets Used by Sysmac Studio's EtherNet/IP Connection Settings

1. Connect the Sysmac Studio to the Controllers.
2. Select **Configurations and Setup – CPU/Expansion Racks – CPU Rack: X Bus – Unit No.: NX-EIP201 () – EtherNet/IP Port Settings – TCP/IP Settings**.
3. Enter the settings for **Packet Filter** to allow packets used by Sysmac Studio's EtherNet/IP connection settings. Refer to *Packet Filter* on page 7-7 for detailed settings.

Method 4: Cycling the Power Supply to the Controller

Cycle the power supply to the NJ/NX-series Controller and transfer/monitor the EtherNet/IP connections settings again.

Note You may need to cycle the power supply when reflecting the changes in the IP address of the EtherNet/IP port or executing Transfer to the Controller.

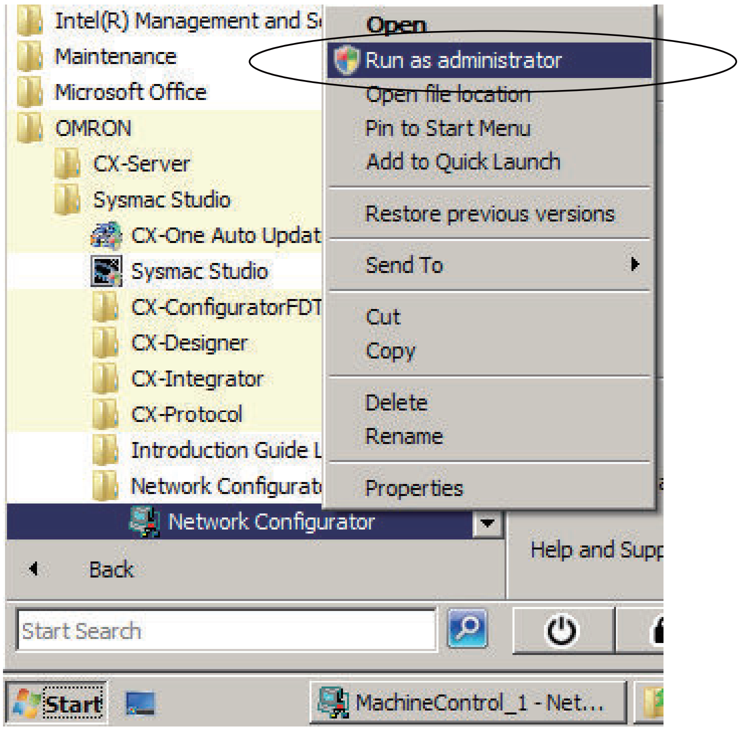
A-4 EDS File Management

This section describes the EDS file management on the Network Configurator.

Precautions for Correct Use

We recommend that you select **Run as administrator** to start the Network Configurator for operations with EDS files.
If you do not select **Run as administrator**, the following condition will result according to Windows user management for security purposes.
The following operations are not valid if you log in with another user account, and you need to restart the Network Configurator again: **Install**, **Create**, **Delete**, and **Create EDS Index File** under **EDS File**.
When you start the Network Configrator, select **Run as administrator** as below.

1. Select the Network Configurator from the Start Menu, and then right-click.
2. Select **Run as administrator** from the displayed pop-up menu.



A-4-1 Installing EDS Files

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 - Install**.
The Install EDS File Dialog Box is displayed.

2 Select the EDS file to install, and click the **Open** Button.

Next, select the icon file (*.ico). The EDS file is added to the Hardware List as a new device.
If the hardware already exists, the new Hardware List will overwrite the previous one.
If the hardware has different versions, each hardware version is added to the Hardware List.

A-4-2 Creating EDS Files

EDS File - Create

The EDS files are required for the Network Configurator to create a network configuration. To create an EDS file, use the following procedure.

1. Select **EDS File** - **Create**.
2. Set the device information. You can obtain the device information from the device on the network if it is online.
3. The device is added to the Hardware List as a new device, just like when you install an EDS file.

