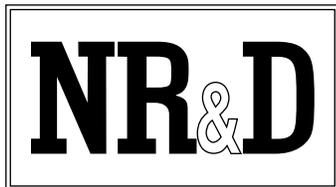


CNOE-800

Installation and Programming Manual

This Manual describes the installation and operation of the CNOE-800 Compact option module.

Effective: 08 June, 2006



Niobrara Research & Development Corporation
P.O. Box 3418 Joplin, MO 64803 USA

Telephone: (800) 235-6723 or (417) 624-8918

Facsimile: (417) 624-8920

www.niobrara.com

POWERLOGIC, SY/MAX, and Square D are registered trademarks of Square D Company.

Modicon, TSX Compact Automation, FactoryCast, Concept, ProWorx, Modbus, and Modbus Plus are registered trademarks of Schneider Automation.

Subject to change without notice.

© Niobrara Research & Development Corporation 2002 - 2004. All Rights Reserved.

Contents

1 Introduction	15
2 Installation and Configuration	17
Module Installation	17
IP Address Configuration	17
Windows to Default IP Address	17
BOOTP/DHCP	17
MSTR's to the CNOE-800	17
Default Gate and Subnet Mask	18
Serial Port Configuration	18
PLC Configuration	18
Resetting to Factory Default Configuration	18
Module Configuration	18
Accessing mailbox and configuration registers	20
CNOE-800 mailbox registers	21
RTS/CTS Handshaking	21
CTS Operation	21
RTS Operation	21
MNIM Compatibility	21
3 SY/MAX and Modbus Message Routing	25
SY/MAX Routing	25
SY/MAX Serial Routing	25
SY/MAX Ethernet Routing	27
Modbus Routing	29
Modbus Serial Routing	29
4 TCP/IP Ethernet Protocol	31
IP Addressing	31
Subnet Masks	32
Default Gateway	32
Port Number	32
Modbus TCP/IP Protocol Mode	32
Client/Server	32
Client IP Look-up Table	33

Server Index Look-up Table	33
Modbus TCP/IP Example	34
Client Operation	34
Server Operation	35
5 SY/MAX 802.3 Mode	37
6 MBTCP+SY/MAX Ethernet MODE	39
MBTCP+SY/MAX Example	39
7 MSTR Operation	43
The MSTR Instruction	43
MSTR Diagram	43
Inputs	44
Outputs	44
Control Block Content	44
Middle Node Content	45
Bottom Node Content	45
Control Block Operation	45
Opcode 1 (Write Multiple 4x Registers)	46
Opcode 2 (Read 4x Registers)	47
Opcode 101 (Write Multiple 0x Coils)	48
Opcode 102 (Read 0x Coils)	49
Opcode 103 (Read 1x Coils)	50
Opcode 106 (Read 3x Registers)	52
Opcode 108 (Write 4x Single Register)	53
Opcode 109 (Write 0x Single Coil)	54
Opcodes 111 & 112 (Read/Write Option Module Port Configuration)	55
Opcode 512 (Reset Option Module to Factory Defaults)	58
Opcode 513 (Set Option Module IP Address)	59
Opcode 516 (Set Option Module Subnet Mask)	59
Opcode 517 (Set Option Module Default Gate)	60
MSTR Error Codes	60
8 Ethernet I/O Scanner	63
Introduction	63
Configuring the Ethernet I/O Scanner Using RPCSW32	63
IP Address	63
ID	63
Timeout	63
Scan Rate	63
Register Space	64
Master (Under Read or Write)	64
Slave (Under Read or Write)	64
Cnt (Under Read or Write)	64
H/O	64
Copying, Pasting, and Automatically Incrementing	64
Editing Global I/O Scanner Configuration	64
Ethernet I/O entries per socket	65

9	MODBUS Modes	67
	Modbus Overview	67
	SY/MAX Message Addressing	68
	Message Translations	68
	SY/MAX to Modbus Translations	68
	Modbus to SY/MAX Translations	69
	Master Operation	69
	Register Bias	70
	Register Calculations	70
	Bit Calculations	70
	Modbus Retries	71
	Driver Mode	71
	RS-485 MODBUS Host Master Mode Example	72
	Modbus Slave Operation	72
	PowerLogic Software use with Modbus Devices	75
	Register 8188	75
	Non-Priority Random Access Reads	76
10	SY/MAX MODE	77
	Mode 1: SY/MAX	77
	SY/MAX Routing Example	77
11	NET-TO-NET MODE	79
	Mode 2: Net-to-Net	79
	NIM Net-to-Net Example	79
	EPE5 Net-to-Net Example	80
12	Peripheral Mode	83
	Mode 3: Peripheral	83
	Driver Mode	83
	Peripheral Mode Example	84
13	Transparent and Share Modes	85
	Modes 4,5: Transparent, Share	85
	TRANSPARENT Mode Example	86
	Driver Mode	87
14	PLogic and PNIM Modes	89
	Mode 6: PowerLogic	89
	PowerLogic Mode Example	90
	Mode 11: PNIM	91
	PNIM Mode Example	92
15	IDEC Mode	95

Mode 7: IDEC	95
Micro-1 and Model 50 Interfacing	95
Micro-1 register addressing	95
Model 50 register addressing	96
IDEC Mode Example	97
16 Gateway Mode	99
Mode 8: Gateway	99
ASCII Command Gateway Functions	99
Gateway READ command	99
Gateway WRITE command	100
Gateway SET command	100
Gateway CLEAR command	100
Gateway BIT command	100
Gateway PRINT command	100
Gateway OMIT Print Command	101
Gateway ADDRESS command	101
Gateway Mode Example	101
BASIC Language Example Program	102
17 Multidrop Mode	103
Mode 9: Multidrop	103
Multidrop Mode Example	104
Driver Mode	105
18 RNIM Mode	107
NORMAL Operation	107
BID Operation	108
Single Slave BID Operation	109
Automatic BID Operation (100 + n)	109
Automatic BID Operation (200 + n)	109
Automatic BID Operation (300 + n)	110
Data Store and Forward Operation	110
Broadcast Operation	111
Mode 12: RNIM Master	112
Mode 13: RNIM Slave	113
Driver Mode	114
Pt to Pt	114
Half Duplex	114
Two Wire	114
RTS/CTS Operation	115
19 Transfer Mode	117
Transfer Example	117
PLC Ladder Rungs	119
"On Ethernet" Example	119

20 Chevron Mode	121
21 Dual Slave Mode	125
SMS Example	125
PLC Programming Example	129
22 Auto-transfer and Auto-Scan	133
Auto-Transfer	133
Auto-Scan	134
Auto-Scan Status	134
Auto-Scan Watchdog	135
Auto-Scan Watchdog Example	135
23 EPeer Mode	137
EPEER Mode	137
24 On Ethernet Option	141
25 Configuration Software RPCSW32	143
RPCSW32	143
Data Entry Keys	144
Online and Offline Editing Screen	145
Drop Number	145
On Ethernet	145
Protocol	146
Baud Rate	146
Parity	146
Data Bits	146
Stop Bits	146
Buffer Limit	146
Mode Specific Sub-menus	146
Driver Mode	146
IP Address	146
Subnet Mask	147
Default Gate	147
MBAP TCP Port	147
TCP Backoff	147
Downstream Timeout	147
Quiet Timeout	147
IP Framing	147
MAC Address	147
E-Peer	148
Error Check	148
Route Appendix	148
Route Replacement	148
Packet size limit	148

Packet time limit	148
Target Route	148
Control Character	148
Echo	149
Highlight	149
Node Priority	149
Number of Nodes	149
Time Slice	149
READ command	149
WRITE command	149
Retry timeout	149
Register Bias	149
Transfer Interval	149
Transfer Route	150
READ Count	150
READ From	150
READ To	150
WRITE Count	150
WRITE To	150
WRITE From	150
Total E-Peer Nodes	150
This Node's Number	150
Start Register	151
Register Count	151
Destination Reg	151
Update Interval	151
Network Id	151
CTS Timer	151
Packet response	151
Bid interval	151
Retries	151
Pause time	152
Message Count	152
Bid Address	152
Transfer Route	152
Backplane Port Mode	152
MSTR Message Reply Timeout	153
Programming Channel idle timeout	153
Ethernet I/O Scanner	153
Ethernet I/O Entries Per Socket	153
HOTKEYS	153
F1 Print Screen hotkey	153
F2 Help Window	153
F3 Statistics Viewer	154
Modbus Slave Routing	162
Port Number	163
Starting Address	163
Address	163
Target TYPE	163
ROUTE	163
Modbus Server Routing for Ethernet Port	164
Index	164
Target TYPE	164
ROUTE	164
Auto-Scan Table	164
Local	165
Remote	165

Count	165
Operation	165
ROUTE	165
Ethernet I/O Scanner	165
IP Address	166
ID	166
Timeout	166
Scan Rate	166
Register Space	166
Master (Under Read or Write)	166
Slave (Under Read or Write)	166
Cnt (Under Read or Write)	166
H/0	166
Outgoing TCP Routing	167
Drop	167
IP Address	167
Downstream Route	167
Offline Functions	167
"Read from disk to memory"	167
"Write from memory to disk"	168
"Edit configuration in memory"	168
"edit Modbus routing"	168
"edit Ethernet I/O scan table"	168
"edit TCP routing"	168
"Send memory to module"	169
"Fetch memory from module"	169
"Print configuration in memory"	169
"Delete configuration file"	169
"Quit offline functions"	169
Utilities	169
View registers	169
Terminal Emulator	170
SETUP	171
Serial SETUP	171
Personal Computer COM: port	171
Modbus/TCP Connection	173
Terminal Emulator SETUP	174
Register Viewer Setup	174
Load from File	175
Command Line Parameters	175

26 Local Registers 177

Module Register Overview	177
Mailbox Registers	178
Statistics Registers	178
Ethernet Port Statistics	178
Data Port Statistics	181
IP Routing Table	183
TCP/IP Port Number	185
TCP/IP Step Size for Incremental Backoff	185
TCP/IP Downstream Timeout	185
TCP/IP Quiet Timeout	185
Ethernet Addresses of Known Drops Registers	185
IP Addresses of Connected Devices	186
E-Peer Active Register	187

E-Net Search	187
Auto-Scan Table Registers	187
Modbus Slave Address Tables	188
TCP/IP Routing Table	189
Setup and Configuration Registers	190
Ethernet Port Control Registers	190
Data Port Control Registers	191
Backplane Port Control Registers	194
Options	196
Clear Function Register	198
Module Identification Registers	198
Global Options Register (Register 8190)	199
Global Options	200

27 Connector Pinouts 201

RS-232 ports on CNOE-800 (RJ45 socket)	201
RS-422/485 ports on CNOE-800 (RJ45 socket)	202
10BaseT (Twisted Pair) Ethernet port on CNOE-800 (RJ45 socket)	202

28 Recommended Cabling 205

Cabling required to configure a CNOE-800	205
CNOE-800 RS-232 to personal computer cabling	205
CNOE-800 RS-232 to 9-pin DTE	205
CNOE-800 RS-232 to 25-pin DTE	206
CNOE-800 RS-485/422 to SY/MAX 9-pin Port	206
Isolated Cabling to SY/MAX Port	207

Appendix A Modbus/TCP Protocol Specifications 209

Appendix B NR&D Internet Access 211

Figures

Figure 1-1 CNOE-800 Front Panel	16
Figure 3-1 Direct connection without route	25
Figure 3-2 Single Network Example	26
Figure 3-3 Multiple Network Example	27
Figure 3-4 Simple Ethernet Network	28
Figure 3-5 Ethernet Router Example	29
Figure 3-6 Modbus Network Example	30
Figure 4-1 RPCSW32 TCP Routing Table	33
Figure 4-2 RPCSW32 Modbus Server Routing Table	34
Figure 4-3 Modbus TCP/IP Example	34
Figure 4-4 TCP/IP Ethernet MSTR Example	35
Figure 6-1 MBTCP+SY/MAX Routing Example	41
Figure 7-1 MSTR Block Diagram	44

Figure 7-2 Sample MSTR	46
Figure 9-1 MODBUS Master Mode Example	72
Figure 9-2 OTHER Modbus Slave Example	73
Figure 9-3 Modbus through SY/MAX Example	74
Figure 9-4 RPCSW32 Modbus Routing Editing Screen	75
Figure 10-1 SY/MAX Mode Example	78
Figure 11-1 NIM Net-to-Net Example	79
Figure 11-2 EPE5 Net-to-Net Example	81
Figure 12-1 Peripheral mode example	84
Figure 13-1 Transparent Mode Example	86
Figure 14-1 PowerLogic Example	90
Figure 14-2 PNIM Modbus/TCP Example	92
Figure 15-1 IDEC Mode Example	97
Figure 16-1 GATEWAY Example	101
Figure 16-2 Terminal Emulator connected to Gateway port	102
Figure 17-1 Multidrop Example	104
Figure 18-1 NORMAL RNIM Example	108
Figure 18-2 RNIM Repeater Example	111
Figure 19-1 Transfer Example 1	118
Figure 19-2 Transfer Communication Rungs	119
Figure 20-1 Chevron Radio Example	122
Figure 20-2 Chevron POWERLOGIC Example	123
Figure 21-1 Dual Slave SMS Example	126
Figure 21-2 Dual Slave PLC Programming Example	129
Figure 22-1 Auto-Scan Watchdog Example	135
Figure 23-1 EPEER Update Interval Timing	139
Figure 24-1 On Ethernet Example	142
Figure 25-1 RPCSW32 Startup Screen	144
Figure 25-2 RPCSW32 oFfline Menu	144
Figure 25-3 RPCSW32 oNline Edit Screen	145
Figure 25-4 F1 Print Screen	153
Figure 25-5 F2 Help Window	154
Figure 25-6 Ethernet Port Statistical Screen (Page 1)	154
Figure 25-7 Ethernet Port Statistical Screen (Page 2)	155
Figure 25-8 Ethernet Port Statistical Screen (Page 3)	155
Figure 25-9 Backplane Port Statistical Screen (Page 1)	157
Figure 25-10 Backplane Port Statistical Screen (Page 2)	157
Figure 25-11 Backplane Port Statistical Screen (Page 3)	158
Figure 25-12 Port 1..2 Statistical Screen (Page 1)	160
Figure 25-13 Port 1,2 Statistical Screen (Page 2)	160
Figure 25-14 Edit Modbus Slave Routing	163
Figure 25-15 Modbus Server Routing for Ethernet Port	164
Figure 25-16 Edit Auto-Scan Table	165
Figure 25-17 Edit Auto-Scan Table	166
Figure 25-18 Edit TCP Routing	167
Figure 25-19 oFfline Read from Disk to Memory	168
Figure 25-20 View Registers	170
Figure 25-21 Terminal Emulator	171
Figure 25-22 SY/MAX Setup Screen	172

Figure 25-23 MODBUS/TCP Setup Screen	173
Figure 25-24 Terminal Emulator Setup Screen	174
Figure 25-25 Terminal Emulator Setup Screen	175
Figure 27-1 Ports 1 and 2 RJ45	201
Figure 27-2 Ports 1 and 2 RJ45	202
Figure 27-3 Ethernet Port RJ45	203

Tables

Table 2-1 Suggested Number of PADs for Hayes Modem Operation	22
Table 3-1 Direct connection routes	25
Table 3-2 Single Network Connection Routes	26
Table 3-3 Multiple Network Connection Routes	27
Table 3-4 Simple Ethernet Network Routes	28
Table 3-5 MEB Routes	29
Table 3-6 Modbus routes	30
Table 4-1 IP Network Classes	32
Table 4-2 Default subnet masks	32
Table 4-3 Modbus/TCP MSTR Example	35
Table 4-4 Modbus Routing for the CNOE-800 E-net port	35
Table 6-1 CNOE-800 IP Table Example	39
Table 6-2 Server Index Table For CNOE-800	39
Table 6-3 Model 450 Routing Examples	40
Table 6-4 NOE Routing Examples	40
Table 7-1 Supported MSTR Opcodes	43
Table 7-2 Supported MSTR Opcodes	45
Table 7-3 Opcode 1 to Modbus/TCP Target	46
Table 7-4 Register Correlation	46
Table 7-5 Opcode 2 Read from Modbus Serial Target on Port 1	47
Table 7-6 Register Correlation	48
Table 7-7 Opcode 101 to Modbus/TCP Target	48
Table 7-8 Bit Correlation between PLC and Target	49
Table 7-9 Opcode 102 Read from Modbus Serial Target on Port 1	50
Table 7-10 Bit Correlation between PLC and Target	50
Table 7-11 Opcode 103 Read from Modbus/TCP Target	51
Table 7-12 Bit Correlation between PLC and Target	52
Table 7-13 Opcode 106 Read from Modbus/TCP Target	53
Table 7-14 Register Correlation	53
Table 7-15 Opcode 108 Write to Modbus Serial Target on Port 2	54
Table 7-16 Register Correlation	54
Table 7-17 Opcode 109 to Modbus/TCP Target	54
Table 7-18 Bit Correlation between PLC and Target	55
Table 7-19 Opcodes 111 & 112 Read/Write Option Module Port Configuration	55
Table 7-20 Ethernet Port Control Registers	56
Table 7-21 Ports 1 and 2 Configuration Registers	57
Table 7-22 Ports 1 and 2 Configuration Registers (Continued)	58
Table 7-23 Backplane Port Configuration Registers	58
Table 7-24 Opcode 512 Reset Option Module to Factory Defaults	59
Table 7-25 Opcode 513 Set Option Module IP Address	59

Table 7-26 Opcode 516 Set Option Module Subnet Mask	60
Table 7-27 Opcode 517 Set Option Module Default Gate	60
Table 7-28 MSTR Error Codes	61
Table 8-1 Diagnostic Block Error Codes	65
Table 8-2 SY/MAX Mode CNOE-800 Setup Example	65
Table 8-3 SY/MAX Mode Personal Computer Route Examples	66
Table 8-4 SY/MAX Mode PLC Route Examples	66
Table 8-5 QUCM Equivalent routes for accessing internal registers	66
Table 9-1 MODBUS Function Code List	67
Table 9-2 SY/MAX Messages	68
Table 9-3 SY/MAX to Modbus Translations	68
Table 9-4 Modbus to SY/MAX Translations with type = "OTHER"	69
Table 9-5 SY/MAX Register to Modbus Register Relationship	70
Table 9-6 SY/MAX Bit to Modbus Coil Relationship	71
Table 9-7 MULTIDROP Routing Examples	72
Table 9-8 CNOE-800 Setup for MULTIDROP Master Connection	72
Table 9-9 Modbus Slave Example Setup	73
Table 9-10 Modbus Example Configuration	73
Table 9-11 Modbus Example Setup	74
Table 9-12 CNOE-800 I configuration	74
Table 9-13 CNOE-800 II configuration	74
Table 9-14 Modicon PLC ID Values	75
Table 11-1 NIM Net-to-Net Routing	79
Table 11-2 MEB Setup for NIM Net-to-Net Connection	80
Table 11-3 NIM Net-to-Net Routing with "On Ethernet"	80
Table 11-4 EPE5 Net-to-Net Routing Examples	81
Table 11-5 CNOE-800 Setup for EPE5 Net-to-Net Connection	81
Table 11-6 EPE5 Setup for EPE5 Net-to-Net Connection	81
Table 11-7 EPE5 Net-to-Net Routing Examples with "On Ethernet"	82
Table 12-1 Peripheral Routing Examples	84
Table 12-2 CNOE-800 Setup for Peripheral Connection	84
Table 13-1 Transparent Routing Examples	86
Table 13-2 CNOE-800 Setup for TRANSPARENT Connection	86
Table 13-3 EPE5 Setup for TRANSPARENT Connection	87
Table 14-1 PowerLogic Routing Examples	90
Table 14-2 CNOE-800 Setup for PowerLogic Connection	91
Table 14-3 CNOE-800 Modbus/TCP Server Setup	92
Table 14-4 SMS3000 Device Setup	93
Table 14-5 CNOE-800 Setup for PNIM Connection	93
Table 15-1 Micro-1 Processor Equivalent Register List	96
Table 15-2 Model 50 Processor Equivalent Register List	96
Table 15-3 IDEC Routing Examples	97
Table 15-4 CNOE-800 Setup for IDEC Connection	97
Table 16-1 Gateway Command Examples	102
Table 17-1 MULTIDROP Routing Examples	105
Table 17-2 CNOE-800 (1) Setup for MULTIDROP Connection	105
Table 17-3 SPE4 Setup for MULTIDROP Connection	105
Table 17-4 CNOE-800 (2) Setup for MULTIDROP Connection	105
Table 18-1 Broadcast Route Values	112

Table 18-2 RNIM Master Register Summary	113
Table 18-3 RNIM Slave Register Summary	114
Table 19-1 Transfer Route Registers	118
Table 20-1 POWERLOGIC CHEVRON Example	123
Table 21-1 POWERLOGIC Example DUAL SLAVE Port	126
Table 21-2 POWERLOGIC Example DUAL SLAVE Port Modbus Routing	126
Table 21-3 POWERLOGIC Example CHEVRON Port	127
Table 21-4 POWERLOGIC Example SMS Communications Connection - Serial	127
Table 21-5 POWERLOGIC Example SMS Setup Devices/Routing	128
Table 21-6 PLC Programming Example DUAL SLAVE Port	129
Table 21-7 PLC Programming Example DUAL SLAVE Port Modbus Routing	129
Table 21-8 PLC Programming Example SY/MAX and Modbus Gate Ports	130
Table 21-9 PLC Programming Example SY/MATE Settings	130
Table 21-10 PLC Programming Example Modsoft Settings	131
Table 22-1 Auto-Scan Entries for both CNOE-800's	136
Table 23-1 E-PEER Register List Example	137
Table 24-1 On Ethernet Routing Examples	142
Table 26-1 Module 4x Register Overview	177
Table 26-2 SY/MAX Ethernet Port Statistics Registers	179
Table 26-3 TCP/IP Ethernet Port Statistics Registers	180
Table 26-4 Ports 1 and 2 Statistics Registers	182
Table 26-5 Backplane Port Statistics Registers	183
Table 26-6 IP Router Table	184
Table 26-7 Ethernet Physical Address Registers	186
Table 26-8 IP Address of connected Sockets Registers	187
Table 26-9 Auto-Scan Configuration Registers	188
Table 26-10 Modbus Slave Address Table	189
Table 26-11 Modbus Slave Starting Address Register	189
Table 26-12 Outbound TCP/IP Routing Table	190
Table 26-13 Module Setup Identification Registers	190
Table 26-14 Ethernet Port Control Registers	191
Table 26-15 Ports 1 and 2 Configuration Registers	192
Table 26-16 Ports 1 and 2 Configuration Registers (Continued)	193
Table 26-17 Baud Rate Values	193
Table 26-18 Data Bits Values	194
Table 26-19 Parity Values	194
Table 26-20 Stop Bits Values	194
Table 26-21 Port Mode Values	194
Table 26-22 Backplane Port Configuration Registers	195
Table 26-23 Options Register Values	196
Table 26-24 Clear Function bit-map	198
Table 26-25 Module Identification Registers	199
Table 26-26 Module ID Example	199
Table 26-27 Global Options Register Values	200
Table 27-1 RS-232 Pinout	201
Table 27-2 RS-485 Pinout	202
Table 27-3 10BaseT Pinout	203

Introduction

The Niobrara CNOE-800 is a TSX Compact[®] option module that gives a Modicon Compact PLC an Ethernet port and/or two extra serial ports. The Ethernet port means the PLC can be programmed via Ethernet, and the PLC can issue MSTR instructions to other devices on the network. The two additional serial ports mean the PLC can issue MSTR instructions out additional serial ports, and in different protocols. The ports also give more serial masters, such as Concept, access to the PLC.

The Ethernet port is a 10baseT port, and can be connected to a standard Ethernet hub. The port can be configured for Modbus/TCP, SY/MAX 802.3, or a combination of these two protocols. The serial ports are switchable RS-232/RS-485 ports. The ports can be configured for any of the standard Niobrara protocol settings. These settings are: SY/MAX, Net-To-Net, Peripheral, Transparent, Share, PLOGIC, IDEC, Gateway, Multidrop, Modbus Host, PNIM, RNIM Master, RNIM Slave, Modbus Gate, Transfer, Chevron, Apollo, Modbus ASCII, and Dual Slave.

The CNOE-800 must be mounted in the primary Compact rack, and can be mounted in slot 3, 4, or 5.

Note: The CNOE-800 will only function with the 386-based Compact Controllers, which are part numbers PC-E984-258, -265, -275, and -285. Additionally, these controllers, must be loaded with Exec version 2.07D or later, which will allow the PLC to support option modules.

Warning: Do not attempt to download new PLC EXEC's through the CNOE-800! The download WILL fail, and the PLC may be rendered unusable. Always perform EXEC downloads via Modbus Plus or Modbus RTU.

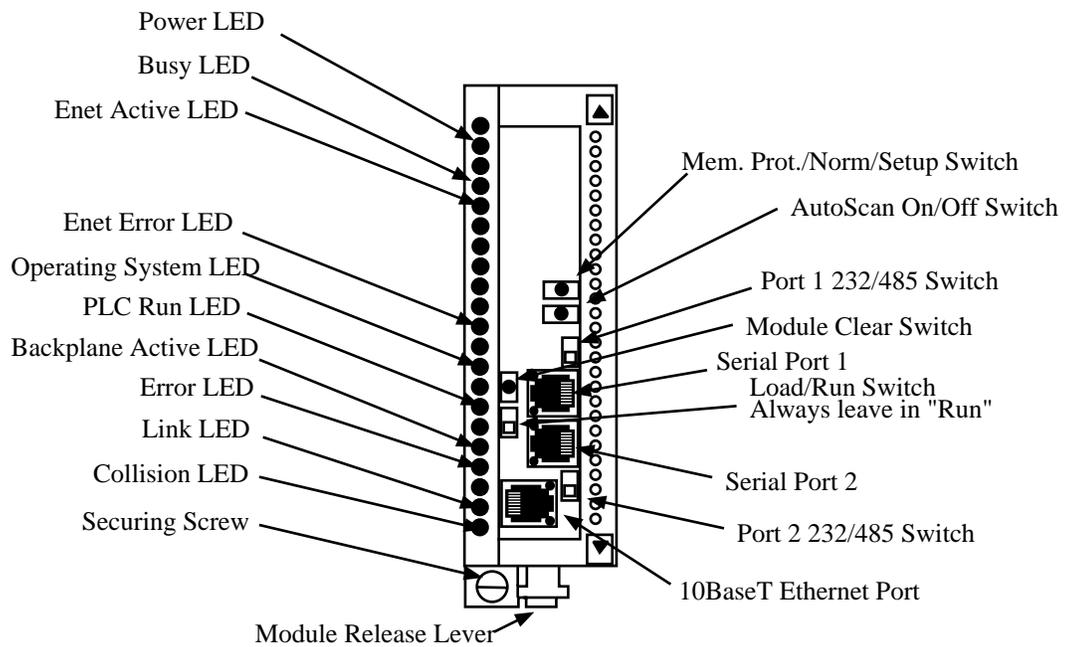


Figure 1-1 CNOE-800 Front Panel

Installation and Configuration

Module Installation

- 1 Make sure the Compact rack is powered down!
- 2 Mount the CNOE-800 in an available slot in the primary rack. Secure the screw at the bottom of the module.

IP Address Configuration

The CNOE-800 comes with a default IP address of 10.10.10.10. A PC on the network running Windows ME/2000/XP can very easily add an additional IP address to an existing adapter, and configure a new IP address using RPCSW32. The CNOE-800 can obtain an IP address via BOOTP or DHCP, or from the PLC using MSTR instructions. At some point in the future, Concept may also support config extensions for Compact PLC's.

Windows to Default IP Address

In the Control Panel of Windows there is an icon for setting up network adapters. Within the setup for adapters is a setting for the properties of TCP/IP. Within the properties, there is an "Advanced" setup button. Click on this button, and add a new IP address of 10.10.10.9. This should be accompanied by a default subnet mask of 255.0.0.0. The PC can now connect to the CNOE-800 as described in the RPCSW32 chapter.

BOOTP/DHCP

The CNOE-800 can get its IP address from any BOOTP or DHCP server on the network. It will also support BOOTP Lite, available from Modicon. Unless the feature is disabled, the CNOE-800 will attempt to obtain a new IP address each time power is cycled. To disable, the user must connect with RPCSW32, and edit the port's parameters, or the register may be directly edited from any available register viewer. The register that controls this option is listed in the port parameters section of the local registers list.

MSTR's to the CNOE-800

The CNOE-800 may also get its IP address from MSTR instructions written directly to the CNOE-800. The user would program an MSTR block where the opcode is 513, the high byte of the fourth implied register is the slot number of the CNOE-800, and the fifth through eighth implied registers contain the

four bytes of the IP address. This will be explained in further detail in the sections covering MSTR instructions.

Default Gate and Subnet Mask

If required, the CNOE-800 can obtain a default gate and subnet from any of three sources: BOOTP/DHCP servers, RPCSW32, or MSTR instructions. A BOOTP or DHCP server will normally hand these values to the CNOE-800 at the same time as the IP address. Once an IP address is established, a user may connect to the CNOE-800 using RPCSW32, and edit the parameters for the Ethernet port. If MSTR's are used, the opcodes are 516 for subnet mask and 517 for default gate, in the same format as described for setting the IP address.