Additional Information

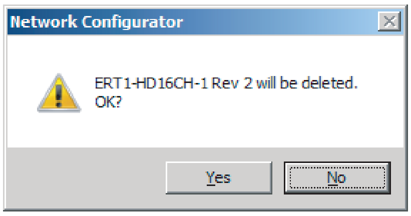
You cannot set device parameters when you create an EDS file with the Network Configurator. Obtain a proper EDS file from the manufacturer of the device to make device parameter settings for the device.

A-4-3 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 dialog box is displayed.



Network Configurator

ERT1-HD16CH-1 Rev 2 will be deleted.
OK?

3. Click the **Yes** Button.
   The selected device is deleted from the Hardware List together with the EDS file.

A-4-4 Saving EDS Files

EDS File - Save

To save the EDS file, use the following procedure.

1 Select the target hardware device in the Hardware List, and then select **EDS File** - **Save**.

2 A Save EDS File Dialog Box is displayed.

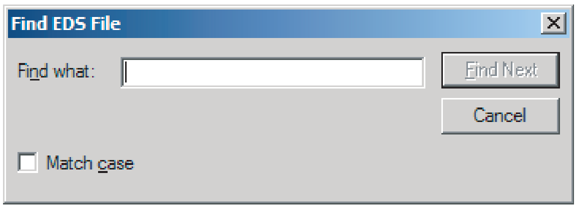
3 Input the folder and file names and click the **Save** Button.
The EDS file is saved.

A-4-5 Searching EDS Files

EDS File - Find

To search the devices in the Hardware List for EDS files, use the following procedure.

1 Select **EDS File** - **Find**.
The following dialog box is displayed.



2 Input the character string to search for, and click the **Find Next** Button.

3 If a matching device is found, the cursor moves to the position of the device.

4 To quit the search operation, click the **Cancel** Button.

Additional Information

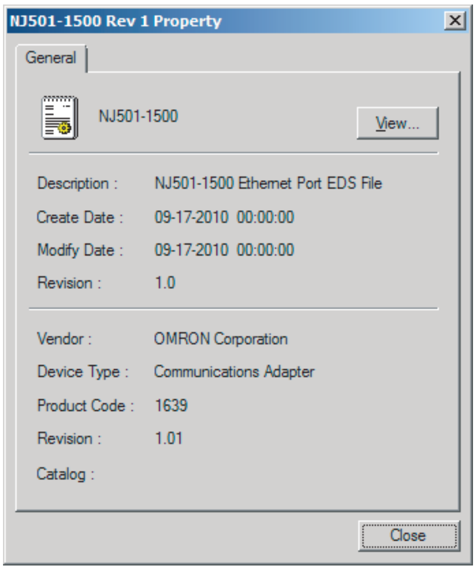
- The search is performed for the device on which the cursor stays and subsequent ones in the Hardware List.
- To search all the devices, select *Hardware* in the Hardware List before you perform the search.

A-4-6 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 dialog box is displayed.



Description : NJ501-1500 Ethernet Port EDS File
Create Date : 09-17-2010 00:00:00
Modify Date : 09-17-2010 00:00:00
Revision : 1.0

Vendor : OMRON Corporation
Device Type : Communications Adapter
Product Code : 1639
Revision : 1.01
Catalog :

The time and date when the EDS file was created is displayed, along with the device information.

A-4-7 Creating EDS Index Files

EDS File - Create EDS Index File

When an EDS file is manually added or when a device is not correctly indicated 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.

A-5 Precautions for Using the Network Configurator on Windows XP, Windows Vista, or Windows 7 or Higher

Better firewall security for Windows XP (SP2 or higher), Windows Vista, and Windows 7 or higher has increased the restrictions for data communications. Before connecting the Network Configurator and an NJ/NX-series CPU Unit and starting communications through the following procedures, you may need to change the settings of the Windows firewall as described in this section.

- If you select **Option** - **Select Interface** - **Ethernet I/F**.
- If you select **Option** - **Select Interface** - **NJ/NX Series Ethernet Direct I/F**.
- If you select **Option** - **Select Interface** - **NJ/NX Series USB Port**.