Serial Port Configuration

By default, serial port 1 is set to be Dual Slave, which is a combination of SY/MAX and Modbus RTU slave. Port 2 is set for Modbus ASCII. Both ports are set at 9600 baud, even parity, and one stop bit. Port 1 is set for 8 data bits, and Port 2 is set for 7. All of these parameters are programmable from either RPCSW32 or MSTR's using opcodes 111 and 112 to read and write. Both methods of modifying the ports will be discussed later in the manual.

PLC Configuration

Since the CNOE-800 is an option module, it really is not necessary to configure it within any software package. Additionally, at the writing of this manual, no programming package supports option modules for the Compact PLC. Contact Modicon for new releases of Concept or ProWorx.

Resetting to Factory Default Configuration

The reset button on the front of the CNOE-800 will reset it back to factory default configuration. To accomplish this, remove the module from the rack, and hold the button in for approximately 20 seconds. Additionally a PLC could reset the module to factory defaults by programming an MSTR instruction with opcode 512. This will be discussed later in the manual.

Module Configuration

Modification of the configuration registers may be accomplished by writing to them via Ethernet with any device capable of generating Modbus/TCP write messages, or via either serial ports with any device capable of generating a SY/MAX or Modbus write. However, it is most conveniently accomplished with the Win32 console program RPCSW32, which is provided with the module at no cost. RPCSW32 may use SY/MAX, Net-To-Net, Gateway, Modbus RTU, Modbus ASCII, or Modbus/TCP.

The configuration and mailbox registers are maintained in nonvolatile memory. This memory is powered by an internal capacitor for approximately 24 hours when the module is removed from the rack.

Each port must have certain parameters configured for proper operation. These parameters include:

- **Drop Number** - The drop number is the device address for that port. The drop number is included in the Route portion of all SY/MAX communication messages and helps to determine the particular units involved in the communication. There are three types of drop numbers:
 - **Ethernet Drop Number** - The Ethernet Drop Number must fall within the range of 00 through 99. This number must be unique from all other SY/MAX 802.3 Ethernet units on the network. If two SY/MAX Ethernet ports have the same Ethernet Drop Number, they will stop communicating and must be manually reset. The factory default Ethernet Drop Number is 00. The drop number has no real meaning in Modbus/TCP mode unless the port is being routed through from some other port.
 - **Data Port Drop Number** - The Data Port Drop Number must fall within the range of 000 through 199. This number must only be unique within a particular CNOE-800. It is permissible to have other CNOE-800 units on the same network with similar Data Port Drop Numbers as long as their Ethernet Drop Number is different.

The factory default Data Port Drop Numbers for Ports 1 and 2 of the CNOE-800 are 002, and 102. For most circumstances these need not be changed. When connecting to a NIM (CRM-510) in Net-to-Net mode, the Data Port Drop Number must be set to match the NDN of the NIM port.

- **Backplane Port Drop Number** - The Backplane Port Drop Number must fall within the range of 000 through 199. This number must only be unique within the CNOE-800. This number is used by the CNOE-800 to route to the PLC.
- **On Ethernet** - The On Ethernet setting determines whether the Data Port or Modbus Port drop number also appears on the Ethernet network. When set to YES, the QUCM accepts messages on the Ethernet targeted for this port as well as messages targeted to its own E-Net port. The "On Ethernet" port drop number must be unique to the Ethernet. This option is valid in SY/MAX 802 or MBTCP+SY/MAX Ethernet mode only.
- **Protocol Mode** - The Protocol setting controls the operation of the Ethernet Port and both Data Ports.
 - Possible values for the Ethernet port are SY/MAX 802, ,Modbus/TCP, and MBTCP+SY/MAX.
 - Possible values are SY/MAX, Net-to-Net, Peripheral, Transparent, Share, PLogic, Idec, Gateway, Multidrop, Modbus Host, PNIM, RNIM Master, RNIM Slave, Modbus Gate, Transfer, Chevron, Modbus ASCII, and DUAL SLAVE. The factory default value is SY/MAX mode. These modes are described in later chapters.
- **IP Address** - The IP address for the Ethernet port must be set when Modbus/TCP or MBTCP+SY/MAX is selected. The IP address must be unique for a given network and should be provided by the network administrator.
- **Subnet Mask** - The subnet mask must be configured in Modbus/TCP or MBTCP+SY/MAX modes for the specific network installed. Consult your network administrator for the proper subnet mask.
- **Default Gate** - The default gateway will be the IP address of the gateway router for the subnet that the CNOE-800 is installed upon. If all IP traffic is local to the physical network, this value may be left at 0.0.0.0.
- **Baud Rate** - The Baud Rate setting must be made to match the peripheral device. Possible values are 50, 75, 110, 134.5, 150, 300, 600, 1200, 1800, 2400, 4800, 7200, 9600, and 19200. (NOTE: If one port is set for 50 or 7200 baud, then the other port may not be set for 75, 150, 1800, or 19200 baud.) The factory default value is 9600 baud. Most SY/MAX and Modbus devices operate at 9600 baud.
- **Parity** - The Parity setting must match the attached peripheral. Possible settings are EVEN, ODD, and NONE. The factory default value is EVEN. Most SY/MAX devices operate at EVEN parity.
- **Data Bits** - The Data Bits setting must match the attached peripheral. Possible settings are 7 bits and 8 bits. The factory default value is 8 bits. All SY/MAX devices must operate with 8 data bits.
- **Stop Bits** - The Stop Bits setting must match the attached peripheral. Possible settings are 1 and 2. The factory default value is 1. Most SY/MAX devices operate with 1 stop bit.
- **Buffers** - The Buffers setting reflects the number of internal message buffers allocated to the Ethernet port. The possible range is 2 to 32 buffers. The factory default value is 32. There is seldom a need to adjust the number of buffers available to a port.
- **Error Check** - The CNOE-800 allows the option of choosing the checksum type for the SY/MAX, NET-TO-NET, and MULTIDROP protocols. The PNIM protocol must be set to CRC, all other modes default to the BCC. The CRC mode allows communication with the CRM-512 multimedia NIM, and SY/MATE PLUS ver. 2.x in parity= NONE setting. The CRC checksum provides a higher level of message security when the parity bit is not being used. When communicating to most SY/MAX devices, the BCC checksum must be used.
- **Driver Mode** - Certain modes of the CNOE-800 allow control of the RS-485 driver and receiver operation.

- The default parameter is point to point (**PT to PT**) where the RS-485 driver and receiver is always enabled. The PT to PT mode operates as a standard RS-422 port and may be used as a 4-wire RS-485 Master. The PT to PT mode allows full duplex operation. This driver mode is available in PERIPHERAL, SHARE, MULTIDROP, RNIM, and MODBUS port modes.
- The **FOUR WIRE** mode allows the RS-485 transmitter to tri-state (high impedance) when the CTS line is not asserted. This mode is used when the CNOE-800 port is a slave on a 4-wire network and is available in PERIPHERAL, SHARE, MULTIDROP, RNIM, and MODBUS modes.
- The **HALF DUPLEX** driver mode has the transmit driver enabled at all times, but disables the receiver while transmitting. This mode is useful when canceling an echo from an attached device. This mode is available in PERIPHERAL, SHARE, RNIM, and MODBUS modes.
- The **TWO WIRE** driver mode allows the RS-485 transmitter to tri-state (high impedance state) when the CTS line is not asserted. The receiver is also disabled while transmitting for a half duplex, multidrop operation. The TWO WIRE mode is suited for a 2-wire multidrop network and is available in the PERIPHERAL, SHARE, MULTIDROP, RNIM, and MODBUS port modes.
- **Route Appendix** - The Route Appendix allows the modification of the route of a SY/MAX packet arriving at the port. The route appendix is activated by having the special drop number 205 somewhere in the incoming packet. The drop number 205 is then replaced with the target route placed in the Route Appendix field. For example: A SY/MAX mode port with a drop number of 101 has the Route Appendix set for 016, 018, 001. An external device attached to that port sends a READ message with the route 101,205. The SY/MAX mode port replaces the 205 drop with the Route Appendix and the resulting route would be 101, 016, 018, 001. The Route Appendix is useful for devices such as the EATON PanelMate operator interface which can only handle 2 drop numbers in its route.
- **Route Replacement** - The Route Replacement is an extension of the Route Appendix feature. When the Route Replacement feature is ON, any incoming route on a SY/MAX message is ignored and the route in the Route Appendix is used instead. This feature may be used to adjust the target of operator interfaces without reprogramming the OI. The Route Replacement/Appendix may be enhanced to include up to 128 eight-drop routes by using Options bit 2. When this Options bit is set for the SY/MAX mode port, incoming route of the form 205,X will have the route located in the Modbus Slave Address Table entry X used for the replacement. The reply will be returned to the sender with the reversed route X,205. This feature may only be used on single-threaded SY/MAX ports and is primarily intended to be used with the PanelMate operator interface.
- **Auto-Transfer** - The Auto-Transfer settings control the operation of the automatic READ, and WRITE, functions for the automatic transfer of data from the peripheral device to the Mailbox register. The Auto-transfer features include Transfer Interval, Transfer Route, Read Count, Read From, Read To, Write Count, Write To, and Write From. The Auto-transfer features are available only on SY/MAX, NET-TO-NET, PLOGIC, IDEC, MODBUS, and PNIM modes.

Accessing mailbox and configuration registers

Reading and writing the CNOE-800 module's local registers is straightforward and is equivalent to reading and writing the registers in a Compact processor. One case requires some special attention. When a CNOE-800 is connected to SY/NET through a Net-to-Net connection to a NIM, the NIM will not pass packets whose terminal drop is that of the Net-to-Net port itself. To overcome this, append a dummy drop to the route to the CNOE-800 which is not the drop of any port in the module. For example, consider a SY/NET configuration with NIM modules number 0 and 1. If a CNOE-800 is connected to port 101, the CNOE-800 must be set so that the Net-to-Net port (connected to the NIM) also has drop 101. The route from the top port of NIM 0 to the CNOE-800's local registers could be 001,101,1. Any drop on SY/NET could also reach the CNOE-800 with a route of 201,101,1 where 201 is the don't care originating drop.

CNOE-800 mailbox registers

When configured as an I/O module, the first 64 mailbox registers within a CNOE-800 may be rack addressed by the PLC and used as PLC inputs or PLC outputs. The first 32 registers appear as 3x registers, and 33 through 64 appear as 4x registers. Data written to the output registers by the PLC appears in the associated mailbox register and may be read by an external device through a port of the CNOE-800.

The register number of the mailbox register is determined as follows:

- ANY OF THE PORTS: The mailbox registers are registers 1 through 2048.
- PLC RACK: The mailbox registers are 1 through 64. Registers 1 through 32 are inputs to the PLC, and 33 through 64 are output from the PLC.

RTS/CTS Handshaking

CTS Operation

In all modes, the CTS input of CNOE-800 ports one and two is available to restrain the CNOE-800 transmitter. If these pins are driven with active polarity, the port will transmit any time it has a message to send. If CTS is left open or driven with inactive polarity, the port will hold characters and not transmit them. CTS may be used by slower peripherals such as printers or displays to restrain the CNOE-800 while the peripheral catches up. CTS restraint cannot be held indefinitely with incoming data as the CNOE-800 has finite internal buffer capacity.

In Multidrop, Peripheral, Share, Modbus, and RNIM modes, there is an adjustable delay between when CTS is raised and when the port transmits. The RNIM CTS delay is controlled by registers 8042 and 8074 for Ports 1 and 2 respectively. The other modes are controlled by the value in registers 8064 and 8096. These register values are in 10mS units.

RTS Operation

The operation of RTS depends on the mode of the port. In SY/MAX, Net-to-Net, PowerLogic, Idec, Gateway, and Transparent mode the RTS pair is used to restrain the attached device sending to the CNOE-800 and inform it that the CNOE-800's internal buffers are filling faster than the received messages can be processed or retransmitted. In these port modes, RTS is normally active unless the CNOE-800 wishes the attached device to stop sending to it in which it will go inactive until the CNOE-800 can catch up.

In Multidrop, Peripheral, RNIM, Share, and Modbus modes, RTS acts in Request to Send fashion. In these port modes, it remains inactive until the port has information to transmit and then goes active until all current data has been transmitted. An external device such as a modem or radio normally accepts RTS as a "push to talk" and uses CTS to tell the CNOE-800 to "go ahead" and transmit.

MNIM Compatibility

The SY/MAX, Net-to-Net, and PLOGIC modes have the ability to adjust the number of PAD characters to define the amount of time that the CNOE-800 port will wait for a response before sending an ENQ. The normal (default) and minimum number of PAD characters sent is 10 characters. Values less than 10 will be ignored and 10 PADs will actually be sent. Registers 8064, and 8096 set the number of PAD characters for Ports 1 and 2 respectively.

The Message Inquire Delay Time (number of PADs) should be set to a value that is slightly longer than the actual turnaround time of the transmission media. Table 2-1 displays settings that have been found to work for a few Hayes compatible modems. Use these values as a fine tuning starting point.

Table 2-1 Suggested Number of PADs for Hayes Modem Operation

Baud Rate	Number of PADs
2400	30
9600	60
14400	90

The SY/MAX serial port channel delay statistics are at registers 2072 and 2104 for Ports 1 and 2 respectively. These registers display the number of bytes sent between the checksum at the end of the SY/MAX packet and the acknowledgment. Add 10 to this value to determine the number of PADs to set to for that channel.

Pressing the "T" key on the keyboard within RPCSW32 while viewing the second Statistics page on a serial port will automatically update the PAD count for the monitored channel.

Reloading Operating System

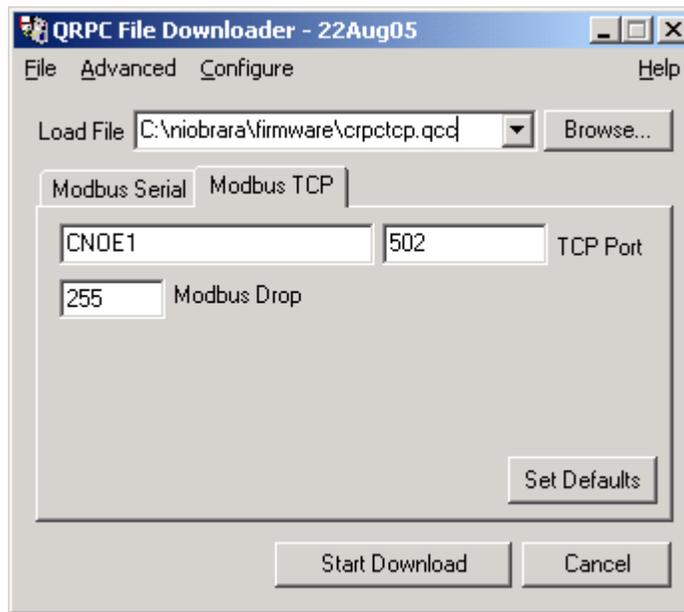


Figure 2-1 RPC Load of CRPC

- Start RPCLOAD.EXE
- Click on the Browse button and select the file crpctcp.qcc.
- Select the Application 1 Radio Button.
- Verify the following:
 - Status Register = 1.
 - Run Pointer Register = 33.
 - Auto Start is checked.
 - Erase Flash is checked.
 - Load File is checked.
 - The Modbus/TCP tab is selected.
 - * The IP Address of the QUCM is entered correctly.

- * The TCP Port number is set to 502.
- * The Modbus Drop is set to 255.
- Press the Start Download button. RPCLOAD will open a progress window to show the status of the download.

SY/MAX and Modbus Message Routing

This chapter provides an overview for SY/MAX and Modbus communication routing.

SY/MAX Routing

SY/MAX Serial Routing

The Square D SY/MAX communication protocol provides a robust full-duplex, peer-to-peer communication between PLCs, programming equipment, data collection equipment, and other peripheral devices. SY/MAX serial devices may communicate with each other directly in a point-to-point fashion. SY/MAX devices do not include network addresses and typically have RS-422 ports with a maximum baud rate of 19,200 baud.

When more than two devices are to be interconnected, external network routing hardware is required. This hardware may include Square D SY/NET Network Interface Modules (NIMs), Niobrara SPE4s, EPE5, MEBs, MUCMs, QUCMs, and CNOE-800's. Each serial port on these routing devices has a SY/NET network drop number assigned to it. These drop numbers are used to develop a path (ROUTE) between the SY/MAX device initiating the message and the target device.

In its simplest form this route is empty (NONE) when the source and target are directly connected. (Figure 3-1)

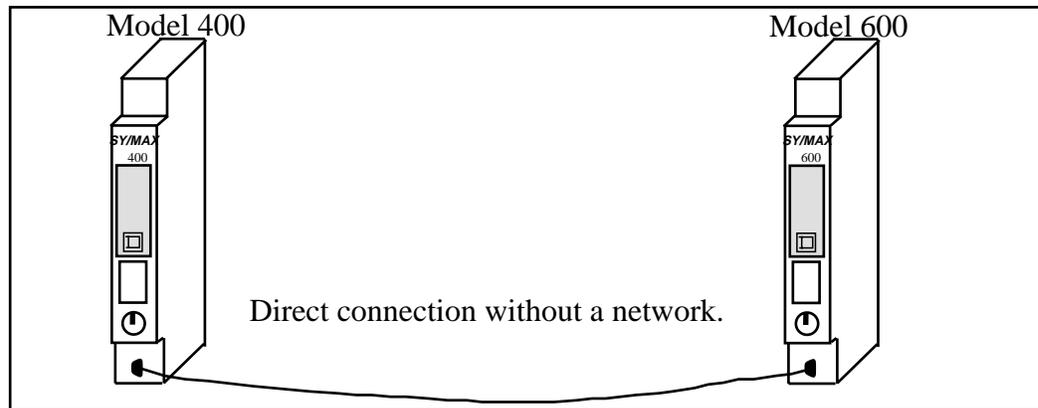


Figure 3-1 Direct connection without route

Table 3-1 Direct connection routes

Source	Target	Route
Model 400	Model 600	NONE
Model 600	Model 400	NONE

When an external network is required, the route contains at least two drops: the first drop is the source's network port, the second drop is the target's network port. In Figure 3-2 a Niobrara SPE4-1D is used as

the network device with Port 0 having a network drop number of 50, Port 1 = 51, Port 2 = 52, Port 3 = 53, and Port 4 = 54.

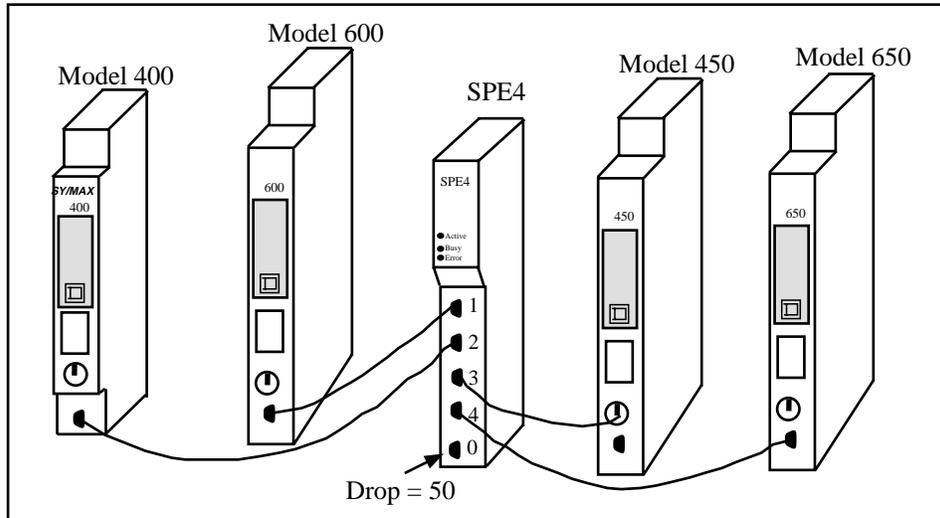


Figure 3-2 Single Network Example

Table 3-2 Single Network Connection Routes

Source	Target	Route
Model 400	Model 600	52, 51
Model 400	Model 450	52, 53
Model 400	Model 650	52, 54
Model 600	Model 400	51, 52
Model 650	Model 450	54, 53

Multiple networks may be connected together and each of these inter-network connections requires an additional drop in the route. (Figure 3-3) The SY/MAX protocol allows for up to 8 total drops in the route.

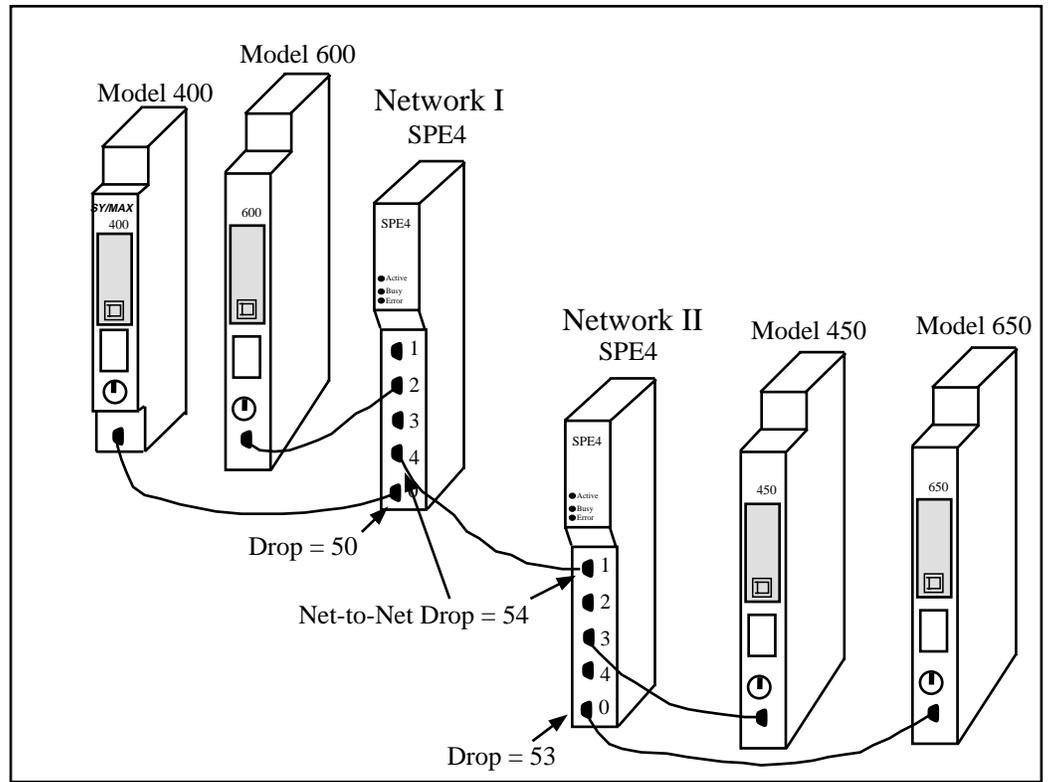


Figure 3-3 Multiple Network Example

Table 3-3 Multiple Network Connection Routes

Source	Target	Route
Model 400	Model 600	50, 52
Model 400	Model 450	50, 54, 56
Model 400	Model 650	50, 54, 53
Model 450	Model 650	56, 53
Model 450	Model 600	56, 54, 52
Model 650	Model 400	53, 54, 50

Connections between multiple networks may include SY/MAX networks, Ethernet networks, or translations between SY/MAX and other network protocols such as Modbus, Modbus Plus, PowerLogic, RNIM, or IDEC.

SY/MAX Ethernet Routing

The SY/MAX 802.3 Ethernet protocol developed as an extension of the SY/MAX serial protocol for high-speed networking (10Mb/sec). Square D PLCs such as the Model 450 and Model 650 processors include an Ethernet port (and virtual NIM) directly within the CPU module. With the network hardware embedded within the processor, the Ethernet port on the PLC has its own drop number. NOTE: This is different than the RS-422 serial ports on Square D PLC which have no built in networking address.

In the simple SY/MAX Ethernet case, devices may communicate by sending messages out their E-Net ports with a two drop route: the first drop is the source's E-Net port and the second drop is the target E-Net Port. (Figure 3-4)

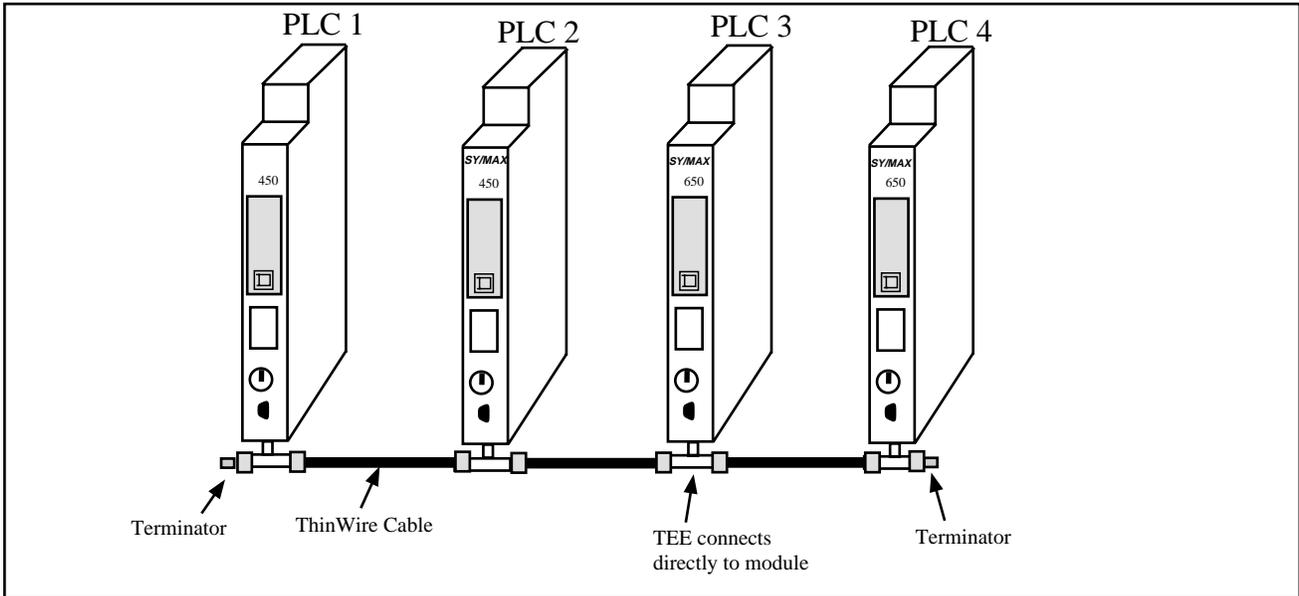


Figure 3-4 Simple Ethernet Network

Table 3-4 Simple Ethernet Network Routes

Source	Target	Route
PLC 1	PLC 2	1, 2
PLC 1	PLC 3	1, 3
PLC 1	PLC 4	1, 4
PLC 2	PLC 4	2, 4
PLC 4	PLC 3	4, 3
PLC 4	PLC 2	4, 2

It is sometimes necessary to connect other SY/MAX serial devices to the Ethernet network so NR&D has developed Ethernet routing modules such as the EPE5, the MEB, the QUCM, and the CNOE-800. These router devices treat the Ethernet as one network and the other serial (and Modbus Plus) ports as other networks. Therefore additional drop numbers are required within the route to negotiate through the router.

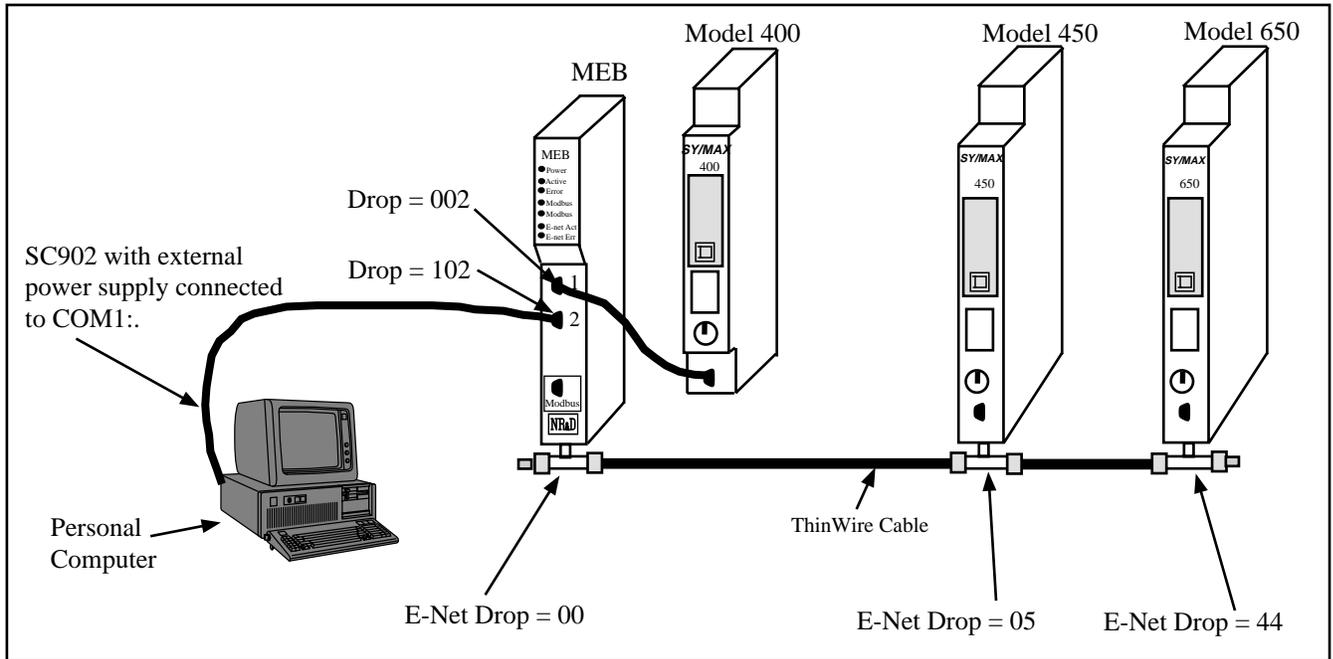


Figure 3-5 Ethernet Router Example

Table 3-5 MEB Routes

Source	Target	Route
Personal Computer	Model 400	102, 2
Personal Computer	MEB	NONE
Personal Computer	Model 450	102, 0, 5
Model 400	Model 650	2, 0, 44
Model 650	Model 450	44, 5

Certain modes of the ports on the Ethernet routers require additional drops in the route. Up to 8 total drop numbers are permitted in the route of a SY/MAX message.

Modbus Routing

Modbus Serial Routing

The Modbus serial protocol provides a master-slave method for programming and data transfer between programmable controllers and peripheral devices. Only the master can initiate the communication. The slaves are only capable of responding to messages sent from the master. Only one master is allowed on a network at one time. Each slave device is configured for a unique address. Each message sent by the master includes the address of the target slave. This technique allows multiple slaves to be placed on the same network.

The Modbus serial protocol has two transmission modes: ASCII and RTU. The ASCII protocol uses a 7-bit data structure and is intended for use with modems. The RTU protocol is the standard 8-bit binary message structure and offers a higher character density and better throughput than the ASCII version. The two protocols are not compatible on the same network at the same time. Modbus ports tend to be RS-232 or sometimes RS-485 and usually have a maximum baud rate of 19,200 baud.

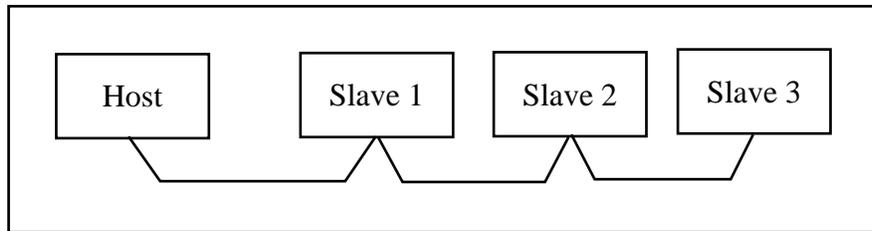


Figure 3-6 Modbus Network Example

Table 3-6 Modbus routes

Source	Target	Route
Host	Slave 1	1
Host	Slave 2	2
Slave 1	Slave 3	Not Directly Possible

Since the Modbus network operates as a master-slave system, it is not possible for slaves to directly communicate with each other. All information transfers must be managed by the host. For instance, if data from Slave 1 must be transferred to Slave 3, then the Host must read the data from Slave 1 and then write that data to Slave 3.

TCP/IP Ethernet Protocol

The Internet suite of protocols is commonly referred to as TCP/IP and includes IP, UDP, TCP, SNMP, Telnet, FTP, TFTP, SMTP, and NFS. The Internet Protocol (IP) is a network layer protocol that provides for packet delivery of all other protocols in the TCP/IP family. It does not provide for guaranteed delivery of packets, proper sequencing of the arrival of packets, or error detection. These features are provided by a higher level protocol such as TCP.

Transmission Control Protocol (TCP) is a connection-oriented means of delivering packets over IP. It provides for the error-free delivery, and proper sequencing of packets from the source to the destination. The application can simply hand a message to TCP and TCP will make sure that it arrives at the target. The CNOE-800 uses TCP/IP to send Modbus/TCP packets across the Ethernet.

User Datagram Protocol (UDP) does not provide for a reliable connection and relies on the application layer for error correction and sequencing. SNMP is the simple network management protocol. FTP is the file transport protocol and TFTP is the trivial file transport protocol. SMTP is the simple mail transport protocol while Telnet is a terminal emulation protocol and NFS is the network file system. The CNOE-800 does not directly support or respond to UDP, SNMP, FTP, TFTP, SMTP, or NFS packets although the internal IP router will process (route) these messages. The CNOE-800 does support a single telnet connection.

The CNOE-800 also provides some support for two other protocols in the TCP/IP suite: address resolution protocol (ARP) and internet control message protocol (ICMP). ARP is used to determine the 48-bit globally unique address of the source and destination Ethernet devices. The RPC-TCP provides ICMP echo request and echo reply support. The ping utility uses these ICMP messages to determine if a particular IP node is functional.

IP Addressing

Every node on a TCP/IP network has a unique IP address. This 32-bit value is typically represented in decimal notation where each byte of the address is displayed in decimal separated by periods (dotted-decimal). For example, a host on Niobrara's network might have the address CEDF331E (hex) is normally displayed as 206.223.51.30 in dotted-decimal notation.

A 32-bit IP address includes both the network ID and host ID for a node. The network ID specifies the network to which the node is attached. The network ID must be unique among all networks within a connected internet. On networks connected to the public Internet, this ID is provided by the InterNIC or DDN-NIC. The host ID identifies the node within its network. Each node must have a unique host ID within a network.

The Internet has been defined address classes to support different network sizes. Each network class is determined by the first byte of the IP address. Table 4-1 displays the IP classes and the total number of network and host IDs for each address class. The example is address w.x.y.z and network address 127 is reserved for loopback testing and interprocess communication on the local computer; it is not a network address. Net and Host IDs 0 and 255 are also reserved.

Table 4-1 IP Network Classes

Class	w values	Net ID	Host ID	Available nets	Available Hosts per net
A	1-126	w	x.y.z	126	16,777,214
B	128-191	w.x	y.z	16,384	65,534
C	192-223	w.x.y	z	2,097,151	254

Subnet Masks

Subnet masks are 32-bit numbers that allow nodes to determine the network ID from the Host ID. Subnet masks are determined by assigning 1's to bits that belong to the network ID and 0's to the bits that belong to the host ID. The result is normally displayed in dotted decimal notation. Table 4-2 displays the default subnet masks for the three Internet classes.

Table 4-2 Default subnet masks

Class	Default subnet mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

NOTE: All devices on a physical network should use the same subnet mask and network ID.

Default Gateway

If a destination IP address is not on the local physical network (the address does not match the subnet mask), the host must send the message to a gateway IP router. This router will know where to send the message on the other network so that it will eventually reach the destination. Typically each local network will only have one (default) gateway.

Port Number

Modbus TCP/IP uses the "well known" port number of 502 decimal and is fixed to this value.

Modbus TCP/IP Protocol Mode

The Modbus/TCP Protocol is enabled by setting the Protocol Mode of the Ethernet Port from SY/MAX 802 to Modbus/TCP or MBTCP+SY/MAX. The Modbus TCP protocol mode is compatible with the Modicon TSX Quantum NOE 211 TCP/IP Ethernet module, Modsoft 4.0 or later, Concept programming software, and many third party HMI packages. Each Modbus TCP node on the IP network must have a unique IP address.

Client/Server

TCP/IP implementations are of the Client/Server nature. A Server waits for connection requests from Clients; i.e. the Client is the node that initiates the connection to the Server. The CNOE-800 can be both a Client and a Server at the same time.

When the CNOE-800 routes a command from the PLC to the Ethernet port, it becomes a Client and a TCP/IP connection is formed between the Client and the target Server. The target Server is determined through the use of the implied registers in the MSTR block. The message command is translated into the Modbus TCP protocol and sent out the Ethernet port, with the Destination Index set by the third implied register in the MSTR block.

When the CNOE-800 forms a connection as a Server and receives a command from the Client, it translates the Modbus TCP message into SY/MAX (or Modbus...), and routes it either to the PLC, or can be routed back out the Ethernet port to another Ethernet device via Modbus/TCP or SY/MAX 802.3. The reply is in-turn translated into Modbus TCP and sent back to the Client.

Client IP Look-up Table

If translating messages from SY/MAX 802.3 to Modbus/TCP, the CNOE-800 must be given a route that points the message out to the appropriate Ethernet device. The CNOE-800 inspects the drop in the route following the E-net drop number for an entry in its IP look-up table. If there is an entry in the table, the command is translated into Modbus TCP and sent to the appropriate Server, otherwise, an error reply is sent to the source of the command. If the optional downstream route is included in the IP table entry, only the last drop in the route is inserted in the command as the index value.

```

C:\WINNT\System32\cmd.exe - rpc
RPC ROUTING PROTOCOL CONVERTER
Niobrara R&D CRPCTCP 14JAN2003 Port 0 31Jan2003
CONFIGURATION AND UTILITY SOFTWARE
oNline o fline utility Setup quit
Edit Drop to TCP/IP Routing Table
DROP IP ADDRESS DOWNSTREAM ROUTE
0 0.0.0.0 NONE
1 0.0.0.0 NONE
2 0.0.0.0 NONE
3 0.0.0.0 NONE
4 0.0.0.0 NONE
5 0.0.0.0 NONE
6 0.0.0.0 NONE
7 0.0.0.0 NONE
8 0.0.0.0 NONE
9 0.0.0.0 NONE
10 0.0.0.0 NONE
11 0.0.0.0 NONE
12 0.0.0.0 NONE
13 0.0.0.0 NONE
14 0.0.0.0 NONE
15 0.0.0.0 NONE

```

Figure 4-1 RPCSW32 TCP Routing Table

Figure 4-1 provides a view of a portion of this routing table from the RPCSW32edit TCP screen for the CNOE-800.

Server Index Look-up Table

The Modbus TCP/IP protocol only includes one drop of routing information in the message structure, this drop number is called the *Destination Index*. The CNOE-800 inspects this index on all incoming Modbus TCP/IP messages and if there is an entry in its look-up table, uses the route in the table for the downstream route. (This is just like the Modbus Slave Table for each of the serial ports.) The ability to communicate with the Compact processor is subject to this table. One of the entries in this table must include a route that is the drop number of the backplane "port." The other 254 entries may be used to bridge Modbus/TCP and SY/MAX 802.3 devices.

```

C:\WINNT\System32\cmd.exe - rpc
RPC ROUTING PROTOCOL CONVERTER
Niobrara R&D CRPCTCP 14JAN2003 Port 0 31Jan2003
CONFIGURATION AND UTILITY SOFTWARE
oNline o fline utility Setup quit
MODBUS SERVER ROUTING FOR ETHERNET PORT
INDEX MODBUS ROUTE
0 MODBUS 1
1 OTHER NONE
2 OTHER NONE
3 OTHER NONE
4 OTHER NONE
5 OTHER NONE
6 OTHER NONE
7 OTHER NONE
8 OTHER NONE
9 OTHER NONE
10 OTHER NONE
11 OTHER NONE
12 OTHER NONE
13 OTHER NONE
14 OTHER NONE
15 OTHER NONE
Type digits to enter route. F4 to edit start address.
Use + and - to select port. Escape to exit.

```

Figure 4-2 RPCSW32 Modbus Server Routing Table

Figure 4-2 provides a view of a portion of this routing table from the RPCSW32edit Modbus Routing screen.

Modbus TCP/IP Example

In this example, the CNOE-800 has an IP address of 199.186.195.22, and a Subnet Mask of 255.255.255.0. It is connected to an Ethernet network through a hub with two Quantum NOx-xxx Ethernet modules and a personal computer running Modsoft. The CNOE-800 will be configured for both Client and Server operation to allow the personal computer to program any of the PLCs as well as allowing any PLC to access data in any other PLC using the MSTR programming block.

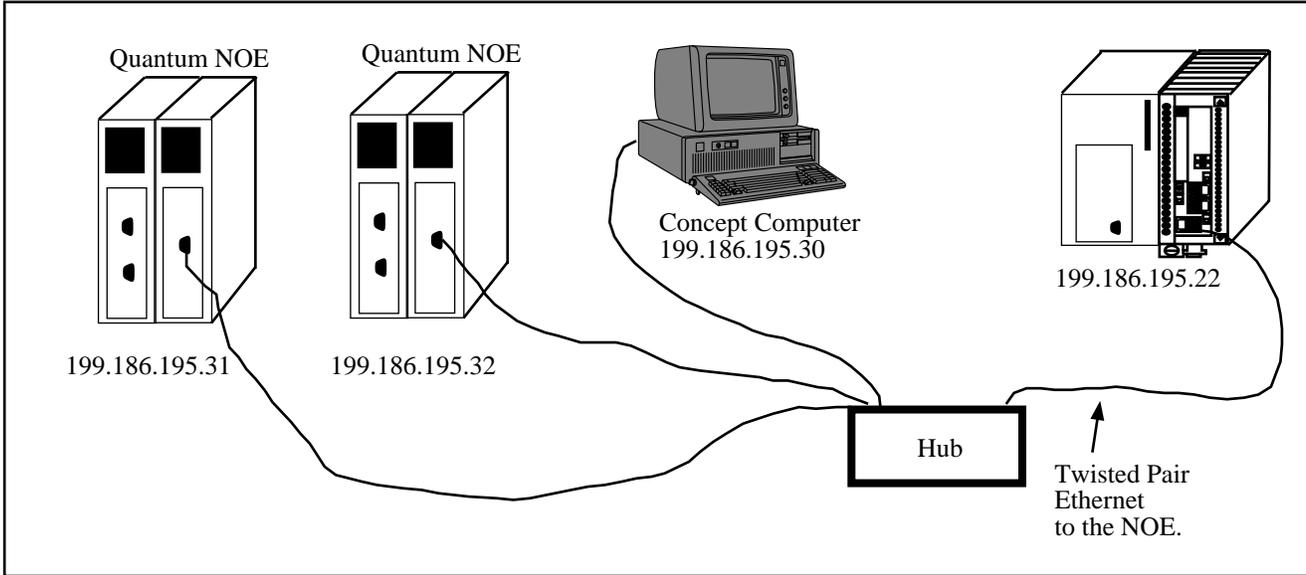
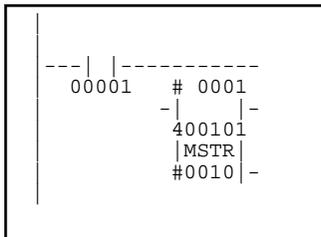


Figure 4-3 Modbus TCP/IP Example

The Ethernet port of the CNOE-800 is connected to a hub along with two Compact TCP/IP Ethernet modules (NOx-xxx). Each NOE has its own IP address, subnet mask, and default gateway as defined in the Compact PLC setup. There is also a personal computer running Modsoft with a TCP/IP stack and its IP address is 199.186.195.30.

Client Operation

For the CNOE-800 to act as a client, the user simply programs MSTR blocks to point at the Quantums on the network. The MSTR will be programmed as below.



Register	Value	Description
400101	2	Opcode
400102	0	Error Status
400103	10	Number of registers
400104	1	Remote Address
400105	x0300	High byte = slot number
400106	199	IP byte 1
400108	186	IP byte 2
400109	195	IP byte 3
400110	31	IP byte 4

Table 4-3 Modbus/TCP MSTR Example

Server Operation

The CNOE-800 may also act as a Modbus TCP/IP Server to allow the Quantums with NOEs and the Modsoft computer with TCP/IP to access the Compact on its Ethernet port. The CNOE-800 uses a 256 entry look-up table to map the Destination Index of the incoming messages to downstream routes. Table 4-4 displays the Modbus Server routing for the CNOE-800 in this example. Destination Index 0 will point to the Compact. This is the default configuration in the CNOE-800. If the backplane drop number is altered, index 0's route must also be altered to match.

Table 4-4 Modbus Routing for the CNOE-800 E-net port

Destination Index	Route
0	1

Figure 4-4 displays a MSTR block and its associated configuration registers for performing a read of Holding registers 400150 through 400154 in the Compact from one of the Quantums with the NOE in Slot #6 of the Compact Rack.

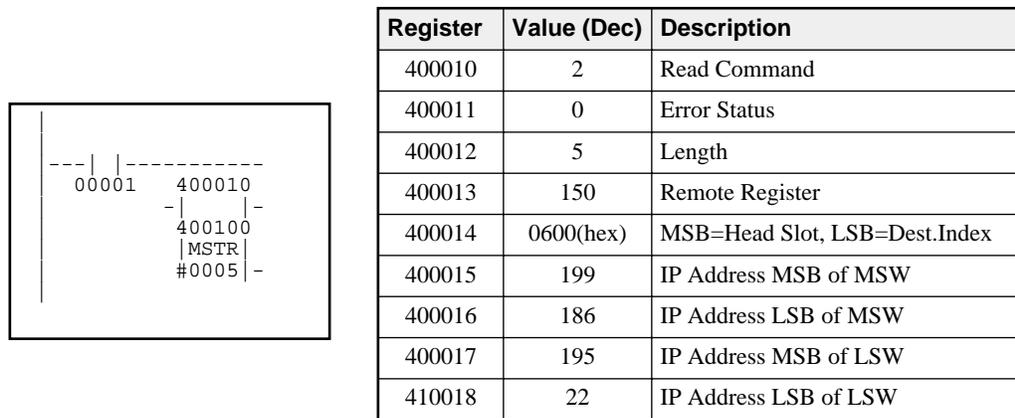


Figure 4-4 TCP/IP Ethernet MSTR Example

Notice that the value in register 400014 is shown in hexadecimal where the upper byte is 06 and the lower byte is 00. The upper byte (MSB) is the slot number of the Compact rack where the NOE is located and in this case slot 6. The lower byte (LSB) is the Destination Index for the outbound TCP/IP message. The value of 00 in the LSB selects Destination Index 00 which points to the downstream route that leads to the Compact. The Destination Index in the Quantum may be any value between 0 and FF hex (0-255) inclusive.

SY/MAX 802.3 Mode

The SY/MAX 802.3 Ethernet protocol is a robust industrial process control communication protocol developed by Square D Company. The CNOE-800 allows a Compact PLC to appear on a SY/MAX 802.3 network. The SY/MAX 802.3 protocol on the 10Mb/s Ethernet allows for high data rates, as the CNOE-800 can process in excess of 26k registers/second. This protocol is defined by the Instruction Bulletin # 30598-775-01A1, SY/MAX 802.3 Communications Protocol and is available only from Square D.

The SY/MAX 802.3 protocol is implemented in a variety of devices including Square D Model 450 and Model 650 PLCs, Square D software SFW390/391 for DEC VAX/VMS computers, Square D SFI610 Ethernet driver for personal computers, Niobrara EPE5, MEB, CNOE-800, and others.

The SY/MAX 802.3 protocol is primarily intended for closed industrial control networks although it will co-exist with other Ethernet protocols such as TCP/IP, DECnet, and Novel on the same physical network. Many production facilities will install an independent Ethernet for process control to provide an additional measure of security. (You don't want someone in Accounting removing a coax terminator and causing the assembly line to come to a screeching halt.)

Because it was developed for industrial control, this protocol has some limitations:

- Only 100 devices may be connected to the same network.
- Although it supports up to 8 drops of SY/MAX routes, the protocol is not Ethernet routeable; it will only pass through multi-protocol bridges and repeaters. Because of this, SY/MAX 802.3 is not suitable for WAN.
- Because it is a proprietary protocol, only a limited number of softwares support it.

When wide area networking is necessary, use the Modbus TCP/IP protocol as described in the next chapter. It uses the TCP/IP protocol and may be routed across IP only routers. Modbus/TCP is openly published and is available on the Internet at <http://www.modbus.org>.

NOTE: The most important thing to remember about SY/MAX 802.3 Ethernet is to set each device to its own unique number between 00 and 99.

MBTCP+SY/MAX Ethernet MODE

The MBTCP+SY/MAX Ethernet mode is a combination of the SY/MAX 802.3 and Modbus TCP modes to allow the integration of remote SY/MAX 802.3 and Modbus TCP devices on the same Ethernet network. As a server only, the CNOE-800 will act exactly as it does in each mode separately. As a client, the CNOE-800 inspects the drop in the route following the drop number of the Ethernet port for an entry in the IP lookup table. If there is an entry in the table, the CNOE-800 translates the command to Modbus TCP, and sends it to the appropriate server. If there is no entry in the table, the command is translated to SY/MAX 802.3, and routed to the appropriate device.

MBTCP+SY/MAX Example

In this example, the CNOE-800's E-net port has a Drop number of 20 with an IP address of 206.223.51.147, Subnet Mask of 255.255.255.0, and a Default Gateway of 206.223.51.1.

An EPE5-D is on the same local network. Its E-net port has a drop number of 26. Port 3 is in SY/MAX mode with a drop number of 103. A Model 400 PLC is connected to this port.

A Model 450 is connected to the same local network as the EPE5-TCP. Its Ethernet's drop number is 24.

A Model 650 is also connected to the local network. Its Ethernet's drop number is 22.

A Modicon Quantum NOE and Processor are connected to the same local network. The NOE's IP address is 206.223.51.148.

An ECM2000 is also connected to the same local network. Its IP address is 206.223.51.156. Attached to the ECM's serial port are two Powerlogic CM's. Their addresses are 2 and 1, respectively.

Since the CNOE-800 can be a client in this example, we need to configure its TCP table. So by setting the CNOE-800's entries 22 through 26, we can use the rest of the route of the incoming message to reach the downstream devices.

Table 6-1 CNOE-800 IP Table Example

Drop	IP Address	Route
22	0.0.0.0	NONE
23	206.223.51.148	NONE
24	0.0.0.0	NONE
25	206.223.51.156	NONE
26	0.0.0.0	NONE

Table 6-2 Server Index Table For CNOE-800

Drop	TYPE	Route
1	OTHER	20,22
2	OTHER	20,24
3	OTHER	20,26,103

The routes required to be set in the Model 450 to reach the target devices are shown in Table 6-3.

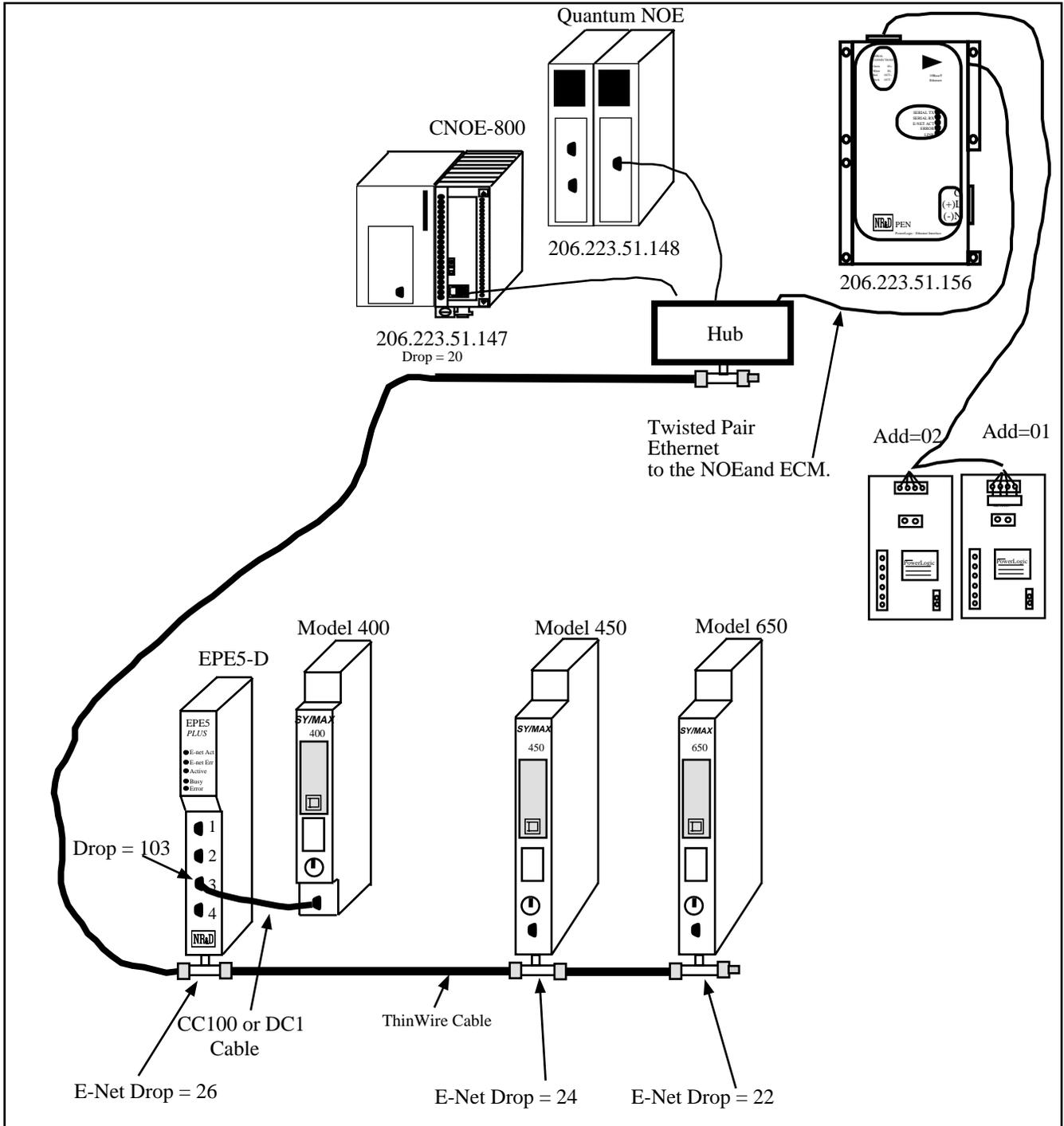
Table 6-3 Model 450 Routing Examples

Target	Route
CNOE-800	24,20
CM #1 on ECM2000	24,20,20,25,1
CM #2 on ECM2000	24,20,20,25,2
EPE5-D	24,26
Model 400	24,26,103
NOE	24,20,20,23,0
Model 650	24,22

Table 6-4 NOE Routing Examples

Target	IP Address	Index
Model 450	206.223.51.147	2
Model 650	206.223.51.147	1
Model 400	206.223.51.147	3
Compact PLC	206.223.51.147	0
Circuit Monitor #1	206.223.51.156	1

Figure 6-1 MBTCP+SY/MAX Routing Example



The first drop in the Model 450's route is always 24, since that is its own Ethernet port. If a Modbus TCP message is desired, the second drop in the route must always be 20, the drop number of the CNOE-800's Ethernet port. In this case the third drop in the route will also be 20, indicating a route back out of the CNOE-800's Ethernet port. The fourth drop in the route will point to the IP table of the CNOE-800. If the corresponding index in the IP table contains an IP address, the message will be translated to Modbus TCP, and sent to the device with that IP address. The last drop in the route will be an index that the target device uses for further routing.

If it is desirable for the NOE to access SY/MAX 802.3 devices on the network, it can simply connect to the CNOE-800, and use the index in the Modbus Routing table to route to the proper device. For exam-

ple, if the NOE needs to access the Model 650, it connects to 206.223.51.147, and uses index 1. Index 1 in the Modbus routing table is a route of 20,22, causing the message to route back out the E-net port using SY/MAX 802.3 to device 22. If the NOE needs to access the Model 450 or the Model 400, it accesses the same IP address, then uses index 2 or 3, respectively. Note that entries 22,24, and 26 in the TCP table of the CNOE-800 must be 0.0.0.0 for the outbound message to be SY/MAX 802.3.

MSTR Operation

The MSTR Instruction

The MSTR instruction allows the Compact PLC to read or write registers in other devices connected to any port on the CNOE-800. The following table lists the opcodes available for use in the CNOE-800.

Table 7-1 Supported MSTR Opcodes

MSTR Operation	MSTR Opcode (Decimal)	Actual Modbus Opcode (Decimal)
Write 4x registers	1	16
Read 4x registers	2	3
Write 0x coils	101	15
Read 0x coils	102	1
Read 1x discretetes	103	2
Read 3x registers	106	4
Write 4x single register	108	6
Write 0x single coil	109	5
Read option module port configuration	111	N/A
Write option module port configuration	112	N/A
Reset option module to factory defaults	512	N/A
Set option module IP address	513	N/A
Set option module subnet mask	516	N/A
Set option module default gate	517	N/A

NOTE: This list may grow as new developments are made. Check the latest version of this manual at <http://www.niobrara.com>.

NOTE: The MSTR Opcodes above 100 are Niobrara Module specific and may not be directly supported by Modicon Programming Software such as Concept or Proworks. It may be necessary to edit the MSTR configuration registers with a data viewer if the programming package complains that the opcode is not supported.

NOTE: A maximum of four MSTR instructions can be active at any given time. More than four may be set active by the ladder logic, but only the first four will execute. As MSTR blocks release the resources of the option, the next MSTR's will use those resources, and execute. It should be noted that the "Active" output from the MSTR block will not turn on until the associated MSTR begins to execute.