Precautions for Correct Use

The main function of the firewall is to prevent illegal access from external sources (e.g., the Internet). The purpose of changing the firewall settings through this procedure is to connect the Network Configurator to an NJ/NX-series CPU Unit. If your computer is connected to an in-house network, make such changes only after confirming that they have no security impact on the network.

A-5-1 Changing Windows Firewall Settings

Windows XP

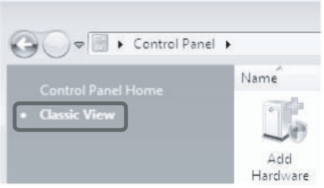
1 When you attempt to connect to the NJ/NX-series CPU Unit from the Network Configurator, the **Windows Security Alert** Dialog Box is displayed.

2 Click the **Unblock** Button.
This allows USB connection and EtherNet/IP connection to the Network Configurator, and you will be able to connect to the NJ/NX-series CPU Unit via the Network Configurator.

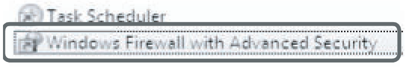
Windows Vista or Windows 7 or Higher

Use the following procedure to change the settings.
Always perform steps 1 to 6 if you cannot go online. The **User Account Control** Dialog Box may be displayed during this procedure. If it appears, click the **Continue** Button and continue with the procedure.

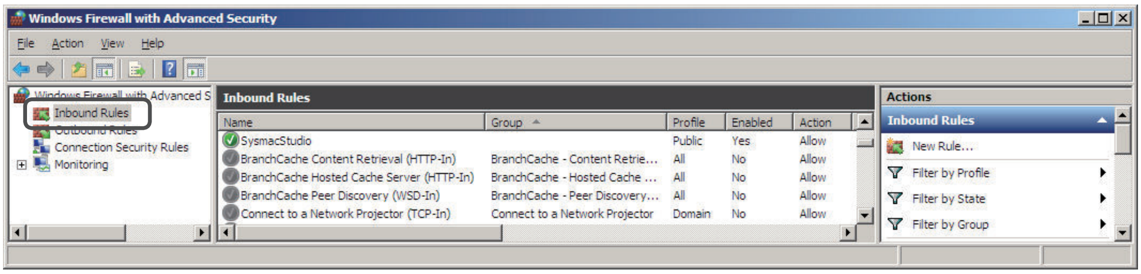
1 Select **Control Panel** from the Windows Start Menu, and select **Classic View** to change the view.



2 Open **Administrative Tools**, and select **Windows Firewall with Advanced Security** in the displayed dialog box.

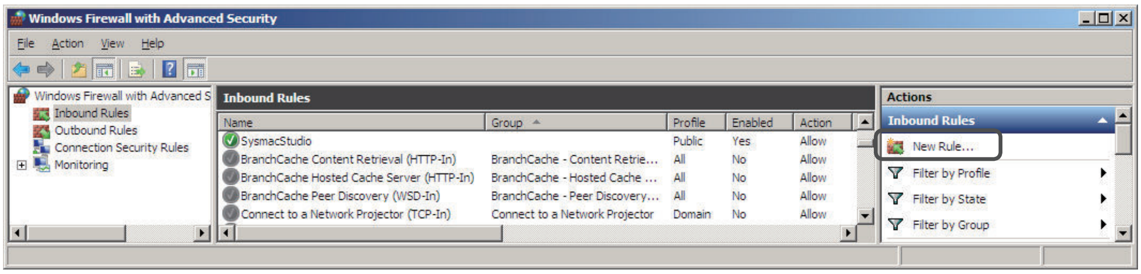


3 Select **Inbound Rules** under **Windows Firewall with Advanced Security on Local Computer** on the left side of the **Windows Firewall with Advanced Security** Dialog Box.