MSTR Diagram

Below is a diagram of the MSTR block. It has two inputs and three outputs.

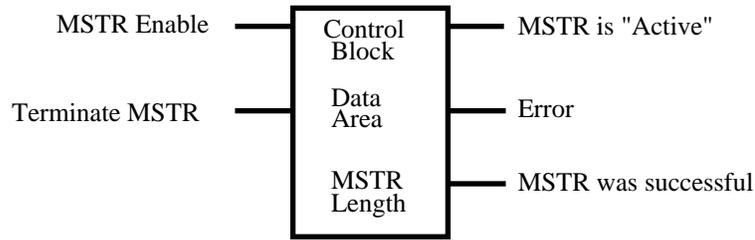


Figure 7-1 MSTR Block Diagram

Inputs

The MSTR block has two inputs: **Enable** and **Terminate**.

Enable activates the MSTR and it must remain latched on until either the **Error** output or **MSTR was successful** output become true. If the **Enable** is turned off before the MSTR is completed then the reply data will be discarded by the CNOE.

Terminate will deactivate the MSTR before a completion or error.

Outputs

The MSTR block has three possible outputs: **Active**, **Error**, and **Success**.

Active will be high while the MSTR is activated. If it is the fifth or higher in a string of five or more MSTR's, this will not be high until a preceding MSTR releases the resources required by receiving a response or terminating in an error.

Error will go high if the MSTR is terminated, or if an error occurs during the operation. The corresponding error code will be placed in the first implied register of the MSTR control block by the CNOE.

Success will go high when the MSTR completes successfully.

Control Block Content

The 4x register assigned in the top node of the MSTR block will be the starting register for the control block of the the MSTR. The control block structure differs according to the network(in this case TCP/IP) and opcode being used. The control block structures for the different opcodes are as follows:

Table 7-2 Supported MSTR Opcodes

Register	Opcode 512	Opcodes 1,2 and 101-109 Modbus/TCP	Opcodes 1,2 and 101-109 SY/MAX 802.3 and Serial Ports	Opcodes 513,516,517	Opcodes 111,112
Displayed	Opcode	Opcode	Opcode	Opcode	Opcode
First implied	Error Status	Error Status	Error Status	Error Status	Error Status
Second implied	Unused	Number of points transferred	Number of points transferred	Unused	Unused
Third implied	Unused	Remote Address	Remote Address	Unused	Unused
Fourth implied	High byte = Option Slot # Low byte = Unused	High byte = Option Slot # Low byte = Destination Index	High byte = Option Slot # Low byte = Unused	High byte = Option Slot # Low byte = Unused	High byte = Option Slot # Low byte = Unused
Fifth implied	Unused	High byte = Must be 0 Low byte = IP byte 1	High byte = Length of Route Low byte = Route 1	High byte = Unused Low byte = IP byte 1	Port # 0 = Ethernet 1 = Serial Port 1 2 = Serial Port 2 3 = Backplane
Sixth implied	Unused	High byte = Must be 0 Low byte = IP byte 2	High byte = Route 2 Low byte = Route 3	High byte = Unused Low byte = IP byte 2	Unused
Seventh implied	Unused	High byte = Must be 0 Low byte = IP byte 3	High byte = Route 4 Low byte = Route 5	High byte = Unused Low byte = IP byte 3	Unused
Eighth implied	Unused	High byte = Must be 0 Low byte = IP byte 4	High byte = Route 6 Low byte = Unused	High byte = Unused Low byte = IP byte 4	Unused

Middle Node Content

The 4x register entered in the middle node of the MSTR block is the first register in a group of consecutive registers that make up the data area. If the MSTR Opcode is a READ opcode, these registers will be the destination for the data. If the Opcode is a WRITE opcode, these registers will be the source for the data.

Bottom Node Content

This is an integer value that specifies the length of the data area specified in the middle node. This must be a value in the range 1...100.

Control Block Operation

The following examples use this MSTR block with the Control Block starting at 40100, the Data Block at 40055, and a maximum count of 20 words. The MSTR is activated when 000010 goes high. The MSTR's top output activates 000001, which latches the MSTR on until it is broken by either the MSTR's error output or its "successful" output. This prevents the MSTR from losing the reply coming from the downstream device.

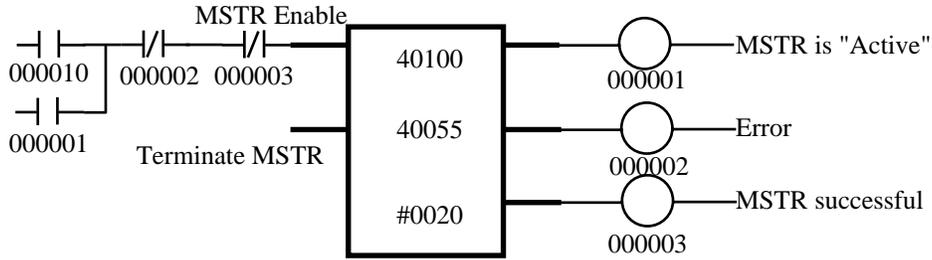


Figure 7-2 Sample MSTR

Opcode 1 (Write Multiple 4x Registers)

MSTR Opcode 1 generates a Modbus opcode 16 multiple register write to the target 4x registers. The data will come from the PLC 4x registers designated by the middle node of the MSTR. The target 4x registers are determined by the third implied register in the control block. The second implied register gives the number of registers transferred by the write.

Table 7-3 shows the Control Block Registers for a CNOE-800 in PLC Slot 3 writing the values from PLC registers 40055 through 40059 to a Modbus/TCP device at IP Address 192.168.0.44, Modbus/TCP Index 1, and remote registers 40245 through 40249.

Table 7-3 Opcode 1 to Modbus/TCP Target

PLC Control Block Register	Value (Decimal)	Value (Hex)	Description
40100	1	0001	MSTR Opcode 1, 4x Write
40101	N/A	N/A	Error Status
40102	5	0005	Number of registers written
40103	245	00F5	Remote 4x register
40104	769	0301	High byte = Slot 3, Low byte = Target Index = 1
40105	192	00C0	Target IP Address
40106	168	00A8	Target IP Address
40107	0	0000	Target IP Address
40108	44	002C	Target IP Address

Table 7-4 gives the correlation of PLC registers to the remote 3x register after the read is completed.

Table 7-4 Register Correlation

PLC Register	Remote Register
40055	40245
40056	40246
40057	40247
40058	40248

Opcode 2 (Read 4x Registers)

MSTR Opcode 2 generates a Modbus opcode 3 multiple register read from the target 4x registers. The data will show up in the PLC 4x registers designated by the middle node of the MSTR. The target 4x registers are determined by the third implied register in the control block. The second implied register gives the number of registers transferred by the read.

Table 7-5 shows the Control Block Registers for a CNOE-800 in PLC Slot 4 reading the values from a Modbus serial device on CNOE port 1 drop 101, Modbus target slave address 29, and remote registers 41001 through 41015.

Table 7-5 Opcode 2 Read from Modbus Serial Target on Port 1

PLC Control Block Register	Value (Decimal)	Value (Hex)	Description
40100	2	0002	MSTR Opcode 2, 4x Read
40101	N/A	N/A	Error Status
40102	16	0010	Number of registers read
40103	1001	03E9	Remote 4x register
40104	1024	0400	High byte = Slot 4, Low byte = not used
40105	613	0265	High byte = Number of drops in route = 2, Low byte = First drop in route = 101
40106	7424	1D00	High byte = Second drop in route = 29 Low byte = Thrid drop in route =Not used
40107	0	0000	High byte = Fourth drop in route = Not Used Low byte = Fifth drop in route =Not used
40108	0	000	High byte = Sixth drop in route = Not Used Low byte = Seventh drop in route =Not used

Table 7-6 gives the Correlation of PLC registers to the remote 3x register after the read is completed.

Table 7-6 Register Correlation

PLC Register	Remote Register
40055	41001
40056	41002
40057	41003
40058	41004
40059	41005
40060	41006
40061	41007
40062	41008
40063	41009
40064	41010
40065	41011
40066	41012
40067	41013
40068	41014
40069	41015
40070	41016

Opcode 101 (Write Multiple 0x Coils)

MSTR Opcode 101 generates a Modbus opcode 15 multiple coil write to the target 0x coils. The data will come from the PLC 4x registers designated by the middle node of the MSTR. The Most Significant Bit of the middle node register is the starting coil for the write data. The target 0x coils are determined by the third implied register in the control block. The second implied register gives the number of coils transferred by the write.

Table 7-3 shows the Control Block Registers for a CNOE-800 in PLC Slot 3 writing the 18 bit values from PLC registers 40055 and 40056 to a Modbus/TCP device at IP Address 192.168.0.44, Modbus/TCP Index 10, and remote coils 00112 through 00127.

Table 7-7 Opcode 101 to Modbus/TCP Target

PLC Control Block Register	Value (Decimal)	Value (Hex)	Description
40100	101	0065	MSTR Opcode 101, 0x Write
40101	N/A	N/A	Error Status
40102	18	0012	Number of coils written
40103	112	0070	Remote 0x starting coil 00112
40104	778	030A	High byte = Slot 3, Low byte = Target Index = 10
40105	192	00C0	Target IP Address
40106	168	00A8	Target IP Address
40107	0	0000	Target IP Address
40108	44	002C	Target IP Address

If PLC register 40055 = A164 (hex) = 1010 0001 0110 0100 (binary) and register 40056 = 8000 (hex) = 1000 0000 0000 0000 (binary) then Table 7-8 will show the correlation between the PLC bits and the remote coils.

Table 7-8 Bit Correlation between PLC and Target

PLC Bit	Remote Coil	Value
40055-1	00112	1
40055-2	00113	0
40055-3	00114	1
40055-4	00115	0
40055-5	00116	0
40055-6	00117	0
40055-7	00118	0
40055-8	00119	1
40055-9	00120	0
40055-10	00121	1
40055-11	00122	1
40055-12	00123	0
40055-13	00124	0
40055-14	00125	1
40055-15	00126	0
40055-16	00127	0
40056-1	00128	1
40056-2	00129	0

Opcode 102 (Read 0x Coils)

MSTR Opcode 102 generates a Modbus opcode 1 multiple coil read from the target 0x coils. The data will show up in the PLC 4x registers designated by the middle node of the MSTR. The target 0x coils are determined by the third implied register in the control block. The second implied register gives the number of coils transferred by the read.

Table 7-9 shows the Control Block Registers for a CNOE-800 in PLC Slot 4 reading the values from a Modbus serial device on CNOE port 1 drop 2, Modbus target slave address 104, and remote coils 00006 through 00009.

Table 7-9 Opcode 102 Read from Modbus Serial Target on Port 1

PLC Control Block Register	Value (Decimal)	Value (Hex)	Description
40100	102	0066	MSTR Opcode 102, 0x Read
40101	N/A	N/A	Error Status
40102	4	0004	Number of coils to read
40103	6	0006	Remote 0x starting coil
40104	1024	0400	High byte = Slot 4, Low byte = not used
40105	514	0202	High byte = Number of drops in route = 2, Low byte = First drop in route = 2
40106	26624	6800	High byte = Second drop in route = 104 Low byte = Thrid drop in route =Not used
40107	0	0000	High byte = Fourth drop in route = Not Used Low byte = Fifth drop in route =Not used
40108	0	000	High byte = Sixth drop in route = Not Used Low byte = Seventh drop in route =Not used

If the remote slave has coils 6, 7, and 9 ON but Coil 8 OFF then PLC

Register 40055 = D000 (hex) = 1101 0000 0000 0000 (binary)

and Table 7-10 will show the correlation between the PLC bits and the remote coils.

Table 7-10 Bit Correlation between PLC and Target

PLC Bit	Remote Coil	Value
40055-1	00006	1
40055-2	00007	1
40055-3	00008	0
40055-4	00009	1
40055-5	N/A	0
40055-6	N/A	0
40055-7	N/A	0
40055-8	N/A	0
40055-9	N/A	0
40055-10	N/A	0
40055-11	N/A	0
40055-12	N/A	0
40055-13	N/A	0
40055-14	N/A	0
40055-15	N/A	0
40055-16	N/A	0

Opcode 103 (Read 1x Coils)

MSTR Opcode 103 generates a Modbus opcode 2 multiple input bit read from the target 1x bits. The data will show up in the PLC 4x registers designated by the middle node of the MSTR. The target 0x coils are determined by the third implied register in the control block. The second implied register gives the number of coils transferred by the read.

Table 7-11 shows the Control Block Registers for a CNOE-800 in PLC Slot 3 reading the values from a Modbus/TCP device on a Modbus/TCP <> Modbus Serial Bridge at IP Address of 10.100.2.123, Modbus target slave address 12, and remote input bits 10223 through 10248.

Table 7-11 Opcode 103 Read from Modbus/TCP Target

PLC Control Block Register	Value (Decimal)	Value (Hex)	Description
40100	103	0067	MSTR Opcode 103, 1x Read
40101	N/A	N/A	Error Status
40102	25	0019	Number of input bits to read
40103	223	00DF	Remote 1x starting bit
40104	780	030C	High byte = Slot 3, Low byte = Target Index = 12
40105	10	000A	Target IP Address
40106	100	0064	Target IP Address
40107	2	0002	Target IP Address
40108	123	007B	Target IP Address

If the remote slave has bits 10126, 10129, 10133, 10134, 10236, 10240, 10242, 10244, 10245, and 10248 ON and the rest OFF then PLC registers

Register 40055 = 1234 (hex) = 0001 0010 0011 0100 (binary)

Register 40056 = 5640 (hex) = 0101 0110 0100 0000 (binary)

and Table 7-12 will show the correlation between the PLC bits and the remote inputs.

Table 7-12 Bit Correlation between PLC and Target

PLC Bit	Remote Coil	Value
40055-1	10223	0
40055-2	10224	0
40055-3	10225	0
40055-4	10226	1
40055-5	10227	0
40055-6	10228	0
40055-7	10229	1
40055-8	10230	0
40055-9	10231	0
40055-10	10232	0
40055-11	10233	1
40055-12	10234	1
40055-13	10235	0
40055-14	10236	1
40055-15	10237	0
40055-16	10238	0
40056-1	10239	0
40056-2	10240	1
40056-3	10241	0
40056-4	10242	1
40056-5	10243	0
40056-6	10244	1
40056-7	10245	1
40056-8	10246	0
40056-9	10247	0
40056-10	10248	1
40056-11	N/A	0
40056-12	N/A	0
40056-13	N/A	0
40056-14	N/A	0
40056-15	N/A	0
40056-16	N/A	0

Opcode 106 (Read 3x Registers)

MSTR Opcode 106 generates a Modbus opcode 4 multiple input register read from the target 3x registers. The data will show up in the PLC 4x registers designated by the middle node of the MSTR. The target 3x registers are determined by the third implied register in the control block. The second implied register gives the number of registers transferred by the read.

Table 7-13 shows the Control Block Registers for a CNOE-800 in PLC Slot 4 reading the values from a Modbus/TCP Ethernet device at IP Address 206.223.51.169, Modbus target slave address 1, and remote registers 30005 through 30008.

Table 7-13 Opcode 106 Read from Modbus/TCP Target

PLC Control Block Register	Value (Decimal)	Value (Hex)	Description
40100	106	006A	MSTR Opcode 106, 3x Read
40101	N/A	N/A	Error Status
40102	4	0004	Number of registers read
40103	5	0005	Remote starting 3x register
40104	1025	0401	High byte = Slot 4, Low byte = Target Index = 1
40105	206	00CE	Target IP Address
40106	223	00DF	Target IP Address
40107	51	0033	Target IP Address
40108	169	00A9	Target IP Address

Table 7-14 gives the correlation of PLC registers to the remote 3x register after the read is completed.

Table 7-14 Register Correlation

PLC Register	Remote Register
40055	30005
40056	30006
40057	30007
40058	30008

Opcode 108 (Write 4x Single Register)

MSTR Opcode 108 generates a Modbus opcode 6 single register write to the target 4x register. The data will come from the PLC 4x register designated by the middle node of the MSTR. The target 4x register is determined by the third implied register in the control block. The second implied register will not be used, as this is always a single register write.

Table 7-3 shows the Control Block Registers for a CNOE-800 in PLC Slot 3 writing the value from PLC register 40235 to a Modbus serial device on CNOE port 2 drop 14, Modbus target slave address 23, and remote register 40001.

Table 7-15 Opcode 108 Write to Modbus Serial Target on Port 2

PLC Control Block Register	Value (Decimal)	Value (Hex)	Description
40100	108	006C	MSTR Opcode 102, 0x Read
40101	N/A	N/A	Error Status
40102	N/A	N/A	Number of Registers to Write (Always 1)
40103	1	0001	Remote 4x Register to Write
40104	768	0300	High byte = Slot 3, Low byte = not used
40105	526	020E	High byte = Number of drops in route = 2, Low byte = First drop in route = 14
40106	5888	1700	High byte = Second drop in route = 104 Low byte = Thrid drop in route =Not used
40107	0	0000	High byte = Fourth drop in route = Not Used Low byte = Fifth drop in route =Not used
40108	0	000	High byte = Sixth drop in route = Not Used Low byte = Seventh drop in route =Not used

Table 7-16 Register Correlation

PLC Register	Remote Register
40055	40001

Opcode 109 (Write 0x Single Coil)

MSTR Opcode 109 generates a Modbus opcode 5 single coil write to the target 0x coil. The data will come from the PLC 4x register designated by the middle node of the MSTR. The Most Significant Bit of the middle node register is bit number one for the write data. The second implied register in the control block gives the bit number to be transferred by the write. The target 0x coil is determined by the third implied register in the control block.

Table 7-17 shows the Control Block Registers for a CNOE-800 in PLC Slot 3 writing the bit value from PLC register 40055 bit 3 to a Modbus/TCP device at IP Address 192.168.0.44, Modbus/TCP Index 10, and remote coil 00112.

Table 7-17 Opcode 109 to Modbus/TCP Target

PLC Control Block Register	Value (Decimal)	Value (Hex)	Description
40100	109	006D	MSTR Opcode 109, Single 0x Write
40101	N/A	N/A	Error Status
40102	3	0003	Number of bit in 40055 to be used
40103	112	0070	Remote 0x coil 00112
40104	778	030A	High byte = Slot 3, Low byte = Target Index = 10
40105	192	00C0	Target IP Address
40106	168	00A8	Target IP Address
40107	0	0000	Target IP Address
40108	44	002C	Target IP Address

If PLC register 40055 = A164 (hex) = 1010 0001 0110 0100 (binary) then Table 7-18 will show the correlation between the PLC bit and the remote coil.

Table 7-18 Bit Correlation between PLC and Target

PLC Bit	Remote Coil	Value
40055-3	00112	1

Opcodes 111 & 112 (Read/Write Option Module Port Configuration)

MSTR Opcode 111 generates a backplane register read from the target option module. The data will show up in the PLC 4x registers designated by the middle node of the MSTR.

MSTR Opcode 112 generates a backplane register write to the target option module. The data will come from the PLC 4x registers designated by the middle node of the MSTR.

The target option module registers are determined by the fifth implied register in the control block.

To avoid writing unwanted data to a port, the user should always perform a read of the desired port, change only the relevant registers, then write the data back to the module.

Table 7-19 shows the Control Block Registers for reading or writing the settings for a port in a CNOE-800 in PLC Slot 4.

Table 7-19 Opcodes 111 & 112 Read/Write Option Module Port Configuration

PLC Control Block Register	Value (Decimal)	Value (Hex)	Description
40100	111 112	006F 0070	MSTR Opcode 111, Option Module Port Configuration Read MSTR Opcode 112, Option Module Port Configuration Write
40101	N/A	N/A	Error Status
40102	N/A	N/A	Not Used
40103	N/A	N/A	Not Used
40104	1024	0400	High byte = Slot 4, Low byte = Not Used
40105	1	0001	Read Serial Port 1
40106	N/A	N/A	Not Used
40107	N/A	N/A	Not Used
40108	N/A	N/A	Not Used

Table 7-20 is a list of the 32 registers that control the operation of the Ethernet port.

Table 7-20 Ethernet Port Control Registers

Port 0	Legal Values	Function
8003	0..99	Ethernet SY/MAX drop number.
8004...8007		Reserved for future use. Do not modify.
8008	2, 260, 272	Protocol Mode 2 = SY/MAX 802.3, 260 = Modbus/TCP, 272 = MBTCP+SY/MAX
8009...8024		Reserved. Do not modify.
8025	1..64	Buffer Limit
8026...8029		Reserved. Do not modify.
8030		Options (See Table 26-23 on Page 196)
8031...8034		Reserved for future use, do not modify

Table 7-21 is a list of the 32 registers that control the operation of the serial ports.

Table 7-21 Ports 1 and 2 Configuration Registers

Port 1	Port 2	Legal Values	Function
8035	8067	0..199	Drop Number
8036	8068	0..14	Baud Rate (See Table 26-17 on Page 193)
8037	8069	0,1	Data Bits (See Table 26-18 on Page 194)
8038	8070	0,1,2	Parity Bits (See Table 26-19 on Page 194)
8039	8071	0,1	Stop Bits (See Table 26-20 on Page 194)
8040	8072	1..19	Protocol Mode (See Table 26-21 on Page 194)
8041	8073	0..256	Packet size limit (Modes 4, 5, and 8)
		1..8192	Auto-transfer Read Source Register (Peripheral)
		0..65535	RNIM Identification Number
8042	8074	0..32767	Time limit (Modes 4, 5, and 8)
		0..32767	MODBUS Host mode retry timeout
		0..65535	RNIM CTS Delay
8043	8075	0..32767	Multidrop window interval
		0..32767	Auto-transfer Interval
		0..65535	RNIM Message Response Timeout
8044	8076	0..200	Priority in Multidrop mode
		1..2048	Auto-transfer Read Destination Register (Mailbox)
		0..65535	RNIM BID Address
8045	8077	0..200	Number of nodes in Multidrop mode
		1..2048	Auto-transfer Write Source Register (Mailbox)
		0..65535	RNIM Number of Retries
8046	8078	0..8	Number of drops in target route (Modes 4,5,8 and Auto-transfer)
8047	8079	0..255	Target Route Drop 1 (Modes 4,5,8 and Auto-transfer)
8048	8080	0..255	Target Route Drop 2 (Modes 4,5,8, and Auto-transfer)
8049	8081	0..255	Target Route Drop 3 (Modes 4,5,8, and Auto-transfer)
8050	8082	0..255	Target Route Drop 4 (Modes 4,5,8, and Auto-transfer)
8051	8083	0..255	Target Route Drop 5 (Modes 4,5,8, and Auto-transfer)
8052	8084	0..255	Target Route Drop 6 (Modes 4,5,8, and Auto-transfer)
8053	8085	0..255	Target Route Drop 7 (Modes 4,5,8, and Auto-transfer)
8054	8086	0..255	Target Route Drop 8 (Modes 4,5,8, and Auto-transfer)
8055	8087	1,2,3,4	MODBUS Host equivalent READ command
8056	8088	5,6,15,16	MODBUS Host equivalent WRITE command
8057	8089	1..32	Buffer Limit

Table 7-22 Ports 1 and 2 Configuration Registers (Continued)

Port 1	Port 2	Legal Values	Function
8058	8090	0..128	Auto-transfer Read Count
		0..65535	RNIM Pause Time
8059	8091	0..128	Auto-transfer Write Count
		0..65535	RNIM Message Count
8060	8092	1..8192	Auto-transfer Write Destination register (Peripheral)
		0..65535	RNIM BID Reply Interval
8061	8093	0..65535	MODBUS Host Offset (Register Bias)
8062	8094		Options (See Table 26-23 on Page 196)
8063	8095	0..127	Modbus Slave Starting Address
8064	8096	0..65525	PAD Count in SY/MAX, N-T-N or CTS Delay in 10mS units for Modbus
8065	8097	0..65535	Modbus RTU inter-character timing in mS. (default is 4 characters)
8066	8098		Reserved for future use, do not modify

Table 7-23 is a list of the 32 registers that control the operation of the backplane port.

Table 7-23 Backplane Port Configuration Registers

Register	Legal Values	Function
8099	0..199	Drop Number
8100...8104		Reserved for future use. Do not modify.
8105	1...32	Span of I/O scan entries per socket.
8106	0...65535	MSTR reply timeout in 1/100ths of a second.
8107...8120		Reserved for future use. Do not modify.
8121	0...65535	Programming channel idle timeout in minutes.
8122...8125		Reserved for future use. Do not modify.
8126		Options (See Table 26-23 on Page 196)
8127...8130		Reserved for future use. Do not modify.

Opcode 512 (Reset Option Module to Factory Defaults)

MSTR Opcode 512 generates a backplane register write to the target option module's command register. The target option module will reset all settings to factory default.

Table 7-24 shows the Control Block Registers for resetting a CNOE-800 in PLC Slot 4.

Table 7-24 Opcode 512 Reset Option Module to Factory Defaults

PLC Control Block Register	Value (Decimal)	Value (Hex)	Description
40100	512	0200	MSTR Opcode 512, Reset Option Module to Factory Defaults
40101	N/A	N/A	Error Status
40102	N/A	N/A	Not Used
40103	N/A	N/A	Not Used
40104	1024	0400	High byte = Slot 4, Low byte = Not Used
40105	N/A	N/A	Not Used
40106	N/A	N/A	Not Used
40107	N/A	N/A	Not Used
40108	N/A	N/A	Not Used

Opcode 513 (Set Option Module IP Address)

MSTR Opcode 513 generates a backplane register write to the target option module to set its IP address. The data will be entered directly into the MSTR control block.

Table 7-25 shows the Control Block Registers for setting a CNOE-800 in PLC Slot 5 with an IP address of 192.168.0.10.

Table 7-25 Opcode 513 Set Option Module IP Address

PLC Control Block Register	Value (Decimal)	Value (Hex)	Description
40100	513	0201	MSTR Opcode 513, Set Option Module IP Address
40101	N/A	N/A	Error Status
40102	N/A	N/A	Not Used
40103	N/A	N/A	Not Used
40104	1280	0500	High byte = Slot 5, Low byte = Not Used
40105	192	00C0	IP Address Byte 1
40106	168	00A8	IP Address Byte 2
40107	0	0000	IP Address Byte 3
40108	10	000A	IP Address Byte 4

Opcode 516 (Set Option Module Subnet Mask)

MSTR Opcode 516 generates a backplane register write to the target option module to set its subnet mask. The data will be entered directly into the MSTR control block.

Table 7-26 shows the Control Block Registers for setting a CNOE-800 in PLC Slot 5 with a subnet mask of 255.255.0.0.

Table 7-26 Opcode 516 Set Option Module Subnet Mask

PLC Control Block Register	Value (Decimal)	Value (Hex)	Description
40100	516	0204	MSTR Opcode 516, Set Option Module Subnet Mask
40101	N/A	N/A	Error Status
40102	N/A	N/A	Not Used
40103	N/A	N/A	Not Used
40104	1280	0500	High byte = Slot 5, Low byte = Not Used
40105	255	00FF	Subnet Mask Byte 1
40106	255	00FF	Subnet Mask Byte 2
40107	0	0000	Subnet Mask Byte 3
40108	0	0000	Subnet Mask Byte 4

Opcode 517 (Set Option Module Default Gate)

MSTR Opcode 517 generates a backplane register write to the target option module to set its default gate. The data will be entered directly into the MSTR control block.

Table 7-27 shows the Control Block Registers for setting a CNOE-800 in PLC Slot 5 with a default gate of 192.168.0.1.

Table 7-27 Opcode 517 Set Option Module Default Gate

PLC Control Block Register	Value (Decimal)	Value (Hex)	Description
40100	516	0204	MSTR Opcode 516, Set Option Module Subnet Mask
40101	N/A	N/A	Error Status
40102	N/A	N/A	Not Used
40103	N/A	N/A	Not Used
40104	1280	0500	High byte = Slot 5, Low byte = Not Used
40105	192	00C0	Default Gate Byte 1
40106	168	00A8	Default Gate Byte 2
40107	0	0000	Default Gate Byte 3
40108	1	0001	Default Gate Byte 4

MSTR Error Codes

Below is a list of error codes returned by the MSTR block. This will appear in the first implied register in the MSTR block.

NOTE: These error codes are only the error codes returned by the CNOE. The PLC itself may also return MSTR error codes. For a list of these, refer to the PLC programming software help section, or to the Modicon Ladder Logic Block Library User Guide (840 USE 101 00).

Table 7-28 MSTR Error Codes

Hex Code	Description
1001	Operation Aborted
2001	Unsupported Opcode
2002	Control Block changed during operation
2004	Invalid port number used with opcode 111,112
2013	Data Block out of PLC memory range
300n	Received Modbus Exception response n
6n40	Bad format in control block, word n
7001	No reply received within reply timeout
7002	Contact Tech. Support
E001	Contact Tech. Support

Ethernet I/O Scanner

Introduction

The CNOE-800's Ethernet I/O scanner allows continual reading and /or writing of data from specified Modbus/TCP slaves without using MSTR resources to do so. The user configures an I/O scan table using RPCSW32. This table specifies information such as the IP address and register address of the data to be accessed. It also specifies the register address of the PLC or the CNOE-800 where the data will be stored.