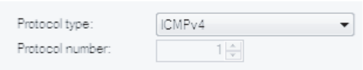
Name	Group	Profile	Enabled	Action
SysmacStudio		Public	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retrie...	All	No	Allow
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Cache ...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discovery...	All	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Projector	Domain	No	Allow

4 Select **New Rule** under **Inbound Rules** in the **Actions** Area on the right side of the dialog box.



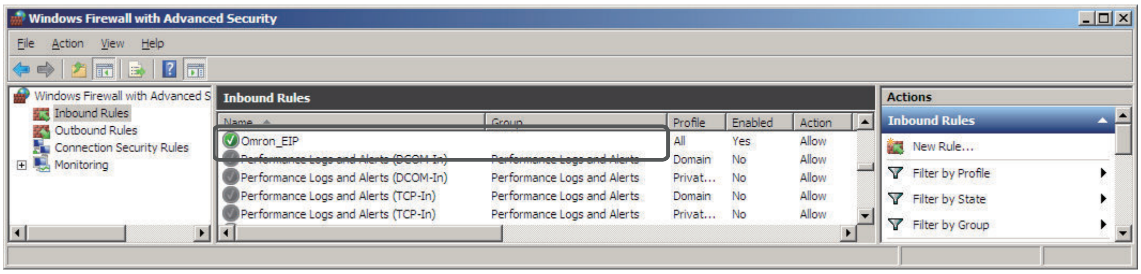
Name	Group	Profile	Enabled	Action
SysmacStudio		Public	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retrie...	All	No	Allow
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Cache ...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discovery...	All	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Projector	Domain	No	Allow

5 Follow the steps below to make the settings in the **New Inbound Rule Wizard** Dialog Box. Select the specified option at each step, and click the **Next** Button to move to the next step.

Rule Type	Select **Custom**.
Program	Select **All Programs**.
Protocol and support	Select **ICMPv4** as the protocol type.  Protocol type: ICMPv4 Protocol number: 1
Scope	Select **Any IP address** for all.
Action	Select **Allow the connection**.
Profile	Select **Domain**, **Private**, and **Public**.
Name	Enter an arbitrary name (e.g., Omron_EIP).

6 Click the **Finish** Button. The rule that you defined (i.e., Omron_EIP) is registered in the list of **Inbound Rules**.

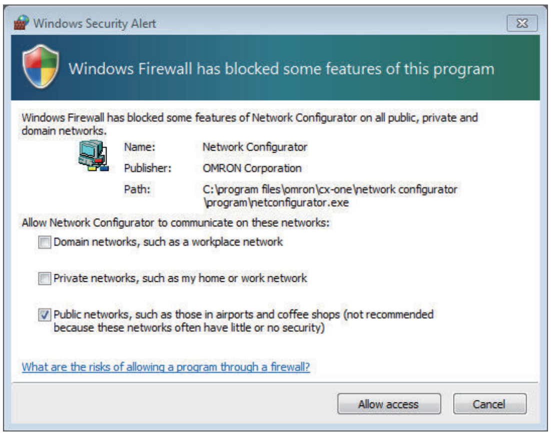
Close the **Windows Firewall with Advanced Security** Dialog Box.



Name	Group	Profile	Enabled	Action
Omron_EIP		All	Yes	Allow
Performance Logs and Alerts (DCOM-In)	Performance Logs and Alerts	Domain	No	Allow
Performance Logs and Alerts (DCOM-In)	Performance Logs and Alerts	Privat...	No	Allow
Performance Logs and Alerts (TCP-In)	Performance Logs and Alerts	Domain	No	Allow
Performance Logs and Alerts (TCP-In)	Performance Logs and Alerts	Privat...	No	Allow

7 When you attempt to connect to the NJ/NX-series CPU Unit from the Network Configurator, the **Windows Security Alert** Dialog Box is displayed.

8 Click the **Allow access** Button.


Windows Security Alert
Windows Firewall has blocked some features of this program
What are the risks of allowing a program through a firewall?
Allow access
Cancel

Windows Firewall has blocked some features of Network Configurator on all public, private and domain networks.