Configuring the Ethernet I/O Scanner Using RPCSW32

The offline menu of RPCSW32 contains a choice called "edit Ethernet I/O scan table." Once selected, the editing screen for the Ethernet I/O Scanner is available. In this table is a list of 128 possible entries that the CNOE-800 can use to access data on the Ethernet. Each entry consists of an IP address, an ID, a timeout, a scan rate, the addresses of the data to be manipulated, the number of registers to be manipulated, and a selection of what to do with the current data on comms failure. Also within the setup page is the information to configure how the PLC interacts with the Ethernet I/O Scanner.

It would be undesirable to edit an I/O scan entry while the scan was active. Consequently, the I/O Scanner table cannot be edited online. To edit the table, start with an offline Fetch memory from module. This copies the current memory of the module into the memory of the software. Then do an offline edit Ethernet I/O scan table. Make all the desired changes, then do an offline Send memory to module.

NOTE: If the CNOE-800 is configured to be an I/O module, all following discussion of register spaces becomes invalid. When configured as an I/O module, there is only one register space. The first 2048 mailbox registers are used in this situation.

IP Address

This is the IP address of the device or bridge to be polled.

ID

This is the device address or bridge index of the device to be polled. This may also be known as Slave ID or destination index.

Timeout

This value determines the timeout, in milliseconds, before the CNOE-800 expires the operation.

Scan Rate

This value determines how often, in milliseconds, the CNOE-800 will poll the device. If set to zero, the CNOE-800 will poll the device as fast as possible.

Register Space

This column precedes the Master and Slave columns for both Read and Write. Although this column has no heading, it allows the user to choose the register space in the device to be polled. Valid choices are 0x, 1, 3x, and 4x. Default is 4x. Press the space bar to toggle, or press 0, 1, 3, or 4 to select.

Master (Under Read or Write)

This value determines the mailbox register in the PLC or the CNOE-800 that is the starting register for the operation. In the PLC, the valid range is limited by the number of registers assigned to the PLC. For the CNOE-800, the valid range is 1 through 2048. A value of 0 disables the I/O scan entry.

Slave (Under Read or Write)

This value determines the register in the Peripheral device that is the starting register for the operation. The valid range is 1 through 8192. A value of 0 disables the I/O scan entry.

Cnt (Under Read or Write)

The Count field determines the number of consecutive registers (or words if discrettes are used) moved in the operation. The valid range is 0 through 120. A value of 0 disables the Auto-Scan entry.

H/O

This setting is set to HLD or 0, depending on the desired function. If set to HLD, the CNOE-800 will hold the value of the last read when the next read times out. If set to 0, the CNOE-800 will reset the registers to 0 if a timeout occurs.

NOTE: If a read and a write are configured in the same I/O scan entry, the CNOE-800 will use Modbus opcode 23, or x17, to issue a read/write in the same message. If the downstream device does not support this opcode, the the user must configure the reads and writes in separate entries.

Copying, Pasting, and Automatically Incrementing

Pressing the F6 key will copy the entire entry for which there is a highlighted cell. Pressing the F7 key will paste the copied data to the entire highlighted entry. Pressing the F8 key will automatically increment the highlighted cell by an appropriate number based on the data in the previous record.

Editing Global I/O Scanner Configuration

Pressing the F4 key will activate the Ethernet I/O Scanner global configuration screen. In this screen the user can select the Health Block start address, the Health Block's register space, and the functioning of the Diagnostic Block and the I/O Disable Block.

The Health Block is a group of eight 3x registers, each containing 16 bits, or 128 1x registers that report the health of the I/O scanner entries. The user can select the starting register address and the register space for the Health Block. The bits read from left to right, so I/O scan entry 1 is the most significant bit of the first 3x register, or the first 1x register. These registers will only be updated when one of the bits in the block changes state.

The Diagnostic Block is a group of 128 registers -- one per I/O scan entry -- that contains diagnostic data related to that entry. The user can configure whether the Diagnostic Block is enabled, the starting register address, and the register space (3x or 4x). The values in these registers are updated once per second. Figure 8-1 gives a list of the error codes associated with a given I/O scan entry. The high byte of each possible error contains the error code, and the xx is a counter that represents each time the I/O scan entry goes from normal operation to an error state. The counter rolls over from xFF to x80, so any number greater than x79 may not be accurate, but certainly means there have been a large number of errors.

Table 8-1 Diagnostic Block Error Codes

Error	Description
0x23xx	Invalid local register address specified
0x3Nxx	Received Modbus exception response N
0x73xx	Waiting for shared socket to connect
0x74xx	Connection actively refused by target (received a Reset)
0x75xx	Message timeout
0x76xx	No response to connect request
0x77xx	Message lost due to insufficient backplane buffers
0xF1xx	Initialization (powering up) state
0xFFxx	I/O Scanner disabled

The I/O Disable Block is a group of eight 4x registers, or 128 0x registers, laid out like the Health Block that creates an ON/OFF bit for each I/O Scanner entry. The user can configure whether the I/O Disable Block is enabled, the starting register address of the block, and the register space (0x or 4x). When the block is enabled, the user can disable a single entry by setting its associated bit to 1, rather than having to erase the entry from the table.

Ethernet I/O entries per socket

In the oNline Edit port parameters screen, the settings for the back plane port include a setting of Ethernet I/O entries per socket. This setting specifies the span of entries that the CNOE-800 will compare for a common IP address. All entries within that span will be single-threaded on a single socket to the specified IP address. When polling devices such as Niobrara's products that have limited numbers of available sockets, this number should be set to something large enough to accommodate that limit. However, for devices that can handle unlimited connections, the user may experiment with this number to achieve maximum throughput of data.

Table 8-2 SY/MAX Mode CNOE-800 Setup Example

Port	Drop Number	Mode	Baud Rate	Parity	Data	Stop	Error Check
E-Net	00	SY/MAX	NA	NA	NA	NA	NA
1	002	SY/MAX	9600	E	8	1	BCC
2	102	SY/MAX	9600	E	8	1	BCC

The Model 400 is connected to Port 1 of the CNOE-800 with an MM7 cable. The Model 450 is connected to an Ethernet cable to the CNOE-800 and Model 650. The Model 450 has an E-Net address of 05. The Model 650 has an E-Net address of 44.

The personal computer may be used to program each of the SY/MAX processors and the CNOE-800. Table 8-3 gives the route required for the personal computer to reach each of the devices.

Table 8-3 SY/MAX Mode Personal Computer Route Examples

Origin	Target	Route
Personal Computer	Model 400	102, 002
Personal Computer	Model 450	102, 000, 005
Personal Computer	Model 650	102, 000, 044
Personal Computer	CNOE-800	NONE

Each of the PLCs may also use the CNOE-800 to share information between themselves, by use of the SY/MAX Network WRITE and READ ladder rungs. Table 8-4 shows the routes required for a few of these combinations.

Table 8-4 SY/MAX Mode PLC Route Examples

Origin	Target	Route
Model 400	Model 450	002, 000, 005
Model 400	Model 650	002, 000, 044
Model 400	CNOE-800	NONE
Model 450	Model 400	005, 000, 002
Model 450	Model 650	005, 044
Model 450	CNOE-800	005, 000
Model 650	Model 400	044, 000, 002
Model 650	Model 450	044, 005
Model 650	CNOE-800	044, 000

Notice that the route from one SY/MAX processor, for instance the Model 400, to another SY/MAX processor, say the Model 650, is the reverse of the route from the 650 to the 400.

As mentioned before, several SY/MAX routes are available to access the registers in the CNOE-800. The routes listed above are all valid but are not all of the possibilities. If the serial SY/MAX message arriving at the CNOE-800 port has no route, the last drop in the route is the drop of that port, the last drop in the route is 204 with the next to last drop being the port, or a drop that is not assigned to the module is encountered, then the message will act on the registers in the module. Table 8-5 below illustrates a few examples of equivalent routes to the CNOE-800.

Table 8-5 QUCM Equivalent routes for accessing internal registers

Origin	Target	Route	Route	Route	Route
Personal Computer	CNOE-800	NONE	102, 204	102, 155	121
Model 400	CNOE-800	NONE	003, 204	003, 099	055, 043
Model 450	CNOE-800	005, 000	005, 000, 204	005, 000, 006	005, 000, 015, 145
Model 650	CNOE-800	044, 000	044, 000, 204	044, 000, 112	044, 000, 044

All communication may occur simultaneously and the available possible paths are not limited to the lists above.

MODBUS Modes

The Modbus protocol is implemented in a wide variety of products including Modicon PLCs, temperature controllers, flowmeters, intelligent valve systems, etc. The CNOE-800 provides a gateway translation from the SY/MAX protocol to/from Modbus RTU (or ASCII) protocol with the Modbus Gate, Modbus Host, and Modbus ASCII modes. The CNOE-800 Modbus Gate and ASCII modes provide reversible translations from SY/MAX messages to Modbus messages and vice versa using a defined series of rules. The Modbus Host mode is used when an explicit opcode and bias is required for a specific master application.

Modbus Overview

The Modicon addressing scheme is somewhat different than SY/MAX. In the SY/MAX PLC there is only one memory address space for data. Input registers, output registers, discrete input bits, and discrete output bits are all treated as registers and bits within these registers. Because of this treatment of memory, the SY/MAX communications protocol requires only one type of message to read, and another to write data to and from external devices.¹

The Modicon addressing method involves separate memory locations for input bits, output bits, input registers, and output registers. These different areas are denoted by the first character in the number that identifies the bit or register. Output bits (coils) are described by values in the range of 0xxxxx. Input bits (coils) are described by values in the range 1xxxxx. Input registers have values 3xxxxx and Output registers have values of 4xxxxx. Consequently the Modbus protocol requires separate messages to access the data in each of these areas. See Table 9-1.

For example, the first output bit in a Modicon PLC is addressed as 00001. The 150th output bit in the PLC is 00150 and is accessed using Function code 1 and written with Function codes 5 and 15. The seventeenth input bit is 10017 and is read by Function code 2. The 2381st input register is addressed by 32381 and is read with Function code 4. And the 52nd holding register is 40052 and read by Function code 3 and written with Function codes 6 and 16.

Table 9-1 MODBUS Function Code List

Function Code	Description	MODBUS Address Range	Notes
01	Read Coil Status	0XXXXXX	
02	Read Input Status	1XXXXXX	
03	Read Holding Register	4XXXXXX	
04	Read Input Registers	3XXXXXX	
05	Force Single Coil	0XXXXXX	
06	Write Single Register	4XXXXXX	
15	Force Multiple Coils	0XXXXXX	
16	Write Multiple Registers	4XXXXXX	
22	Masked Write Register	4XXXXXX	Not supported by all PLCs.
100	Random Read Holding Registers	4XXXXXX	Used by Powerlogic, not supported in any PLCs.

¹ The SY/MAX protocol includes both Priority and Non-priority READ and WRITE messages, but the different messages still operate on the same memory address space.

SY/MAX Message Addressing

The SY/MAX protocol supports a variety of operations for transferring data from device to device.

Table 9-2 SY/MAX Messages

Opcode (hex)	Description	Notes
20	Priority Read	May be generated by SY/MAX PLCs.
00	Non-Priority Read	
04	Non-Priority Random Access Read	
1e	Priority Write	May be generated by SY/MAX PLCs.
02	Non-Priority Write	
1e	Priority Alarm	Special version of Priority Write generated by SY/MAX PLCs.
22	Priority Print ASCII	

The SY/MAX PLC processors will only generate the Priority messages for peer-to-peer communication. These are the messages sent when a TWRITE, TALARM, TREAD, or network TPRINT is issued.

The Non-Priority WRITE message has the provision for a bit mask. This means that specific bits may be written to the remote device in a register without modifying other masked bits within that register. The Priority WRITE statement available in the PLC has no provision for a bit mask.

Message Translations

When messages cross from SY/MAX to Modbus media or vice-versa with a Niobrara bridge product (SPE4, EPE5, MEB, QUCM,CNOE-800) they are either reversibly translated or encapsulated and sent transparently. Translatable messages may be sent by one brand of device and operate successfully on another. By means of Niobrara's other translations, Modbus messages translated to SY/MAX operations may also operate on IDEC, PLOGIC, PNIM, and RNIM devices. Untranslatable SY/MAX or Modbus messages should only be directed to a device of the same brand to avoid unpredictable results. SY/MAX, PLOGIC, PNIM, and IDEC serial ports will return an encapsulated error to encapsulated Modbus messages. Modbus Host and Modbus Gate serial ports will return an encapsulated error to encapsulated SY/MAX messages. Net-to-Net, RNIM, MULTIDROP, Ethernet, SY/NET, and Modbus Plus ports forward all messages transparently.

SY/MAX to Modbus Translations

SY/MAX originated messages which can be reversibly translated are listed in Table 9-3.

Table 9-3 SY/MAX to Modbus Translations

SY/MAX Message	Modbus Message
Priority Read (0x20)	Read Holding Registers (3)
Non-Priority Read (0x00)	Read Holding Registers (3)
Priority Write (0x1E)	Write Multiple Registers (16)
Non-Priority Write (0x02) with mask all ones.	Write Multiple Registers (16)
Non-Priority Write (0x02) with mask containing < 16 contiguous ones, count = 1.	Masked Write Register (22)

All other SY/MAX commands will be encapsulated following Modbus opcode 17 (0x11) with a single parameter 0x01 and sent transparently over the Modbus media. Replies to encapsulated SY/MAX queries are encapsulated with opcode 17 and parameter 0x02. This opcode normally has no parameters, so

the presence of parameters allows the router to determine that the message is an encapsulated SY/MAX command and not a valid Modbus opcode 17.

Modbus to SY/MAX Translations

Modbus originated messages which can be reversibly translated are as follows.

Table 9-4 Modbus to SY/MAX Translations with type = "OTHER"

Modbus Message	SY/MAX Message
Read Coil Status (1)	Priority Read (0x20) with status register address 0xMN03 where M is the start bit modulo 16 and N is the bit count modulo 16
Read Input Status (2)	Priority Read (0x20) with status register address 0xMN05 where M is the start bit modulo 16 and N is the bit count modulo 16
Read Holding Registers (3)	Non-Priority Read (0x00) status field with Transnum 0x03
Read Input Registers (4)	Non-Priority Read (0x00) status field with Transnum 0x04
Force Single Coil (5)	Non-Priority Write (0x02) with Transnum 0x05 and single bit set in mask
Preset Single Register (6)	Non-Priority Write (0x02) status field with Transnum 0x06
Force Multiple Coils (15) if all coils lie in one register and count < 16. Force multiple coils with coil count = 1 may be detranslated as force single coil.	Non-Priority Write (0x02) with Transnum 0x0f and appropriate (not 0xfff) mask
Write Multiple Registers (16)	Non-Priority Write (0x02) with Status field with Transnum 0x10
Masked Write Register (22)	Non-Priority Write (0x02) with Transnum 0x10 and appropriate mask.
Random Read (100)	Non-Priority Random Read (0x04)

All other Modbus messages will be encapsulated for transmission of SY/MAX media in a Print command (0x22) with status register address 0xBAD5. This normally illegal status register value enables downstream translations to distinguish the encapsulated messages from an actual SY/MAX print message (which must be encapsulated to ride Modbus media). Replies to untranslatable Modbus messages are encapsulated as the Print Reply (0x92) with the same, illegal, status register address. Encapsulated Modbus query and response packets include a byte for the Modbus address following the status register address bytes. This byte is unused but is required for compatibility with existing Niobrara Modbus to SY/MAX translations. Niobrara translator conforming to this specification set this unused byte to zero on transmission and ignore it on reception.

If the target device type is set to "MODBUS" then only opcodes 03, 16, 22, and 100 are translated and all other opcodes will be encapsulated as above.

Master Operation

The Modbus Gate, Host, and ASCII modes may be used to connect Modbus slaves and networks of slaves to SY/NET. The Modbus Gate and ASCII modes use the translations in Table 9-3 to convert SY/MAX messages to Modbus serial messages. The Modbus Host mode allows the user to select the Modbus opcode and register bias (offset) for the translation. It is recommended that the Modbus Gate mode be used unless the user explicitly needs to alter the normal translation.

Register Bias

Modbus address values may fall outside the valid SY/MAX range of 1..8192. The CNOE-800 Modbus Host port provides an offset value called the Register Bias. The Register Bias may be set for any 16 bit value from 0 to FFFF hex (-23768 to 32767 dec). The Register Bias is only applied to Modbus Host Master translations and is not applied on Modbus messages incoming to an CNOE-800 Modbus Host or Gateway Slave port.

Register Calculations

The Modbus commands which are register operations, (3, 4, 6, 16) are related to the SY/MAX REMOTE address specified in the READ or WRITE by the following formula:

$$\text{MODBUS address} = (\text{SY/MAX REMOTE address}) + (\text{Register Bias})$$

NOTE: The Modbus Gate port always has Register Bias = 0. Also, the SY/MAX register address generated in a Modbus Slave translation always uses the Register Bias = 0

Example: A SY/MAX read is routed to a Modbus Host (Master) port of a CNOE-800. The Read Opcode is set for 4 because it is desired to read input register 300121 in a Modbus Slave PLC. The Register Bias is set to 0. The Modbus Address to be read is 121. The SY/MAX remote address for the READ is therefore: $(121) - 0 = 121$.

Example: A SY/MAX multiple register write is routed to a Modbus Host (Master) port of a CNOE-800. The Write Opcode is set to 16. The target registers in the Modbus devices start at 49175. The value 9175 is outside the range of the SY/MAX 8192 limit so the Register Bias must be set to a larger number such as 4000. With this value, the SY/MAX remote register number will be: $(9175) - 4000 = 5175$.

Table 9-5 displays the SY/MAX register to Modicon Register relationship for the CNOE-800 Modbus Host Master translation.

Table 9-5 SY/MAX Register to Modbus Register Relationship

SY/MAX Register	Modbus Register Bias = 0	Modbus Register Bias = 1	Modbus Register Bias = 500
1	1	2	501
2	2	3	502
3	3	4	503
4	4	5	504
5	5	6	505
6	6	7	506
7	7	8	507

Bit Calculations

Since the SY/MAX family does not differentiate between bit address and register address, the CNOE-800 MODBUS port must perform a translation to accomplish this task. The SY/MAX READ and WRITE messages support 16 bits per register address, so the translation to MODBUS coil address occurs in sections of 16 coils and occur on 16 bit boundaries. The MODBUS commands which are coil (bit) operations (1, 5, 15) are related to the REMOTE address specified in the READ or WRITE by the following formula:

$$\text{Coil Start Address} = (((\text{SY/MAX REMOTE address}) + (\text{Register Bias}) - 1) * 16) + 1$$

The start address refers to the address of bit 1 of the SY/MAX register. Table 9-6 displays the SY/MAX bit relationship to the Modbus coils for the CNOE-800 Modbus Master.

Table 9-6 SY/MAX Bit to Modbus Coil Relationship

SY/MAX Register	SY/MAX Bits	Modbus Bits Bias = 0	Modbus Bits Bias = 1	Modbus Bits Bias = 500
1	1...16	1...16	17...32	8017...8033
2	1...16	17...32	33...48	8034...8049
3	1...16	33...48	49...64	8050...8065
4	1...16	49...64	65...80	8066...8081
5	1...16	65...80	81...96	8082...8097
6	1...16	81...96	97...112	8098...8113
7	1...16	97...112	113...128	8114...8129

Modbus Retries

If a Modbus packet is transmitted from the CNOE-800 port and a valid reply is not received from the Modbus device, the CNOE-800 will wait for the amount of time specified in the MODBUS RETRY timeout register for that port. The CNOE-800 will then rebroadcast the message and wait for a valid reply. The CNOE-800 will retry only twice after the initial message.

Driver Mode

The Driver Mode setting for the Modbus modes allows the control of the RS-485 transmitter and receiver. For most applications, the PT to PT mode is the proper driver mode. This mode allows full duplex operation with the transmitter enabled at all times. This can be used to drive a 4-wire multidrop network as a master.

The FOUR WIRE mode causes the transmit driver to follow CTS. When CTS is enabled, the driver is enabled. When CTS is not enabled, the driver is allowed to tri-state at a high impedance. This mode is useful when the port is acting as a slave on a 4-wire multidrop network.

The TWO WIRE mode causes the transmit driver to follow CTS and the receiver to be disabled while transmitting. This mode allows the use of a 2-wire multidrop network.

Modbus peripherals are available in a variety of configurations. For most applications, you should set the port to 9600 baud, 8 data bits, EVEN parity (sometimes ODD) and 1 stop bit.

RS-485 MODBUS Host Master Mode Example

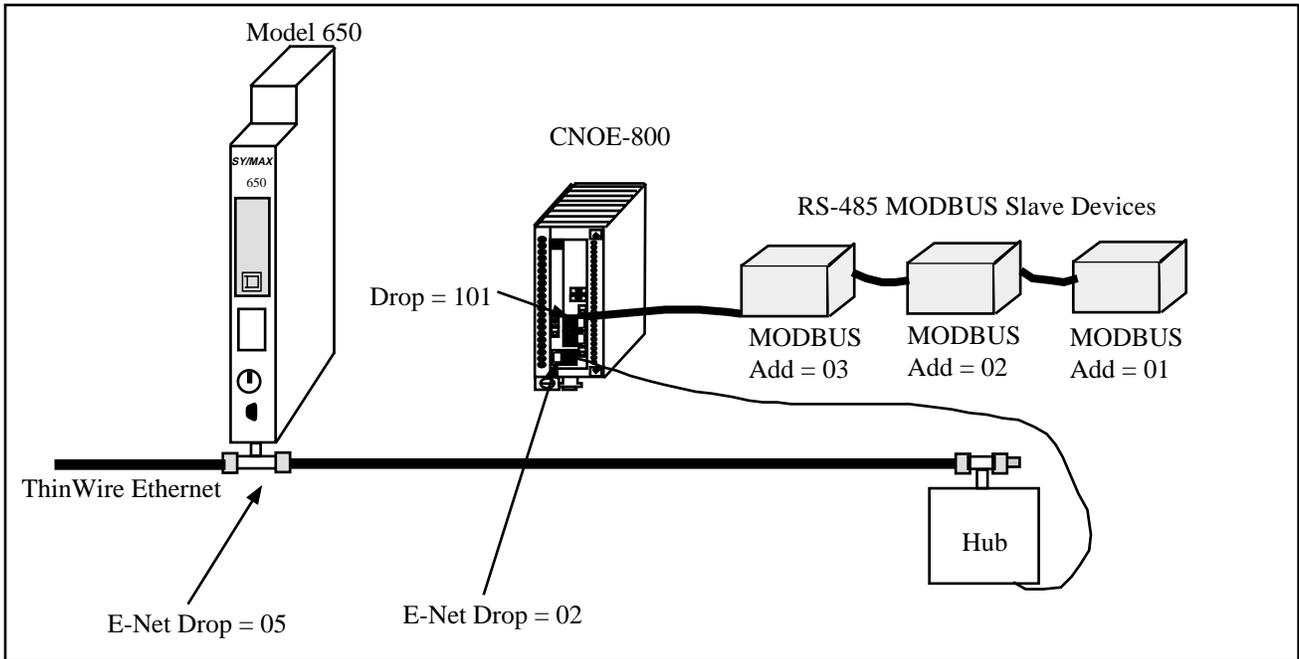


Figure 9-1 MODBUS Master Mode Example

Table 9-7 MULTIDROP Routing Examples

Origin	Target	Route
Model 650	MODBUS Slave 1	005, 002, 101, 001
Model 650	MODBUS Slave 3	005, 002, 101, 003

Table 9-8 CNOE-800 Setup for MULTIDROP Master Connection

Port	Drop #	Mode	Baud Rate	Parity	Data	Stop	Driver Mode
E-Net	02	SY/MAX	NA	NA	NA	NA	NA
1	101	Modbus Host	9600	E	8	1	Pt to PT

If the MODBUS peripherals are equipped for 4-wire RS-485 operation, up to 32 units may be connected to a single CNOE-800 RS-422 port. Set the Options bits for that Modbus port for Multidrop False and FULL Duplex.

If a 2-wire RS-485 network is required, set the Options bits for that port for Multidrop TRUE and HALF Duplex.

Modbus Slave Operation

The CNOE-800 Modbus Slave operation allows a Modbus Master to read and write data into SY/MAX devices via SY/NET. The CNOE-800 Modbus Slave port listens to the Master for messages that have Addresses that match entries in its Modbus Address table. Messages that do not correspond to addresses in the table are ignored. This functionality is similar to the operation of the Modicon BM-85 in Silent Master configuration.

The SY/MAX route generated for the translated message is determined by the setting in the Modbus Address table for that CNOE-800 port. Each CNOE-800 RS-422 port has its own table that is capable of holding 128 eight drop SY/MAX routes that correspond to 128 consecutive Modbus Slave addresses. The starting point of these 128 entries is adjustable using the Base Drop for that port. Therefore, two CNOE-800 ports connected in a multidrop fashion are able to respond to all 255 Modbus addresses.

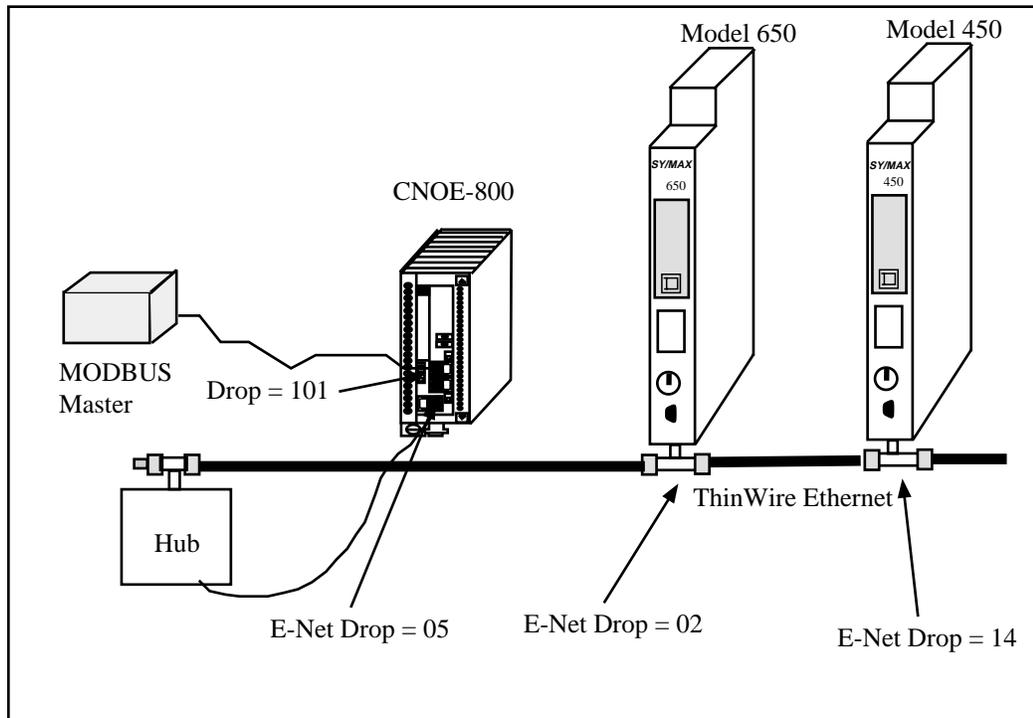


Figure 9-2 OTHER Modbus Slave Example

Table 9-9 Modbus Slave Example Setup

Origin	Target	Modbus Address	SY/MAX Route in the Modbus Address Table
Modbus Master	Model 650	1	101, 005, 002
Modbus Master	Model 450	2	101, 005, 014
Modbus Master	CNOE-800 Mailbox	3	101, 204

Table 9-10 Modbus Example Configuration

Port	Drop #	Mode	Baud Rate	Parity	Data	Stop	Driver Mode
E-Net	05	SY/MAX	NA	NA	NA	NA	NA
1	101	Modbus Gate	9600	E	8	1	Pt to Pt

Since the incoming Modbus message is translated to SY/MAX, it is possible to have any message routed to any other type of port on the SY/NET for further translation. This includes target devices such as PowerLogic units on PNIM ports, PLOGIC ports, IDEC units, and other speciality NIMs.

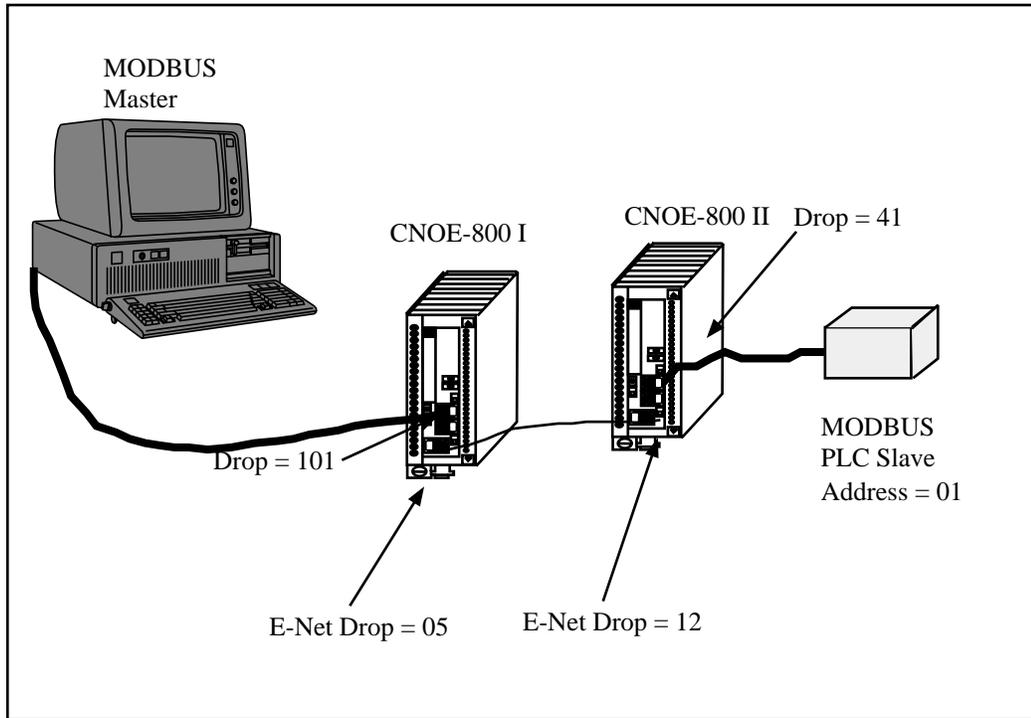


Figure 9-3 Modbus through SY/MAX Example

Table 9-11 Modbus Example Setup

Origin	Target	Modbus Address	SY/MAX Route in the Modbus Address Table
Modbus Master	Modbus PLC Slave	15	101, 005, 012, 041, 001

Table 9-12 CNOE-800 I configuration

Port	Drop #	Mode	Baud Rate	Parity	Data	Stop	Driver Mode
E-Net	05	SY/MAX	NA	NA	NA	NA	NA
1	101	Modbus Gate	9600	E	8	1	Pt to Pt

Table 9-13 CNOE-800 II configuration

Port	Drop #	Mode	Baud Rate	Parity	Data	Stop	Driver Mode
E-Net	12	SY/MAX	NA	NA	NA	NA	NA
1	41	Modbus Gate	9600	E	8	1	Pt to Pt

Figure 9-4 displays a Modbus Routing table for the previous application from the Edit Modbus Routing screen of EPE5SW.

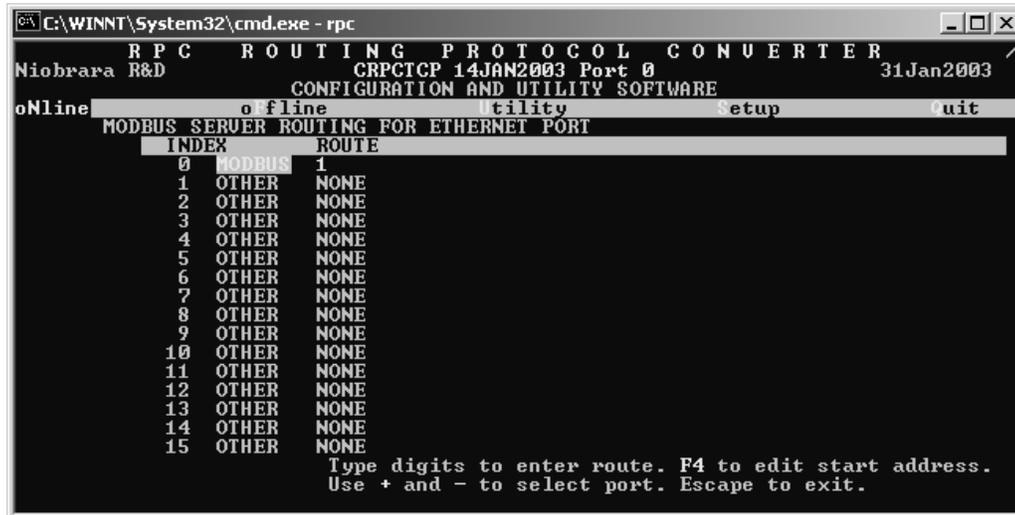


Figure 9-4 RPCSW32 Modbus Routing Editing Screen

PowerLogic Software use with Modbus Devices

The Modbus Host mode acting as a Master may be used to connect Modbus compatible devices to SY/NET for use with operator interfaces such as PowerLogic's System Manager software.

Register 8188

The entire suite of PowerLogic software packages includes the "feature" that they use a Read of register 8188 to determine if a device is online. Unfortunately, not all Modbus devices have registers that extend to 8188 and an error will be returned on the translation. If it is possible, Niobrara recommends that the user assign 8192 registers to the address space to be read in the target device. Otherwise, Bit 9 of the Options register for the port may be set to enable the Modbus port to recognize the single read of register 8188 and translate that read into the Modbus opcode 17 (11hex) to determine the PLC ID of the Modbus Device.

The Modbus PLC ID message returns a one byte ID, a run/halt byte, and a variety of other information about the PLC. The Modbus Host port will return the PLC ID in the LSB of the R[8188] reply. Bit 15 of R[8188] will always be set in this reply. Bit 16 of R[8188] will indicate the run/halt state of the PLC; if set, the PLC is in run and if clear, the PLC is in halt. Table 9-14 displays the currently used PLC IDs from Modicon.

Table 9-14 Modicon PLC ID Values

ID Value	PLC Type
0	Micro 84
1	484
2	184/384
3	584
8	884
9	984/Quantum

For example, if a Modicon 984 is attached to a Modbus Host port with Bit 9 of the Options register set, if the PLC is in run, a read of R[8188] will return the data C009 (hex) and if the PLC is in halt, the data 4009 (hex) will be returned.

Non-Priority Random Access Reads

The PowerLogic softwares all make extensive use of the SY/MAX Non-Priority Random Access Read message. This is a highly efficient use of the SY/MAX protocol and can provide excellent throughput for gathering large amounts of non-contiguous data. Niobrara and Square D have collaborated to develop a random read for the Modbus protocol. At the time of this writing only Niobrara and PowerLogic devices support opcode 100; Modicon PLCs do not. Because of this incompatibility, the Modbus Host mode must be used to connect most Modbus devices with PowerLogic software networks.

The Modbus Host mode translates each element of a random read to the corresponding Modbus read. So, an update of a custom table in System Manager with 60 entries, may very well translate to 60 Modbus RTU messages.

The Modbus Gate translation translates SY/MAX Random Access Reads into Modbus Random Reads for shipment across the Modbus media and hence require another Modbus Gate translation to restore the SY/MAX read. This technique allows the full use of the Random Read with SY/MAX and PowerLogic equipment.

Mode 1: SY/MAX

Either of the CNOE-800's two data ports can be set to SY/MAX mode for connection to a PLC, programming terminal, personal computer, operator interface, or other SY/MAX compatible device. Messages received on one CNOE-800 SY/MAX port are processed according to the route in the message. If the message is routed to another SY/MAX or Net-to-Net port within the same module, the packet will be retransmitted from that port. If the message has no route or is addressed to a null drop (204) or other drop not within the same CNOE-800 module, it is processed by the CNOE-800 itself and, if it is a read or write message, can access internal mailbox or configuration registers.

SY/MAX Routing Example

Figure 8-2 is an example of connecting three SY/MAX rack PLCs and a Personal computer together so that they may exchange data and be programmed by a single personal computer by means of the proper routing of communication packets.

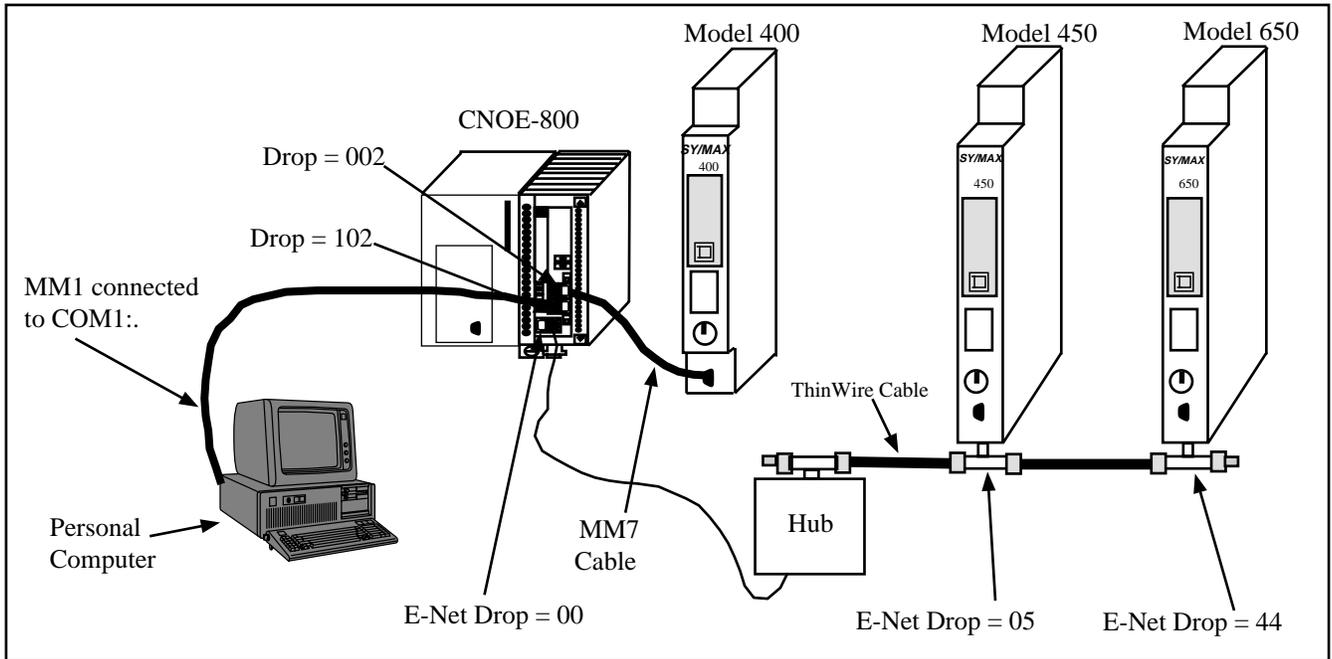


Figure 10-1 SY/MAX Mode Example

The Personal computer is connected to Port 2 of a CNOE-800 using an MM1 cable to its COM1: port. The CNOE-800 has the setup shown in Table 8-2 below:

NET-TO-NET MODE

Mode 2: Net-to-Net

If a data port of the CNOE-800 is connected to a NIM (CRM-510), the RS-422 port of a SY/LINK board, or to another CNOE-800, QUCM, MEB, EPE5 or SPE4 port, both ports must be configured in Net-to-Net mode and both ports must have the same drop number. By using the Net-to-Net mode the CNOE-800 may be used as a bridge between SY/NET and Ethernet.

NIM Net-to-Net Example

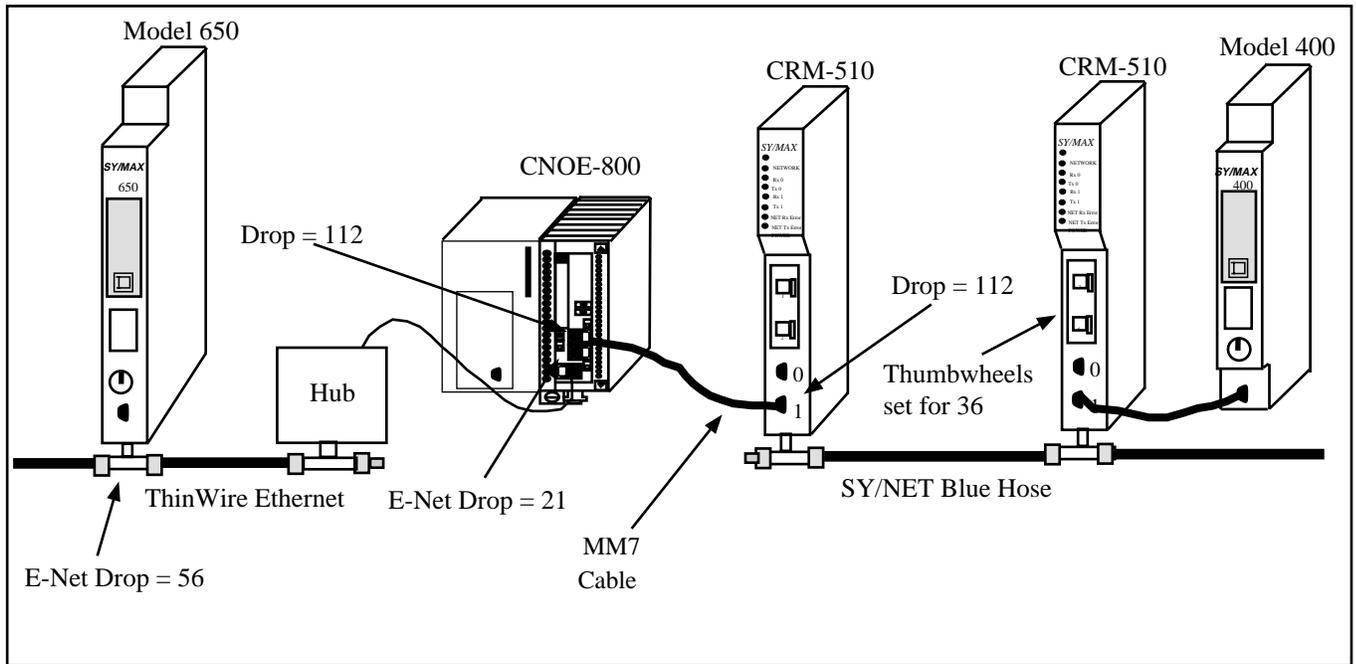


Figure 11-1 NIM Net-to-Net Example

Figure 11-1 displays a Blue Hose network connected to an QUCM with a 9600 baud Net-to-Net connection. The CNOE-800 is connected to a Model 650 via E-Net.

Table 11-1 NIM Net-to-Net Routing

Origin	Target	Route
Model 650	Model 400	056, 021, 112, 136
Model 400	Model 650	136, 112, 021, 056
Model 400	CNOE-800	136, 112, 99

Table 11-2 MEB Setup for NIM Net-to-Net Connection

Port	Drop #	Mode	Baud Rate	Parity	Data	Stop	Error Check
E-Net	21	SY/MAX	NA	NA	NA	NA	NA
1	112	Net-to-Net	9600	E	8	1	BCC

The use of the "On Ethernet" option of the Net-to-Net port on the CNOE-800 could allow several other routing possibilities including those listed in Table 11-1 and Table 11-3. Notice that since the Net-to-Net drop number is 112, the CNOE-800 will place drop number 12 on the Ethernet. Therefore drop number 12 must not reside on the Ethernet in any other device excluding this CNOE-800. To take advantage of this, Port 2 might be set to drop number 12 and placed "On Ethernet" at no expense.

Table 11-3 NIM Net-to-Net Routing with "On Ethernet"

Origin	Target	Route
Model 650	Model 400	056, 112, 136
Model 400	Model 650	136, 112, 056
Model 400	CNOE-800	136, 112, 99

EPE5 Net-to-Net Example

When the SY/MAX limit of 100 nodes is reached on a SY/MAX Ethernet extended LAN, a bridge must be used to further extend the network. A pair of CNOE-800 units (or EPE5) connected in Net-to-Net fashion will serve as this type of bridge. See Figure 11-2.

Additional throughput may be realized by increasing the baud rate to 19200, changing the parity to NONE, and using the CRC Error check. Adding an additional connection between another pair of ports on the CNOE-800s, (EPE5s) and splitting the routing load across two ports will also increase throughput.

This type of arrangement is also useful if a modem link is required between Ethernet LANs. The modems may be placed between the CNOE-800 (EPE5) ports allowing great distances between Ethernet LANs. The Niobrara RM14K rack mount SY/MAX compatible modem is ideal for this application, permitting baud rates of up to 14400 on dial-up, leased line, and radio links.

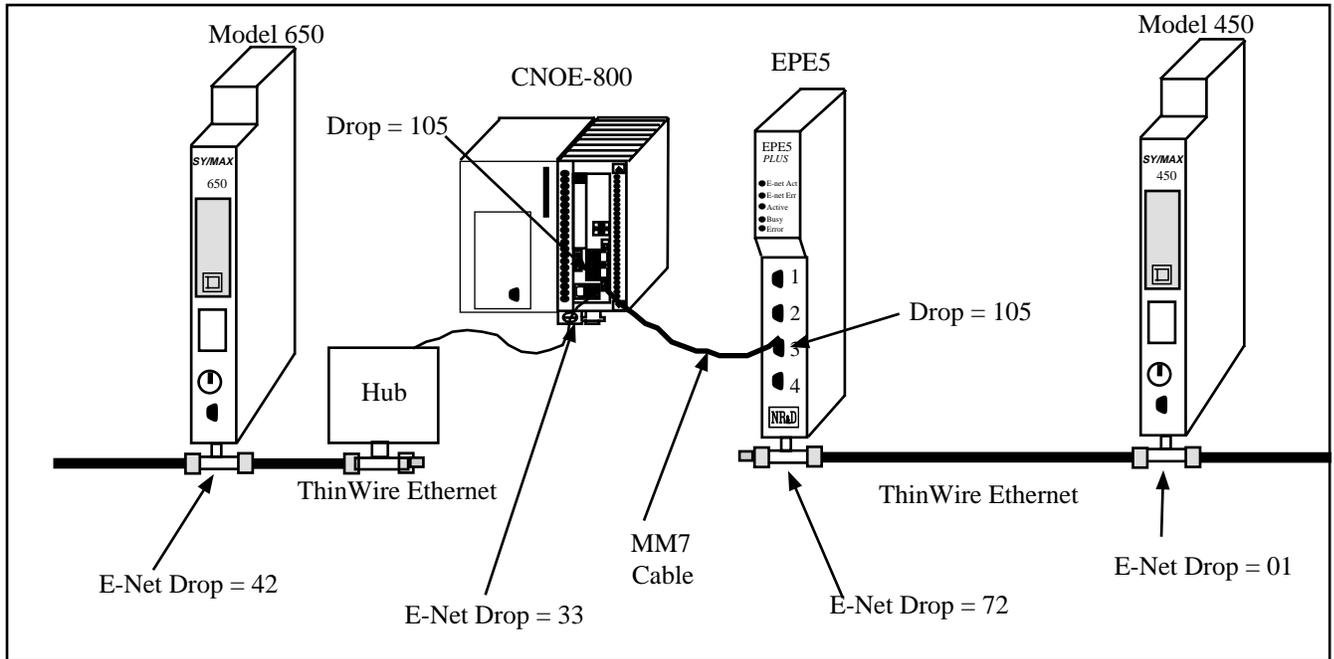


Figure 11-2 EPE5 Net-to-Net Example

Table 11-4 EPE5 Net-to-Net Routing Examples

Origin	Target	Route
Model 650	Model 400	042, 033, 105, 072, 001
Model 650	CNOE-800 Mailbox	042, 033
Model 650	EPE5 Mailbox	042, 033, 105
Model 450	Model 650	001, 072, 105, 033, 042
Model 450	CNOE-800 Mailbox	001, 072, 105
Model 450	EPE5 Mailbox	001, 072

Table 11-5 CNOE-800 Setup for EPE5 Net-to-Net Connection

Port	Drop #	Mode	Baud Rate	Parity	Data	Stop	Error Check
E-Net	33	SY/MAX	NA	NA	NA	NA	NA
2	105	Net-to-Net	19200	None	8	1	CRC

Table 11-6 EPE5 Setup for EPE5 Net-to-Net Connection

Port	Drop #	Mode	Baud Rate	Parity	Data	Stop	Error Check
E-Net	72	SY/MAX	NA	NA	NA	NA	NA
3	105	Net-to-Net	19200	None	8	1	CRC

The use of the "On Ethernet" option of the Net-to-Net ports on the CNOE-800 and EPE5 could allow several other routing possibilities including those listed in Table 11-4 and Table 11-7. Notice that since

the Net-to-Net drop number is 105, the CNOE-800 will place drop number 05 on its Ethernet and the EPE5 will place the drop number 05 on its Ethernet. Therefore drop number 05 must not reside on either Ethernet in any other device. To take advantage of this, another port in each module may be set to drop number 05 and placed "On Ethernet" at no expense.

Table 11-7 EPE5 Net-to-Net Routing Examples with "On Ethernet"

Origin	Target	Route
Model 650	Model 400	042, 105, 001
Model 650	CNOE-800 Mailbox	042, 033
Model 650	EPE5 Mailbox	042, 033, 105
Model 450	Model 650	001, 105, 042
Model 450	CNOE-800 Mailbox	001, 072, 105
Model 450	EPE5 Mailbox	001, 072

Peripheral Mode

Mode 3: Peripheral

A CNOE-800 serial port set to peripheral mode is capable of receiving SY/MAX network print requests routed to it through the SY/MAX and Net-to-Net ports in the same module. These network print requests are translated to raw ASCII and transmitted by the port. Network print messages are generated by a PLC when a print rung is executed on a PLC communication port which has been configured for network mode by previously issuing either a read or write rung including a route. The baud rate, data width, and parity setting of the peripheral mode port should be set to match the attached peripheral device. The route should consist of the drop number of the port connected to the originating device, any net-to-net drops, and the drop number of the peripheral mode port. The terminal emulator provided in MEBSW may be useful for testing peripheral mode ports.

Driver Mode

The Driver Mode setting for the Peripheral mode allows the control of the RS-485 transmitter and receiver. For most applications, the PT to PT mode is the proper driver mode. This mode allows full duplex operation with the transmitter enabled at all times. This can be used to drive a 4-wire multidrop network as a master.

The FOUR WIRE mode causes the transmit driver to follow CTS. When CTS is active, the driver is enabled. When CTS is inactive, the driver is allowed to tri-state at a high impedance. This mode is useful when the port is acting as a slave on a 4-wire multidrop network.

The HALF DUPLEX mode has the transmitter enabled at all times, but the receiver is disabled while transmitting. This feature is useful for ignoring an echo from the attached device.

The TWO WIRE mode causes the transmit driver to follow CTS and the receiver to be disabled while transmitting. This mode allows the use of a 2-wire multidrop network.

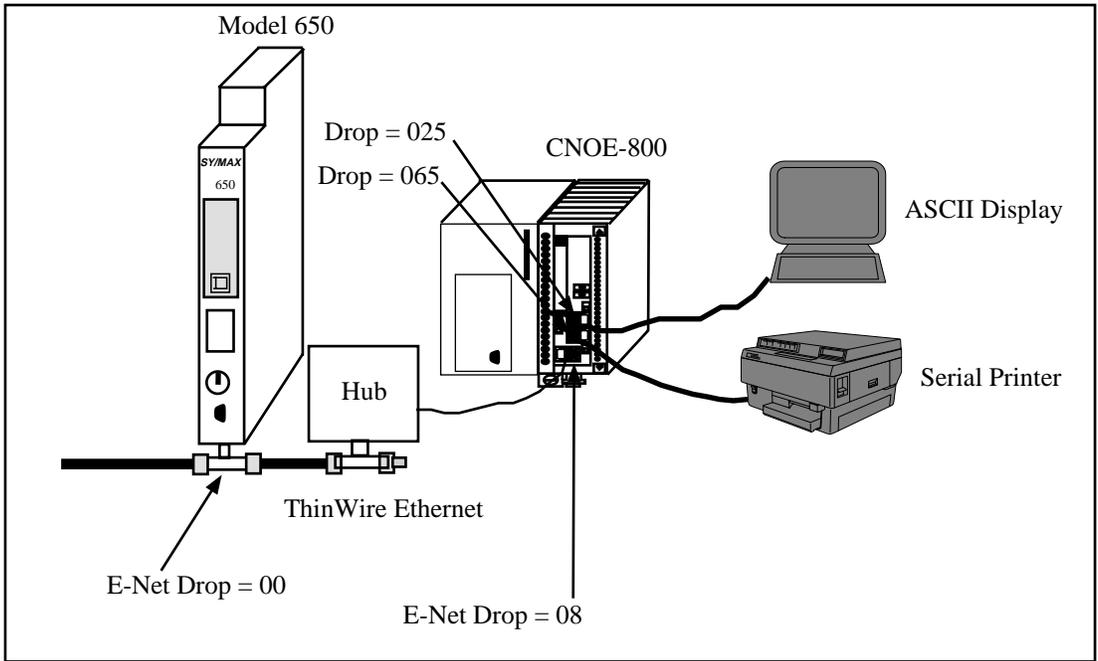


Figure 12-1 Peripheral mode example

Peripheral Mode Example

Table 12-1 Peripheral Routing Examples

Origin	Target	Route
Model 650	ASCII Display	000, 008, 025
Model 650	Printer	000, 008, 065

Table 12-2 CNOE-800 Setup for Peripheral Connection

Port	Drop #	Mode	Baud Rate	Parity	Data	Stop	Driver Mode
E-Net	08	SY/MAX 802.3	NA	NA	NA	NA	NA
1	25	Peripheral	9600	N	7	1	Pt to Pt
2	65	Peripheral	9600	N	7	1	Pt to Pt

Transparent and Share Modes

Modes 4,5: Transparent, Share

Transparent and Share modes are identical except for the behavior of the RTS pin (see RTS/CTS Handshaking, on page below). These modes are used to interface non-SY/MAX devices to the SY/MAX environment so that their communications can be carried on the SY/NET network or through SY/MAX modems or routers such as the EPE5. Transparent mode communication between ports in the same module can be used for PLC controlled switching of serial data. Transparent communication between ports in different modules can be used to transmit non SY/MAX serial ASCII messages over SY/NET, SY/MAX, or Modbus Plus cabling along with other SY/MAX or non-SY/MAX traffic. Example applications of transparent mode include:

- Connecting serial terminals to non-SY/MAX computers through the SY/NET network.
- Connecting distributed printers to non-SY/MAX computers.
- Sharing a printer between a SY/MAX PLC and a non-SY/MAX computer.
- Sharing a printer between a Modbus PLC and a non-Modbus computer.
- Programming Micro-1 or Model 50 processors through SY/NET.
- Programming Micro-1 or Model 50 processors through SY/MAX modems (Niobrara 2496X or RM14K).
- Baud rate or word size conversion of non-SY/MAX data or Modbus data.

Each transparent port accepts ASCII input and processes it as a series of SY/MAX network print messages. Each packet is transmitted according to the target route of the originating port. The route should consist of the drop number of the originating port, any Net-to-Net drops, and the drop number of the receiving port. For two-way communication, the receiving port should be programmed with the the same drops in reverse order. The target route can be configured using MEBSW or dynamically by a write messages generated by a PLC or Gateway port.

Packet assembly is performed by accepting characters until either an ASCII carriage return is encountered, the transparent mode packet size limit is exceeded, or the transparent mode time limit is exceeded between characters. Setting the packet size to 1 will cause each character entering the port to be transmitted without delay but will result in slow throughput because of the large overhead of sending each character as a packet. Larger packets are more efficient but will not be transmitted until they are terminated by a carriage return or timeout. For full duplex interactive applications, set the timeout to just slightly longer than the transmission time of a single character at the port's baud rate and word structure. For example, at 9600 baud a time limit of 2 (hundredths of a second) might be used.

TRANSPARENT Mode Example

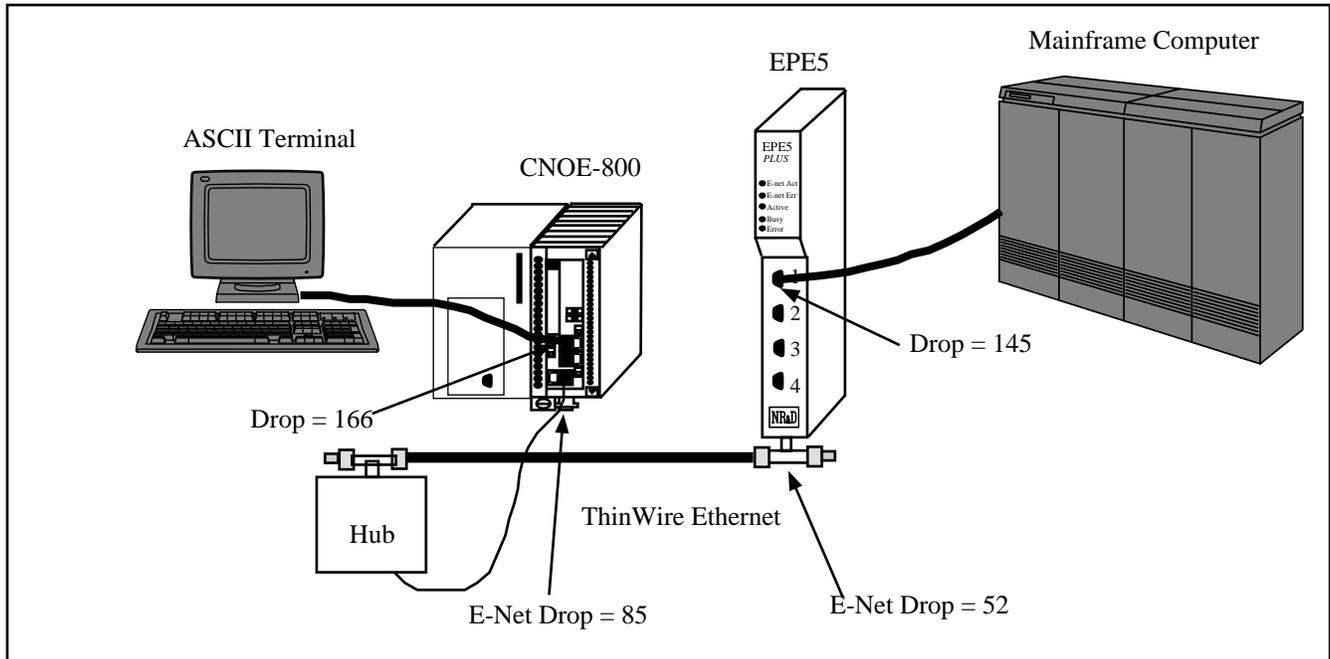


Figure 13-1 Transparent Mode Example

Table 13-1 Transparent Routing Examples

Origin	Target	Route
ASCII Terminal	Mainframe	166, 085, 052, 145
Mainframe	ASCII Terminal	145, 052, 085, 166

Table 13-2 CNOE-800 Setup for TRANSPARENT Connection

Port	Drop #	Mode	Baud Rate	Parity	Data	Stop
E-Net	85	SY/MAX	NA	NA	NA	NA
1	166	Peripheral	19200	N	7	1

Table 13-3 EPE5 Setup for TRANSPARENT Connection

Port	Drop #	Mode	Baud Rate	Parity	Data	Stop
E-Net	52	SY/MAX	NA	NA	NA	NA
2	145	Peripheral	19200	N	7	1

The ports connected to the terminal and the Mainframe computer should be set to the appropriate values of baud rate, parity, data bits, and stop bits, for those devices.