Name: Network Configurator
Publisher: OMRON Corporation
Path: C:\program files\omron\cx-one\network configurator \program\netconfigurator.exe

Allow Network Configurator to communicate on these networks:

☐ Domain networks, such as a workplace network

☐ Private networks, such as my home or work network

☑ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

(On Windows 7) This allows USB connection and EtherNet/IP connection to the Network Configurator, and you will be able to connect to the NJ/NX-series CPU Unit via the Network Configurator.

A-6 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.

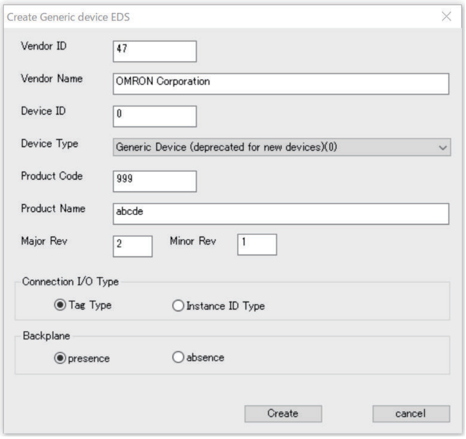
The procedures to create a Generic Device and the procedures to create a tag or tag set are shown below.

Additional Information

The procedures after creating a tag or tag set are the same as for devices that have EDS files. Refer to *9-2 Setting Tag Data Links* on page 9-15.

A-6-1 Creating Generic Devices

1 Select **Create Generic Device** from the **EDS File** Menu.
The Create Generic device EDS Dialog Box is displayed.



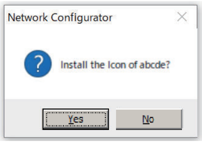
Create Generic device EDS

Vendor ID: 47
Vendor Name: OMRON Corporation
Device ID: 0
Device Type: Generic Device (deprecated for new devices)(0)
Product Code: 999
Product Name: abcde
Major Rev: 2
Minor Rev: 1

Connection I/O Type
● Tag Type ○ Instance ID Type

Backplane
● presence ○ absence

2 Set the information for the device and click the **Create** Button.
A confirmation dialog to install an icon is displayed.

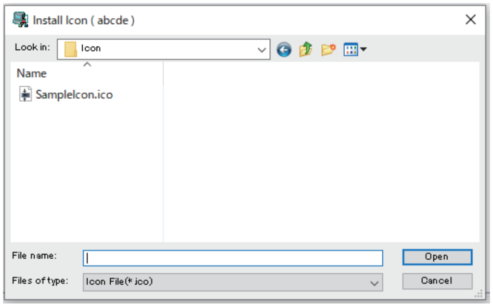


Network Configurator

Install the Icon of abcde?

3 Set a device icon.

- If you click the **Yes** Button:
  The **Install Icon (EDS file name)** Dialog Box is displayed.

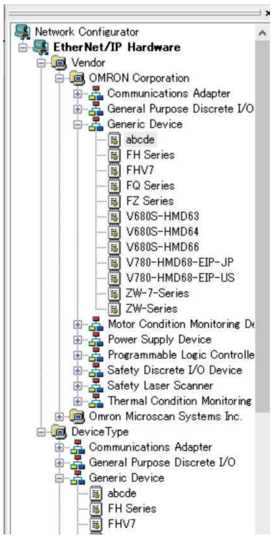


Look in: Icon

Files of type: Icon File(*.ico)

- 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.



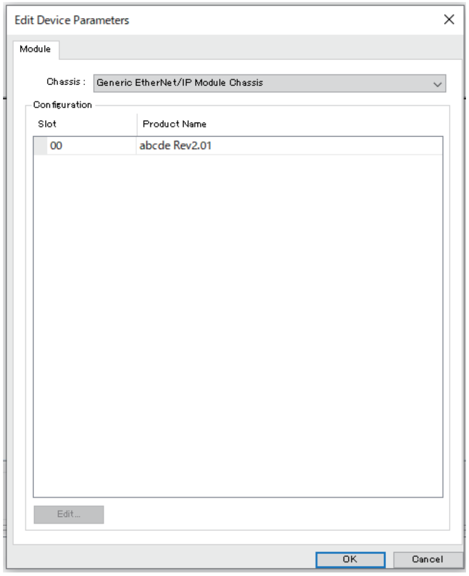
A-6-2 Creating a Tag or Tag Set for Generic Device

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.