If the Devices are RS-232 but the EPE5 ports are RS-422, the **SC902** cable may be used to connect the external devices to the network module.

Baud rates of 19200, may be used for higher throughput. Set the timeout to just slightly longer than the transmission time of a single character at the port's baud rate and word structure.

Another use for the Transparent mode is the remote programming of other PLCs over SY/NET. The Model 50 or Micro-1 processors may be programmed through transparent ports over Ethernet. Set the Port connected to the Personal Computer running SFW50 or SFW30 for Transparent mode. Set the Port connected to the processor to IDEC mode. The IDEC port will accept network print messages and pass those along to the PLC. The IDEC port will then send the reply back to the Transparent port to complete the message.

Driver Mode

The Driver Mode setting for the Share mode allows the control of the RS-485 transmitter and receiver. For most applications, the PT to PT mode is the proper driver mode. This mode allows full duplex operation with the transmitter enabled at all times. This can be used to drive a 4-wire multidrop network as a master.

The FOUR WIRE mode causes the transmit driver to follow CTS. When CTS is enabled, the driver is enabled. When CTS is not enabled, the driver is allowed to tri-state at a high impedance. This mode is useful when the port is acting as a slave on a 4-wire multidrop network.

The HALF DUPLEX mode has the transmitter enabled at all times, but the receiver is disabled while transmitting. This feature is useful for ignoring a hardware echo from the attached device.

The TWO WIRE mode causes the transmit driver to follow CTS and the receiver to be disabled while transmitting. This mode allows the use of a 2-wire multidrop network.

PLogic and PNIM Modes

Mode 6: PowerLogic

The CNOE-800 can be used to route SY/MAX read and write messages originated by a PLC, computer, or CNOE-800 Gateway port to a PowerLogic network of one or more PowerLogic modules. The CNOE-800 handles the difficult task of allowing one communication process to be allowed for only one circuit monitor at a time, permitting multiple accessors to poll the units independently.

The PNIM mode is different from the PLOGIC mode. The PLOGIC mode uses the modified SY/MAX protocol that the PowerLogic Circuit monitors can use. Since the PLOGIC mode conforms to the SY/MAX protocol, other SY/MAX devices may be used to extend the connection from the CNOE-800 port to the Circuit Monitors, including SY/MAX compatible modems like the 2496X and RM14K. The PNIM mode converts the SY/MAX protocol to the PNIM protocol. This protocol is not the same as SY/MAX and SY/MAX devices such as the 2496X may not be used to extend the connection.

Since the PowerLogic Circuit Monitors will communicate with the PLOGIC and PNIM modes, it is recommended that the PNIM mode be used when connecting to PowerLogic Circuit monitors. The PNIM mode will return an error 17 if the slave does not respond while the PLOGIC mode simply times out.

The route used should be the route from the accessor to the CNOE-800 port connected to the PowerLogic bus with an additional drop corresponding to the PowerLogic drop number set in the PowerLogic unit's rotary address switches. The port should be configured for 8 data bits, even parity, 9600 baud, and PLOGIC mode for connecting with units "out of the box". The baud rate may be changed to other values to match the application.

The PowerLogic units operate on a 4-wire RS-485 network and may be connected directly to the RS-422 port of the CNOE-800. The CNOE-800 supplies internal biasing for its receive data lines so the PowerLogic RS-485 Multipoint Communications Adapter (MCA-485) is not required for operation with the CNOE-800. See the recommended cabling section at the end of this manual.

PowerLogic Mode Example

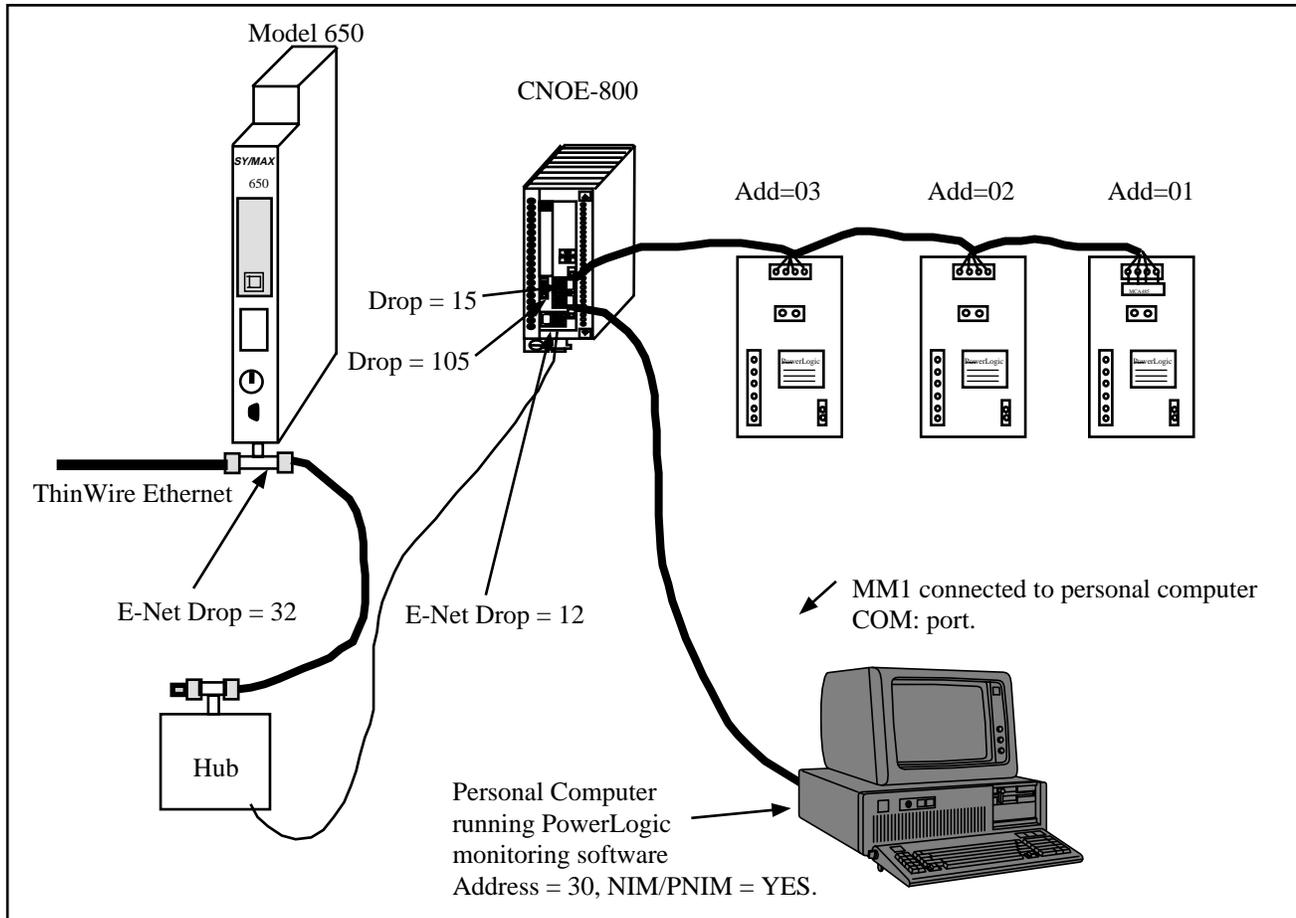


Figure 14-1 PowerLogic Example

Table 14-1 PowerLogic Routing Examples

Origin	Target	Route
Model 650	CM 1	032, 012, 015, 001
Model 650	CM 3	032, 012, 015, 003
Personal Computer	CM 1	30, 105, 015, 001
Personal Computer	CM 2	30, 105, 015, 002

Table 14-2 CNOE-800 Setup for PowerLogic Connection

Port	Drop #	Mode	Baud Rate	Parity	Data	Stop
E-Net	12	SY/MAX	NA	NA	NA	NA
1	015	PLOGIC	9600	E	8	1
4	105	SY/MAX	9600	E	8	1

The PowerLogic units are set up as 4-wire. The Personal Computer has an address of 30 and NIM/PNIM is set to YES.

Mode 11: PNIM

The CNOE-800 can be used to route SY/MAX read and write messages originated by a PLC, computer, or CNOE-800 Gateway port to a network of one or more devices that communicate using the PNIM protocol. This includes PowerLogic Circuit monitors, Altivar motor drives, and other PNIM devices. The CNOE-800 handles conversion from SY/MAX protocol to PNIM protocol.

The PNIM mode is different from the PLOGIC mode. The PLOGIC mode uses the modified SY/MAX protocol that the PowerLogic Circuit monitors can use. Since the PLOGIC mode conforms to the SY/MAX protocol, other SY/MAX devices may be used to extend the connection from the CNOE-800 port to the Circuit Monitors, including SY/MAX compatible modems like the 2496X and RM14K. The PNIM mode converts the SY/MAX protocol to the PNIM protocol. This protocol is not the same as SY/MAX and SY/MAX devices such as the 2496X may not be used to extend the connection.

Since the PowerLogic Circuit Monitors will communicate with the PLOGIC and PNIM modes, it is recommended that the PNIM mode be used when connecting to PowerLogic Circuit monitors. Since the PNIM mode ensures an acknowledgment from the network devices, network security is enhanced over the PLOGIC mode.

The route used should be the route from the accessor to the CNOE-800 port connected to the PNIM bus with an additional drop corresponding to the drop number set for the attached PNIM device.. The port should be configured for 8 data bits, even parity, 9600 baud, and PNIM mode for connecting with units "out of the box". The baud rate may be changed to other values to match the application.

The PNIM units operate on a 4-wire RS-485 network and may be connected directly to the RS-422 port of the CNOE-800. The CNOE-800 supplies internal biasing for its receive data lines so the PowerLogic RS-485 Multipoint Communications Adapter (MCA-485) is not required for operation with the CNOE-800. See the recommended cabling section at the end of this manual.

PNIM Mode Example

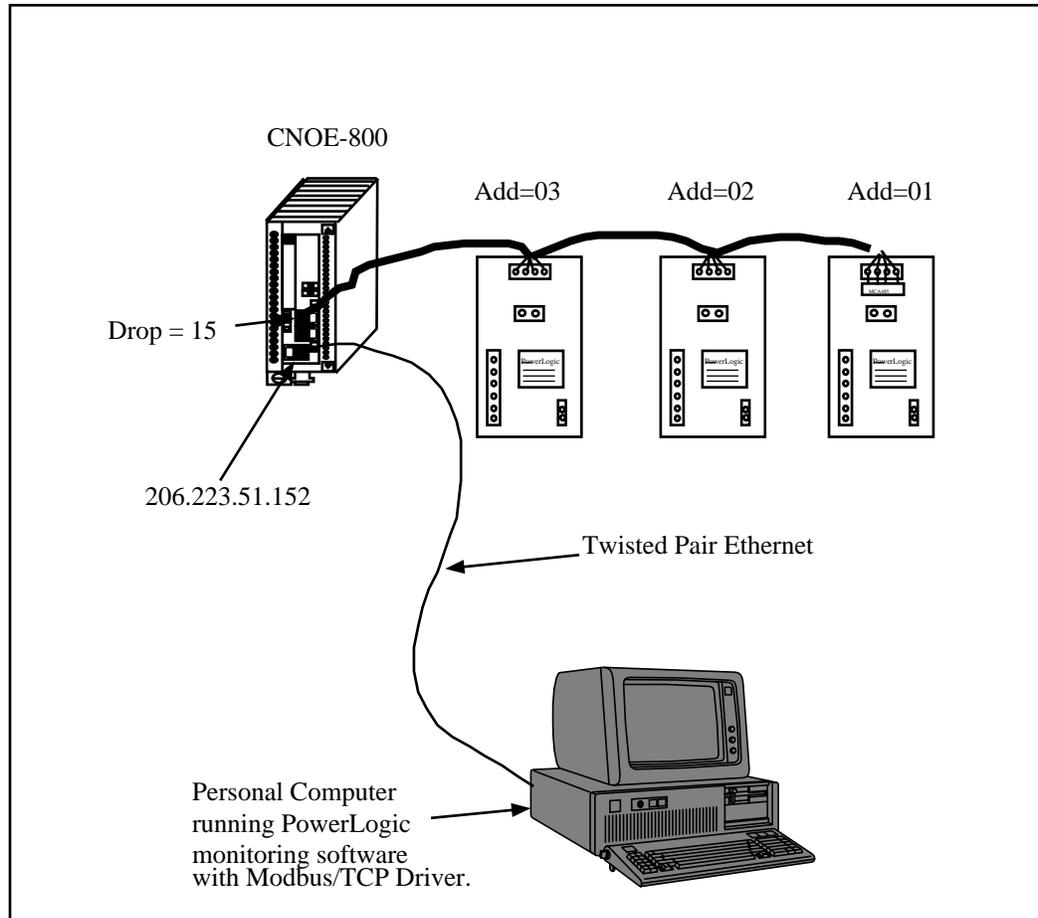


Figure 14-2 PNIM Modbus/TCP Example

Table 14-3 CNOE-800 Modbus/TCP Server Setup

Index	TYPE	ROUTE
0	OTHER	15,1
1	OTHER	15,2
2	OTHER	15,3

Table 14-4 SMS3000 Device Setup

Device	IP Address	Index
CM 1	206.223.51.152	0
CM 2	206.223.51.152	1
CM 3	206.223.51.152	2

Table 14-5 CNOE-800 Setup for PNIM Connection

Port	Drop #	Mode	Baud Rate	Parity	Data	Stop
E-Net	206.223.51.152	MODBUS/TCP	NA	NA	NA	NA
1	15	PNIM	9600	E	8	1

Mode 7: IDEC

Micro-1 and Model 50 Interfacing

The CNOE-800 can translate SY/MAX read and write messages such as those generated by Read and Write rungs in a PLC ladder program to IDEC format read and write rungs compatible with the Micro-1 or Model 50. A network of either of these processors can be connected to a single CNOE-800 port and then accessed by devices connected to other ports on the module. The route for such messages should include all drops necessary to reach the CNOE-800 port, and one additional drop corresponding to the drop number of the Micro-1 or Model 50 processor within the ring network. The CNOE-800 is not capable of translating IDEC format requests to SY/MAX requests. This mode is useful when one or more Micro-1 or Model 50 processors are used as remote I/O blocks for a SY/MAX processor. Even if only one IDEC compatible processor is connected to the port, it must be assigned a drop number. A drop setting of zero or none cannot be used. A single Micro-1 or Model 50 processor can be conveniently connected to an CNOE-800 port with a Niobrara ID422 or MD422 cable respectively. To connect a network ring of multiple units, use the RIU-10 or RIU-20 from Square-D.

When accessing I/O points, internal relays, and shift register bits, the register number in the SY/MAX read or write message is translated to a Micro-1 or Model 50 bit address. Sending a SY/MAX read message will return the state of the eight bits starting at the specified address. Therefore register 256 bit 8 is the same contact as register 257 bit 7. This also means that successive 8 bit registers are addressed at register numbers 8 registers apart. For example, the first internal relay register (8 bits) is found at address 512 but the second 8 bit internal relay register is at address 520, not address 513.

Timer, counter, and the Model 50 data registers are 16 bits wide and are addressed as words. This means the first data register is at address 1792 and the second at address 1793. When interfacing with the Model 50, the most efficient communications will result from reading and writing the data registers and programming the Model 50 to internally address inputs and outputs.

When accessing timer and counter registers, a Read access returns the current value of the timer or counter register. A Write access loads the associated preset register.

Micro-1 register addressing

To communicate with the Micro-1, the CNOE-800 port should be set to 9600 baud, even parity, 8 data bits, 1 stop bit, IDEC mode. This table shows the SY/MAX register number to use to access various Micro-1 resources.

Table 15-1 Micro-1 Processor Equivalent Register List

Micro-1 Register	SY/MAX Register Equivalent	Notes
Onboard Input	256	
Expansion Input	264	
Onboard Output	384	Bits 1 - 5 only
Expansion Output	392	
Internal Relays	512 - 760	
Shift Registers	768 - 888	
Timers	1024 - 1103	
Counters	1280 - 1326	

Model 50 register addressing

To communicate with the Model 50, the CNOE-800 port should be set to 9600 baud, no parity, 8 data bits, 2 stop bits, IDEC mode. This table shows the SY/MAX register number to use to access various Model 50 resources.

Table 15-2 Model 50 Processor Equivalent Register List

Model 50 Register	SY/MAX Register Equivalent	Notes
Inputs	256 - 376	
Outputs	384 - 504	
Internal Relays	512 - 744	
Shift Registers	768 - 888	
Timers	1024 - 1103	16 Bits / register
Counters	1280 - 1324	16 Bits / register
Data Register	1792 - 1891	16 Bits / register

IDEC Mode Example

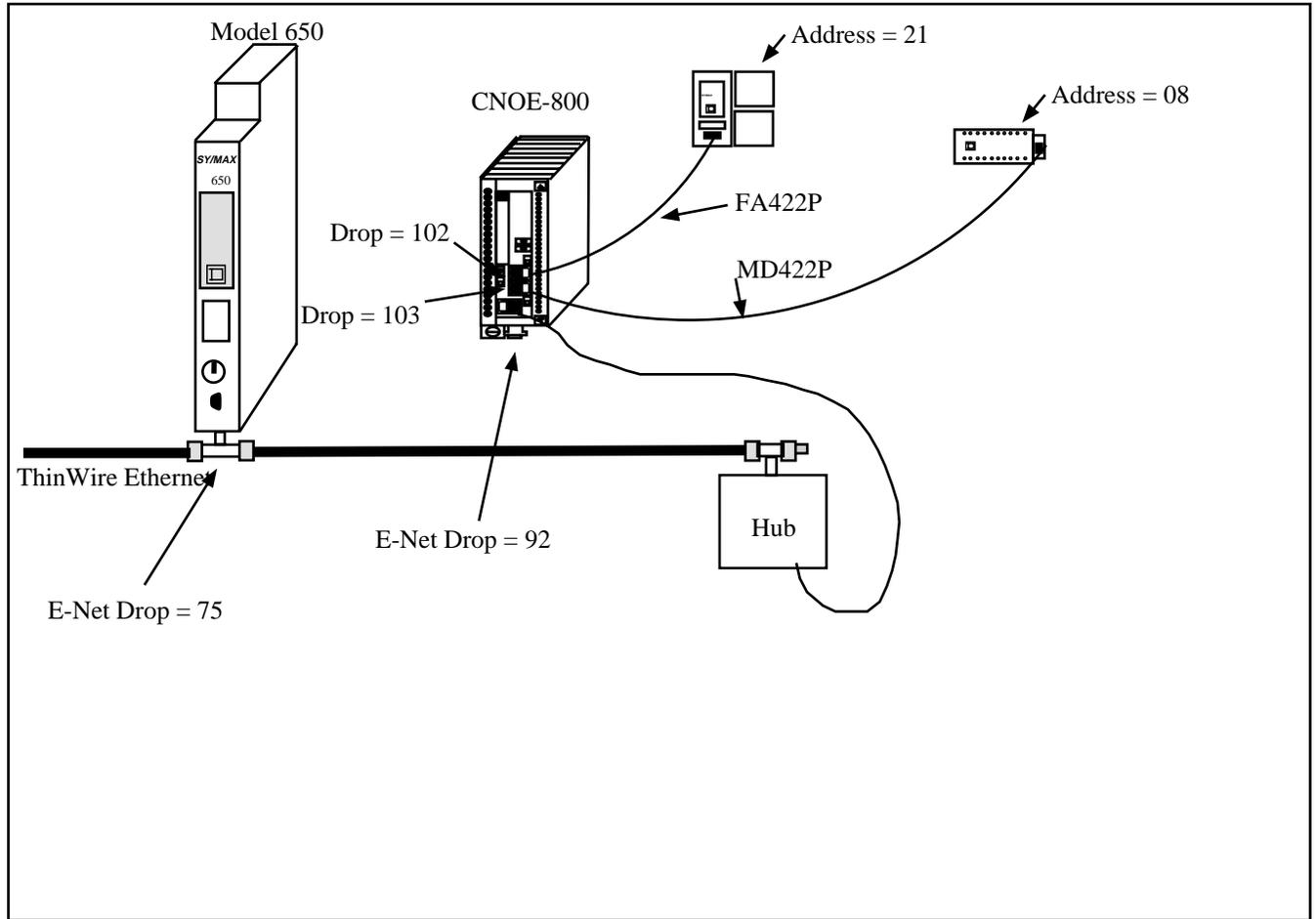


Figure 15-1 IDEC Mode Example

Table 15-3 IDEC Routing Examples

Origin	Target	Route
Model 650	Model 50 on Port 1	075, 092, 102, 021
Model 650	Micro-1 on Port 2	075, 092, 103, 008

Table 15-4 CNOE-800 Setup for IDEC Connection

Port	Drop #	Mode	Baud Rate	Parity	Data	Stop
E-Net	92	SY/MAX	NA	NA	NA	NA
1	102	IDEC	9600	N	8	2
2	103	IDEC	9600	E	8	1

Gateway Mode

Mode 8: Gateway

ASCII Command Gateway Functions

To simplify access to SY/MAX devices such as PLCs, Niobrara's various modules, PowerLogic modules, and IDEC mode PLCs, the CNOE-800 provides a Gateway mode. A port in Gateway mode accepts simple ASCII commands and translates them to properly formatted SY/MAX read, write, and print messages. Using the CNOE-800 Gateway mode, any device with an ASCII serial port can communicate with the SY/MAX devices. This function facilitates interfacing BASIC or C programs or non-SY/MAX PLCs to SY/MAX devices (or, through an IDEC port, the Micro-1 or Model 50).

The target of all Gateway commands is determined by a route from the Gateway port to the destination device. If the destination is connected to the same module, the route may be the drop of the Gateway port followed by the drop of the destination port. If the target device is connected to another CNOE-800 or to a NIM connected to the Gateway CNOE-800 through SY/NET, the second drop will be that of the Net-to-Net port within the Gateway module and additional drops will be added to route the message through the additional network devices. A null route with no drops will direct Gateway accesses to the local processor equivalent mailbox or configuration registers within the CNOE-800 module. The target route may be set by using MEBSW (or other means) to modify the Target Route configuration registers or through the Gateway by use of the Gateway ADDRESS command. The target port can also be a PowerLogic or IDEC mode port and accesses made to the registers of those devices. When addressing PowerLogic or IDEC devices, don't forget the final drop should be the drop of the target unit in the IDEC or PowerLogic network. If the target port is an IDEC mode CNOE-800 port connected to Micro-1 or Model 50 processors, the Set and Clear commands can be applied much more quickly than the Write command to I/O, IR, or SFR registers.

Each Gateway mode command consists of a letter, one or more decimal numeric parameters separated by non-numeric delimiters and either an ASCII carriage return or a time delay. The commands are described individually below. The command termination parameters of packet size limit and packet time limit are the same as for Transparent mode. Unless it is not possible to terminate each command with a carriage return, a packet size limit of 128 and time limit of 100 (1 second) are recommended.

The terminal emulator provided in RPCSW32 is useful for testing the gateway features.

Gateway READ command

To read from one or more registers of the addressed SY/MAX device, send the Read command to the Gateway port. The command consists of an 'R' followed by the register number optionally followed by a register count. The 'R' may be immediately followed by the first digit of the register number or they may be separated by any number of non-numeric characters. The first non-numeric character encountered in the register number likewise delimits it.

The register count, if present is separated from the register by one or more non numeric characters and terminated by any non numeric character or the end of the packet. The reply to a successful read command will be the decimal value of the register followed by a carriage return. If multiple registers are read (i.e. a count field is present and is greater than 1), then the decimal values for the registers will be output separated by ASCII spaces and with a carriage return after the last value. The following are all valid read commands:

- R 100
- r100,10
- READ 100 FOR 10
- Ralph was here 100 years ago.

Gateway WRITE command

The Write command is used to transmit a new value to one or more registers in the target device. The write command is formatted as a letter 'W' followed by zero or more non-numeric characters, followed by the decimal register number, followed by one or more non-numeric characters, followed by the decimal value to be written. Multiple registers can be written by appending additional values to the command delimited by strings of one or more non-numeric characters. The command packet may be terminated by a carriage return or by a time delay. The following are examples of valid Gateway write commands:

- W 100 2
- w100=2,3
- WRITE 100 WITH THE VALUE 2 AND ONE-HUNDRED ONE WITH THE VALUE 3
- We can use anything to separate 100 from 2.

Gateway SET command

The Gateway set command sends a modified write message which will set a single bit in the specified register of the target device to one. The command is an ASCII "S" followed by the register number and bit number. The following are valid bit set commands:

- S 200.3
- s200 16
- SET 200-3

Gateway CLEAR command

The Gateway clear command sends a modified write message which will clear a single bit in the specified register of the target device to zero. The command is an ASCII "C" followed by the register number and bit number. The following are valid bit clear commands:

- C 200.3
- c200 16
- Clear 200-3

Gateway BIT command

The Gateway bit test command sends a read message to the target device and evaluates the returned value to determine the state of the specified bit. The Gateway port will output an ASCII "1" if the bit is set or a "0" if not. The command is an ASCII "B" followed by the register number and bit number. The following are valid bit set commands:

- B 200.3
- b200 16
- Bit 200-3

Gateway PRINT command

The Gateway print command formats an ASCII message as a SY/MAX network print message and forwards it to the target device. The target should be a NIM port in peripheral mode or an CNOE-800 port

in Peripheral, Transparent, or Share mode, or another Gateway port. The print command is any string starting with an ASCII "P". All characters following the "P" will be emitted by the destination port followed by a carriage return line feed sequence.

Note: A carriage return and line feed will be appended to the message regardless. If a carriage return is sent at the end of the string from the Gateway device, then the string emitted from the peripheral port will have two carriage returns and a line feed. If this presents a problem, use the character limit or inter-character time limits to terminate the message from the Gateway device. If the carriage return and line feed sequence is not desirable, use the Omit print command.

The following are valid Gateway Print commands:

- PHello
- pNow is the time for all good men...