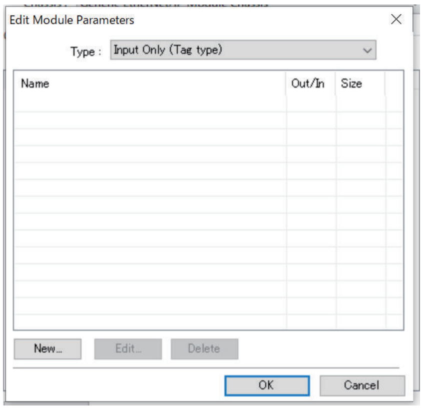
2 Double-click the device icon.
The **Edit Device Parameters** Dialog Box is displayed.



Chassis : Generic EtherNet/IP Module Chassis

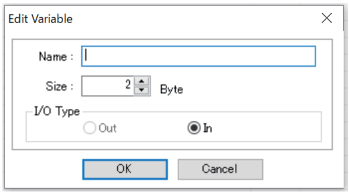
Slot	Product Name
00	abcde Rev2.01

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.



Type : Input Only (Tag type)

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.



Size : 2 Byte
I/O Type ○ Out ● In

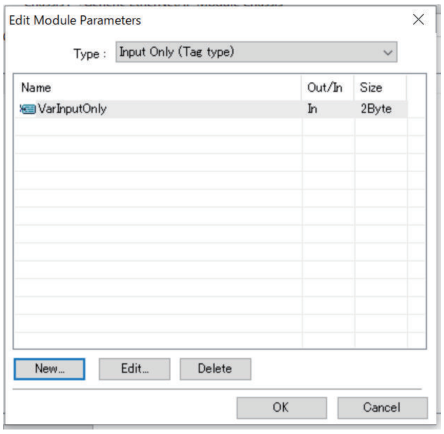
5 Set the following parameters for the variable.

- **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.



Type : Input Only (Tag type)

Name	Out/In	Size
VarInputOnly	In	2Byte

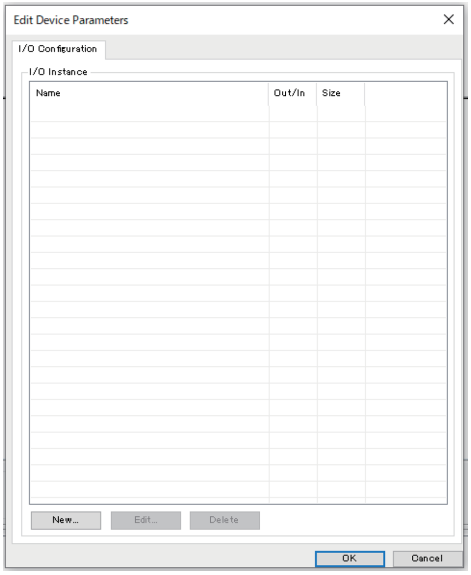
7 Repeat steps 4 through 6 to register the required variables. Click the **OK** Button when the registration is complete.

Creation Procedure for Instance ID Type

1 Add the Generic Device that you created to the network window.

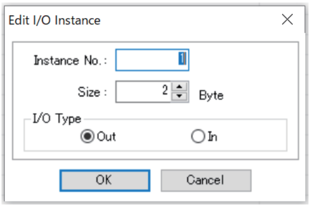
2 Double-click the device icon.

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.



Instance No. : 1

Size : 2 Byte

I/O Type
● Out ○ In

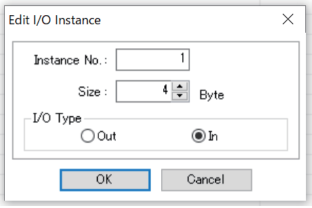
4 Enter the following parameters.

- **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.



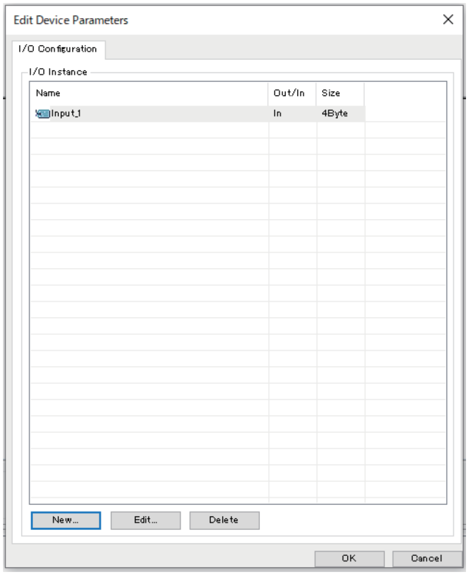
Instance No. : 1

Size : 4 Byte

I/O Type
○ Out ● 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.



Name	Out/In	Size
Input_1	In	4Byte

6 Repeat steps 3 through 5 to register the required I/O instances. Click the **OK** Button when the registration is complete.

A-7 TCP/UDP Port Numbers Used for the NX-series EtherNet/IP Unit

The following table shows the applications that the NX-series EtherNet/IP Unit uses TCP/UDP ports, port numbers, port types, protocols used, default port states, usages, and how to change a port from open to close.

TCP/UDP ports (servers) other than those shown below are not used.

Application	UDP port number	TCP port number	Port type	Protocol used	Default port state	Usage	How to change from open to close
SSH/SFTP	---	22	System port	SSH/SFTP	Close	For maintenance	---
DNS client	53	---	System port	DNS	Close	Used when using the DNS client.	---
X Bus[*1]	67	---	System port	DHCP	Close	Used for communications with the CPU Unit.	---
	520	---	System port	RIP[*2]			
	44819	---	User port	CIP			
	---	9910	User port	TCP (OMRON protocol)			
BOOTP client	68	---	System port	BOOTP	Close	Used when using the BOOTP client.	---
HTTP server	---	80	System port	HTTP	Close	Used for communications with the Sysmac Studio.	---
SNMP	161	---	System port	SNMP (SNMPv1, SNMPv2C)	Close	Used when using the SNMP agent.	---
SNMP trap	162	---	System port		Close	Used when using the SNMP trap.	---
HTTPS server	---	443	System port	HTTPS	Open	Used for communications with the Sysmac Studio.	Use the Packet Filter. [*3]
EtherNet/IP tag data links	2222	---	User port	CIP	Open	Used for the EtherNet/IP tag data links.	On the Sysmac Studio, select **EtherNet/IP Port Settings** - **CIP Settings**, and then select **Do not use** for **CIP Message Server**.
Sysmac Studio	9600	---	User port	OMRON protocol	Open	Used for communications with the Sysmac Studio.	Use the Packet Filter. [*4]

Application	UDP port number	TCP port number	Port type	Protocol used	Default port state	Usage	How to change from open to close
CIP messages	44818	44818	User port	CIP	Open	Used for the CIP messages.	On the Sysmac Studio, select **EtherNet/IP Port Settings** - **CIP Settings**, and then select **Do not use** for **CIP Message Server**.

*1. The TCP/UDP port used for communications between the CPU Unit and the NX-series EtherNet/IP Unit via the X Bus. It cannot be used by a user.

*2. An abbreviation for Routing Information Protocol. RIP is a protocol used to exchange route information between communications devices such as routers in order to find the shortest distance from one point to another point in the network.

*3. Closing the port may prevent communications with the Sysmac Studio and the NA-series HMI. Refer to *Troubleshooting when support software cannot go online* in the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* on how to make corrections.

*4. Closing the port may prevent communications with the Sysmac Studio. Refer to *Troubleshooting When You Cannot Go Online from the Sysmac Studio* in the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* on how to make corrections.

Index

Index

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:

Cat. No. W627-E1-02 0623