Gateway OMIT Print Command

The Gateway Omit command is a network print command that omits the carriage return and line feed sequence. This allows the printing of exact characters from a peripheral port without the addition of the carriage return and line feed. If no terminator is needed, use the inter-character timeout or character limit settings for the Gateway port to terminate the string. An example of using the Omit command is to send the attention command to a Hayes modem to return it to the command mode. This is accomplished by pausing one second, sending +++, and pausing one second. The three plus signs must not have any other characters with them. The valid command would be: O+++

Gateway ADDRESS command

The target for Gateway commands may be set with the Gateway address command. This command is an ASCII "A" followed by up to eight decimal drops separated by strings of one or more non numeric characters. Remember that the first drop should be the drop number of the Gateway port itself. The following are valid Gateway ADDRESS commands:

- A8,10
- ADDRESS 008 102 104

Gateway Mode Example

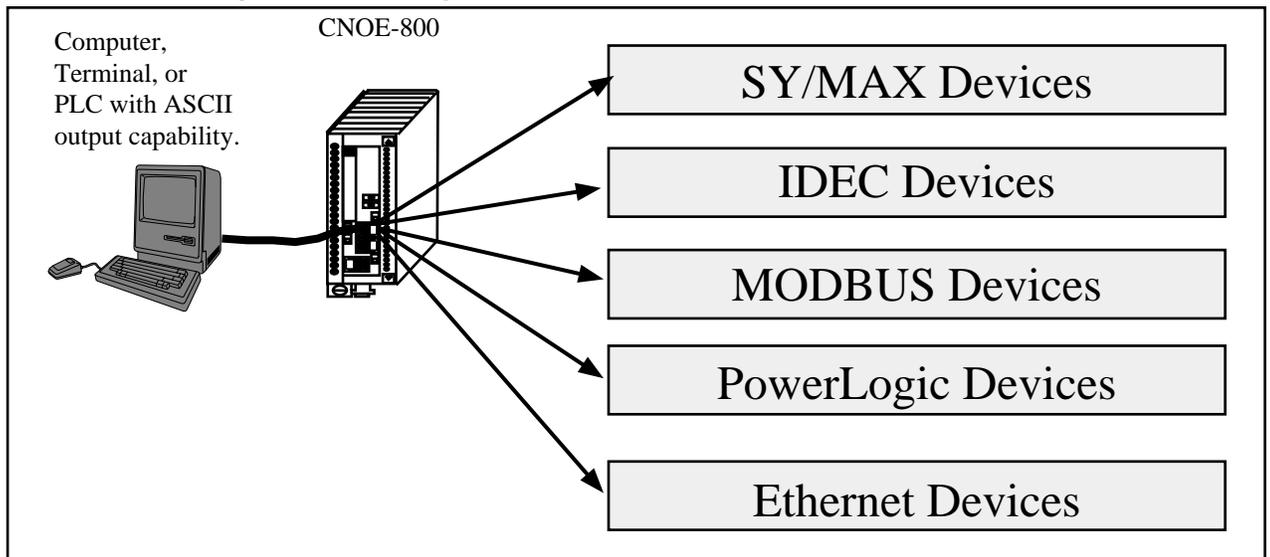


Figure 16-1 GATEWAY Example

The Gateway mode simplifies access to SY/MAX devices, such as PLCs, NR&D's various modules, the CNOE-800 itself, and any other external mode of the CNOE-800 (IDEC, PLogic, MODBUS, etc.). A Gateway port accepts simple ASCII commands and translates them to properly formatted SY/MAX

read, write, and print messages. Any device with an ASCII serial port may be used to communicate with SY/MAX devices

Figure 16-2 represents a view of the Terminal Emulator from RPCSW32 connected to an CNOE-800 Gateway port.

```
Type ctrl-End to exit terminal. Type F7 to begin capture to a file.
Type F9 to change terminal communication setup.
To send hex sequence, type INSERT key, enter hex codes, type ENTER.
r1<0D>
0<0D>
r1,10<0D>
0 0 32768 0 0 0 0 4660 65278 1234<0D>
w12,55,67<0D>
<0D>read12<0D>
55<0D>
s12.1<0D>
<0D>r12<0D>
55<0D>
s12.16<0D>
<0D>r12<0D>
32823<0D>
c12,1<0D>
<0D>r12<0D>
32822<0D>
Enter hex codes to send: 10 05
<10><05>█
```

Figure 16-2 Terminal Emulator connected to Gateway port

Table 16-1 Gateway Command Examples

Command	Description	Example
READ	Reads one or more registers from addressed device.	R 8001.10
WRITE	Writes one or more registers to addressed device.	W 100,2,5
SET	Sends modified write to set a single bit.	S 200-3
CLEAR	Sends modified write to clear a single bit.	C 315,2
BIT	Sends read to determine state of bit.	b375 15
PRINT	Sends ASCII message, adds CR and LF.	PHello
OMIT	Sends ASCII message without CR and LF.	oHello
ADDRESS	Sets the target route for the Gateway port.	A8,10

BASIC Language Example Program

This sample program should run on a PC using most BASIC interpreters. Set the Gateway port to 9600,N,8,1 and connect to COM1 of the PC.

```
10 OPEN "COM1,9600,N,8,1" for RANDOM as 1 'Open the PC's COM port.
20 PRINT #1, "A 3,4" 'Set the route for the Gateway port.
30 INPUT #1, A$ 'Receive the CNOE-800's CR reply.
40 PRINT #1, "R 5,10" 'Read registers 5 through 15 in the target.
50 INPUT #1, B$ 'Receive the reply data.
60 PRINT B$ 'Print data to screen. Format: Reg5 Reg6 Reg7...
70 CLOSE 1 'Close PC's COM port
80 END
```

Multidrop Mode

Mode 9: Multidrop

The CNOE-800 multidrop port mode can be used to route packets between three or more CNOE-800/SPE4 modules over a single communication medium such as an RS-485 pair or multidrop modems or radios. In multidrop mode, the CNOE-800 units on the line use a time division scheme to arbitrate access to the line. When an individual CNOE-800 desires to transmit, it asserts its RTS pair and waits for the modem to respond with CTS. Then it transmits the packet and waits for a response from the receiving unit. All units monitor the line and watch for packets with their individual address.

NOTICE: The MULTIDROP mode is ideally suited for use with a 2-wire RS-485 multidrop network. If a radio or multidrop modem network is to be used, it is recommended that the RNIM mode be used. It is better suited for radio and other multidrop modem applications.

To configure a multidrop network, you must set the Number of Nodes, Time Slice and Node Priority of each node. The Number of Nodes and Time Slice are set the same for all modules. The Node Priority of each module is set to a unique value between 1 and the Number of Nodes. The value of Time Slice is calculated based on the speed of transmission and the RTS to CTS delay of the modem or other network interface. The time slice should be the transmission time for four characters plus the worst case RTS to CTS delay and rounded up to the next highest hundredth of a second. In any case, the time slice should not be less than 5. If you are having trouble with a multidrop configuration, increase the time slice.

The number of nodes in a multidrop configuration is limited only by available drop numbers and by the limits of the transmission medium but the larger the network, the slower will be the throughput for a given packet.

The modem, network controller, or radio type used must be such that all units receive data transmitted by any one unit and that any unit can accept transmit data when its CTS pair is active. It is unimportant whether or not the transmit data is echoed to the transmitting CNOE-800 port.

Multidrop Mode Example

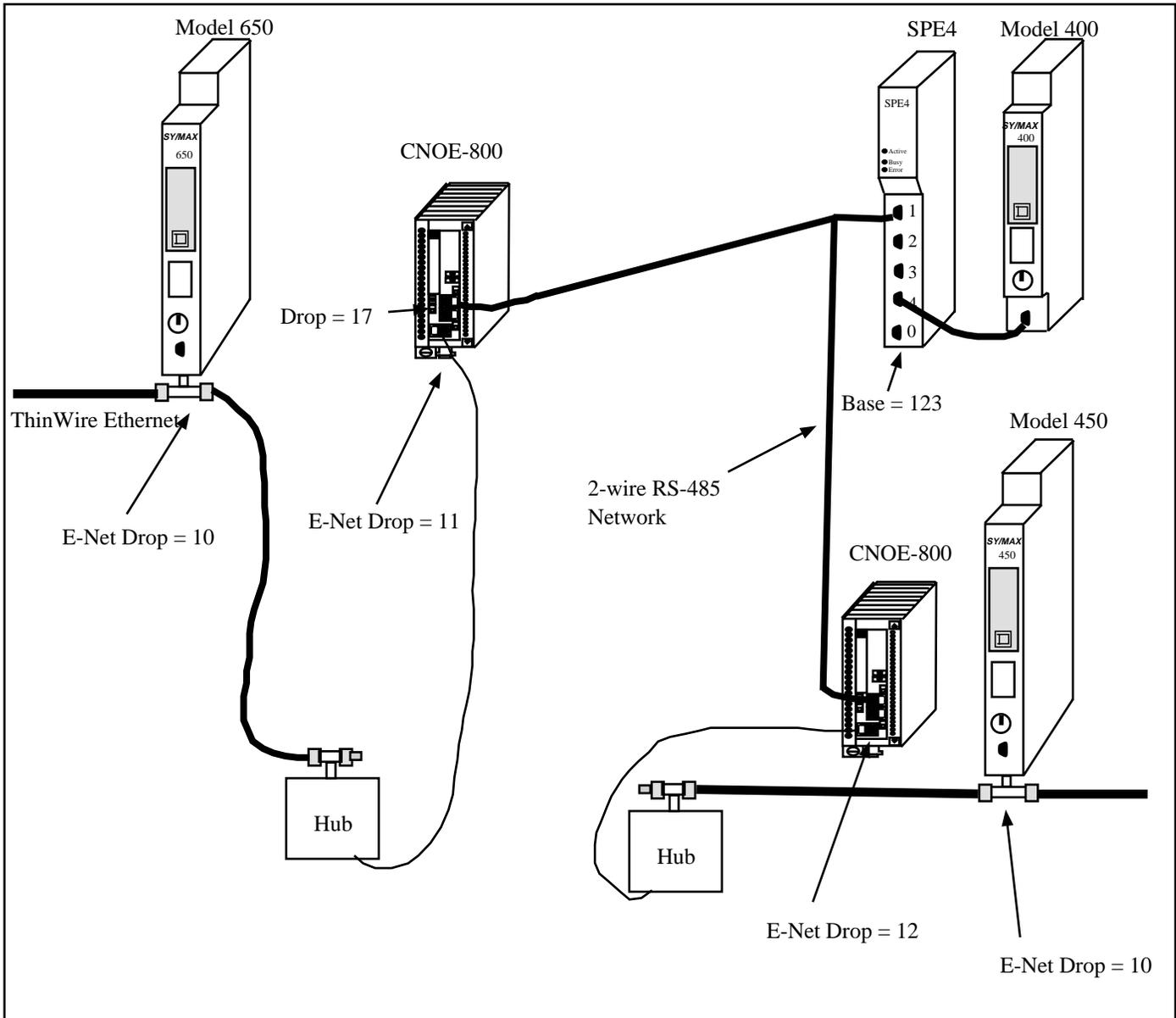


Figure 17-1 Multidrop Example

Multidrop mode is used to allow several CNOE-800s to communicate over a single medium such as a 2-wire RS-485 network. The CNOE-800 units use a time division scheme to arbitrate access to the communication system that depends upon the number of nodes and the priority of its node. When ready to broadcast, the CNOE-800 asserts RTS and waits for CTS from the modem before transmitting.

its packet. All other CNOE-800s monitor the incoming packets for their address and then route the packet accordingly.

Table 17-1 MULTIDROP Routing Examples

Origin	Target	Route
Model 650	Model 400	10, 11, 17, 124, 127
Model 650	Model 450	10, 11, 17, 19, 12, 10
Model 400	Model 650	127, 124, 17, 11, 10
Model 400	Model 450	127, 124, 19, 12, 10
Model 450	Model 650	10, 12, 19, 17, 11, 10
Model 450	Model 400	10, 12, 19, 124, 127

Table 17-2 CNOE-800 (1) Setup for MULTIDROP Connection

Port	Drop #	Mode	Baud Rate	Parity	Data	Stop	Error Check	Driver Mode
E-Net	11	SY/MAX	NA	NA	NA	NA	NA	NA
1	17	MULTIDROP	19200	None	8	1	CRC	TWO WIRE

Table 17-3 SPE4 Setup for MULTIDROP Connection

Port	Drop #	Mode	Baud Rate	Parity	Data	Stop	Error Check	Driver Mode
1	124	MULTIDROP	19200	None	8	1	CRC	TWO WIRE
4	127	SY/MAX	9600	E	8	1	BCC	NA

Table 17-4 CNOE-800 (2) Setup for MULTIDROP Connection

Port	Drop #	Mode	Baud Rate	Parity	Data	Stop	Error Check	Driver Mode
E-Net	12	SY/MAX	NA	NA	NA	NA	NA	NA
2	19	MULTIDROP	19200	None	8	1	CRC	TWO WIRE

Driver Mode

The Driver Mode setting for the MULTIDROP mode allows the control of the RS-485 transmitter and receiver. For most applications, the PT to PT mode is the proper driver mode. This mode allows full duplex operation with the transmitter enabled at all times. This can be used to drive a 4-wire multidrop network as a master.

The HALF DUPLEX mode has the transmitter enabled at all times, but the receiver is disabled while transmitting. This feature is useful for ignoring an echo from the attached device.

The TWO WIRE mode causes the transmit driver to follow CTS and the receiver to be disabled while transmitting. This mode allows the use of a 2-wire multidrop network.

RNIM Mode

The RNIM mode provides compatibility with the Square D CRM-560 RNIM. Two modes of RNIM operation are RNIM Master (Mode 12) and RNIM Slave (Mode 13). The RNIM protocol provides remote network access to SY/MAX devices using a half-duplex connection via radio/microwave/fiber optic/telephone links with the addition of a modem device. For a twisted pair RS-485 link, it is recommended that the MULTIDROP Mode be used rather than RNIM. (See page 103.) The RNIM protocol is designed for Master/Slave operation while the Multidrop protocol is intended for Peer-to-Peer communication.

The RNIM mode makes use of the RTS/CTS handshake lines in Push-to-Talk mode. The RNIM protocol may be used in conjunction with other SPE4s, EPE5s, MEBs, QUCMs, MPE3s, CRM-560s, and other RNIM compatible devices.

The RNIM protocol provides a single Master device to communicate with up to 99 Slave devices. Communication may occur through any of four mechanisms:

- Direct Master originated to Slave (NORMAL operation)
- Slave originated to Master (BID operation)
- Slave to Slave command relaying (STORE/FORWARD operation)
- Master originated broadcasting (BROADCAST operation)

Full SY/MAX message support, including all types of READs, WRITEs, and Programming is provided over the RNIM link.

NORMAL Operation

In general communication occurs by way of devices on the Master's local network sending messages routed to devices on a Slave's local network. The Master is usually located in a base station or control room and the Slaves are at the remote sites.

Under NORMAL operation, messages from the network of the Master are routed to a device on the network of a Slave. The SY/MAX route from the originator determines the exact path to the target device. In Figure 18-1, the Master RNIM is the CRM-560 and the SPE4 and CNOE-800 units are acting as Slave devices. If a PLC on the "Blue Hose" at NIM address 134 needs to read a register in the Model 400 connected to the SPE4, a route of 134, 36, 24, 27 would be used. To communicate with the Model 450, the route 134, 36, 19, 12, 10 is required.

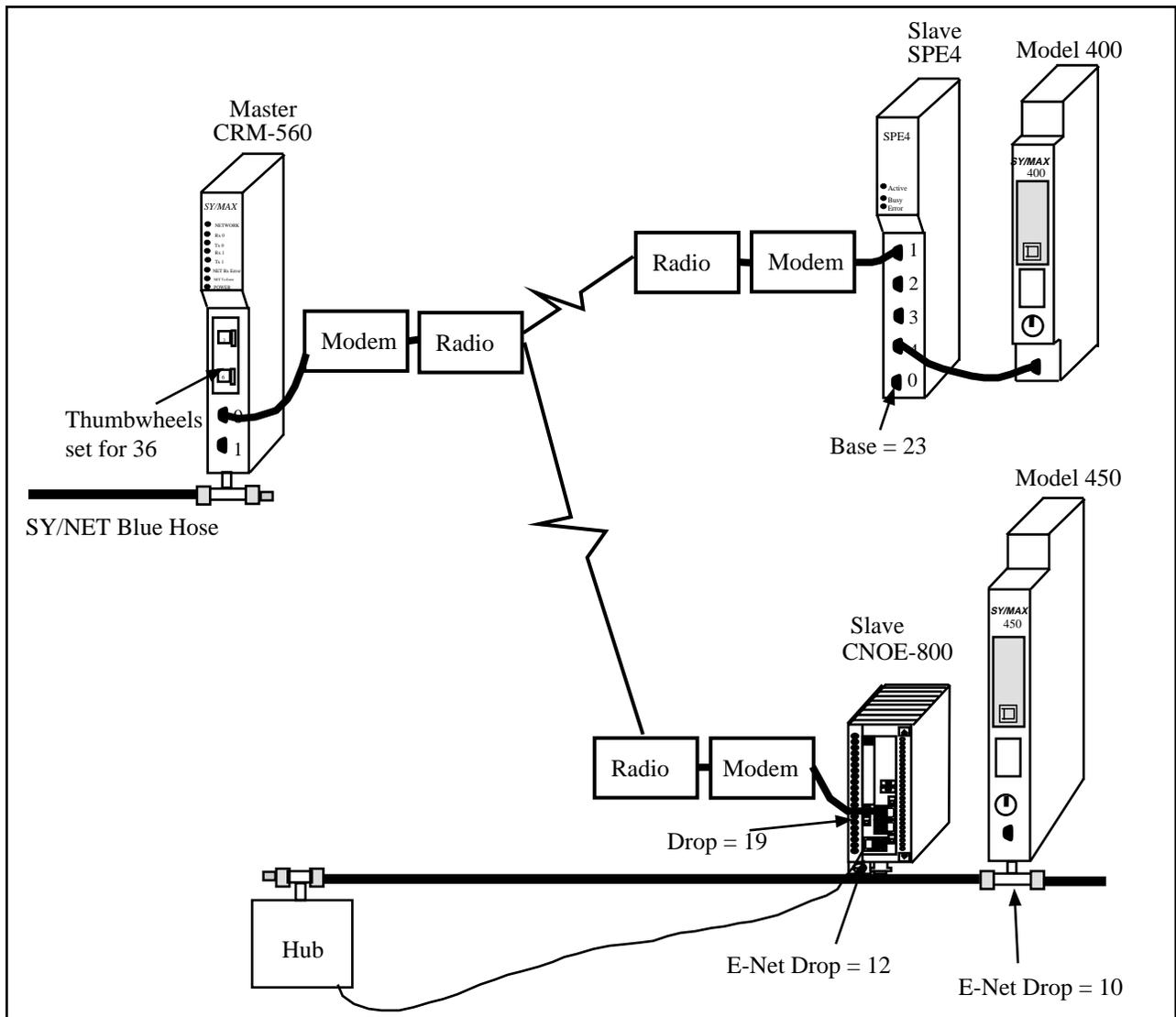


Figure 18-1 NORMAL RNIM Example

The RNIM protocol is a single-threaded half-duplex system. Single-threaded refers to the fact that only one message may be outstanding at any given time. Half-duplex refers to the fact that the transmission media only supports communication in one direction at a time. When a message arrives at the Master, it places that message in a buffer until the current message on the remote network is completed. Once the current message is complete, the new message is sent.

BID Operation

Under NORMAL operation, any device on the Master's network may communicate to any device on either Slave network. If a device on a Slave network attempts to send a message to a device on the Master's or another Slave's network, the Slave will buffer the message until a BID operation from the Master allows it to send the message.

In a BID operation, the Master temporarily releases its control of the remote network and allows individual Slaves the opportunity to transmit a stored message. A BID message is a special message sent from the Master to the Slave. The Slave has a limited amount of time to send its message.

NOTE: In the CNOE-800 RNIM Slave, this time is set by the Reply timeout setting. This time is fixed at 2 seconds in the CRM-560.

NOTE: A CRM-560 Slave will not respond to consecutive BIDs within 30 seconds of a successful BID. The CNOE-800 RNIM Slave does not include this restriction. The CNOE-800 will respond to any BID if it has a message in its Command buffer.

NOTE: The CNOE-800 Master will allow Slave to Slave automatic BIDs if the Reply timeout is large enough.

Single Slave BID Operation

When a Master BIDs a Slave, it relinquishes its control of the remote network to the slave. On a CRM-560, a BID is sent by writing the Drop number of the Slave to register 21 of the Master RNIM. On the SPE4 or CNOE-800, the drop number is written to the setup register for the RNIM Master mode port. When the Slave unit receives a BID, if it has one or more messages in its "buffer" it will transmit that message as though it is a Master. If more than one message is in the buffer, the message that has been in the buffer the longest will be transmitted. After the Slave completes its message transaction, control of the network returns to the Master.

The Slave is allowed to send only one message per BID regardless of the number of buffered messages.

If the Slave has no message to send, it simply ignores the BID and the Master will time out after 2 seconds (CRM-560 Master) or Reply timeout (CNOE-800 Master).

NOTE: To BID Slave address 00, use the BID address 100.

Automatic BID Operation (100 + n)

It is possible to automatically BID consecutive Slaves by writing the highest Slave drop number plus 100 to the BID register in the Master. The Master will BID the Slave and after a complete message cycle (or timeout), the Master will decrement the drop number by 1 and BID the next slave. This will continue for each drop number until 0 is reached. All drop numbers will be BID regardless if a Slave with that number is present on the network.

For example, if the number 134 is placed in the BID register, the Master will bid unit 34, then unit 33, 32, 31, ... 1, 0.

The BID interval setting is used to control the rate of BIDDing. The Reply timeout is used to control the time that the Master waits for a BID to be completed. The Masters timing sequence is as follows:

- 1 A value is written to the Bid address register.
- 2 A BID is sent to that address - 100.
- 3 The Master waits for the Reply timeout amount of time.
- 4 The Master waits for the BID interval amount of time. All queued NORMAL messages will be sent during the BID interval delay.
- 5 If the BID address is 100 then the automatic BID ends.
- 6 The BID address is decremented by one and flow returns to step 2.

If the Master receives a NORMAL message(s) while performing an Automatic BID, the process will be interrupted at the end of the current BID (during the BID interval) and the NORMAL message(s) will be sent. After the NORMAL message(s) is complete (or retries exhausted), the Automatic BID will be resumed.

Automatic BID Operation (200 + n)

It is possible to continuously automatically BID a single Slave by writing the Slave drop number plus 200 to the BID register in the Master. The Master will BID the Slave and after a complete message cycle (or timeout), the Master will BID the Slave again.

For example, if the number 207 is placed in the BID register, the Master will bid unit 07, then unit 07, ...

The BID interval setting is used to control the rate of BIDDing. The Reply timeout is used to control the time that the Master waits for a BID to be completed. The Masters timing sequence is as follows:

- 1 A value is written to the Bid address register.
- 2 A BID is sent to that address - 200.
- 3 The Master waits for the Reply timeout amount of time.
- 4 The Master waits for the BID interval amount of time. All queued NORMAL messages will be sent during the BID interval delay.
- 5 Flow returns to step 2.

If the Master receives a NORMAL message(s) while performing an Automatic BID, the process will be interrupted at the end of the current BID (during the BID interval) and the NORMAL message(s) will be sent. After the NORMAL message(s) is complete (or retries exhausted), the Automatic BID will be resumed.

Automatic BID Operation (300 + n)

It is possible to continuously automatically BID consecutive Slaves by writing the highest Slave drop number plus 300 to the BID register in the Master. The Master will BID the Slave and after a complete message cycle (or timeout), the Master will decrement the drop number by 1 and BID the next slave. This will continue for each drop number until 0 is reached. After the 00 Slave is BID, the BID restarts at the starting address. All drop numbers will be BID regardless if a Slave with that number is present on the network.

For example, if the number 334 is placed in the BID register, the Master will bid unit 34, then unit 33, 32, 31, ... 1, 0, 34, 33, 32, ... 1, 0, 34, 33, 32,...

The BID interval setting is used to control the rate of bidding. The Reply timeout is used to control the time that the Master waits for a BID to be completed. The Masters timing sequence is as follows:

- 1 A value is written to the Bid address register.
- 2 A BID is sent to that address - 300.
- 3 The Master waits for the Reply timeout amount of time.
- 4 The Master waits for the BID interval amount of time. All queued NORMAL messages will be sent during the BID interval delay.
- 5 If the BID address is 300 then the BID address is reset to the initial value.
- 6 The BID address is decremented by one and flow returns to step 2.

If the Master receives a NORMAL message(s) while performing an Automatic BID, the process will be interrupted at the end of the current BID (during the BID interval) and the NORMAL message(s) will be sent. After the NORMAL message(s) is complete (or retries exhausted), the Automatic BID will be resumed.

Data Store and Forward Operation

In addition to the NORMAL and BID operations, all Slave units can function as a repeater. If a Master is located where it cannot reach a Slave unit because of excessive distance or some other barrier, a Slave that is within reach of the Master and the final target Slave may be used as a repeater.

The STORE and FORWARD feature of the RNIM Slave is used by simply including the drop number of the repeater Slave plus 100 in the route.

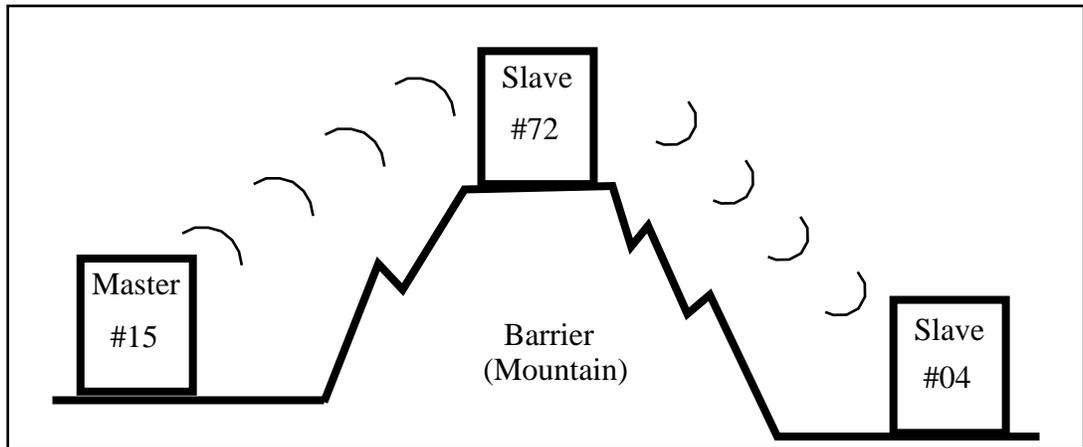


Figure 18-2 RNIM Repeater Example

Figure 18-2 displays an RNIM Master (15) on one side of a mountain, a Slave (04) on the other side of the mountain, and a Slave (72) at the top that can communicate with the other two. If a source on the Master's network (16) wants to send a READ to a PLC (87) on the Slave's network on the other side of the mountain, the route would be: 16, 15, 172, 4, 87.

The repeater unit can still function as a normal Slave if it is the target of the route. For instance, if the same source targets a PLC (21) on the network of the Slave at the top of the mountain, the route would be: 16, 15, 72, 21.

NOTE: It is not possible to perform an indirect BID using the STORE and FORWARD feature of an intermediate Slave.

Broadcast Operation

Due to physical differences between the Square D CRM-560 and QUCM, the Broadcast Operation implementation varies. The CNOE-800 RNIM Slave will respond equally to either the even or odd Broadcast message that correspond to Table 18-1 and this response will be acting upon the internal registers within the CNOE-800.

Table 18-1 Broadcast Route Values

	Slave Drop #	CRM-560 Slave Port	CNOE-800 Response	Broadcast Route Value
General Broadcast	00-99	#1	Internal	254
		Twin-ax	Internal	253
Partial Broadcast	90-99	#1	Internal	252
		Twin-ax	Internal	251
	80-89	#1	Internal	250
		Twin-ax	Internal	249
	70-79	#1	Internal	248
		Twin-ax	Internal	247
	60-69	#1	Internal	246
		Twin-ax	Internal	245
	50-59	#1	Internal	244
		Twin-ax	Internal	243
	40-49	#1	Internal	242
	Twin-ax	Internal	241	
30-39	#1	Internal	240	
	Twin-ax	Internal	239	
20-29	#1	Internal	238	
	Twin-ax	Internal	237	
10-19	#1	Internal	236	
	Twin-ax	Internal	235	
00-09	#1	Internal	234	
	Twin-ax	Internal	233	

If it is desired to route a broadcast message to all CNOE-800 RNIM Slaves with Drop numbers in the fifties and send a broadcast message our all of the other SY/MAX mode ports on the CNOE-800, simply use the route number 244 in the position normally held by the Slave address and 254 for the last drop in the route.

Mode 12: RNIM Master

Several operational parameters of the RNIM Master in the CNOE-800 are adjustable. Table 18-2 displays the control registers in the CNOE-800 and the equivalent registers in the Square D CRM-560. The CNOE-800 retains the previous setup parameters upon power-up while the CRM-560 always returns to the factory default settings.

It is important that the Master and all Slave units on the same network be set for the same parameter values. If CRM-560s are included in the network, it is important to note that the BID response timeout is fixed at two seconds in the CRM-560 while it is adjustable in the CNOE-800.

Bit 9 of the Options register for a RNIM Master controls the Enable of the Master. If this bit is set (on), the RNIM Master is disabled. This allows multiple Masters to be connected to the Remote Network for redundancy.

Table 18-2 RNIM Master Register Summary

CRM-560 Register	SPE4/CNOE-800 Register				Description	Notes
	Port 1	Port 2	Port 3	Port 4		
18	8041	8073	8105	8137	Identification number.	Must be the same for all RNIMs on the same network. CRM-560 defaults to 0 on power-up.
19	8042	8074	8106	8138	Clear to Send (CTS) Delay (10mS units)	CRM-560 defaults to 500mS on power-up.
20	8043	8075	8107	8139	Message Response timeout (10mS units)	CRM-650 defaults to 20 seconds on power-up. The QUCM also uses this value as the BID timeout.
21	8044	8076	8108	8140	BID address number	00 to 99 Single BID. 100 to 199 Automatic BIDs. 200 to 299 Continuous Single BIDs 300 to 399 Continuous Automatic BIDs.
22	8045	8077	8109	8141	Number of Retries (when no ACK received)	CRM-560 defaults to 3 on power-up.
23	8062	8094	8126	8158	Master Disable	Set bit 9 in the SPE4/CNOE-800 options register to disable the Master. Set the CRM-560 register to decimal 123 to disable the Master.
25	8058	8090	8123	8155	Pause Time (10mS units)	CRM-560 defaults to 15 seconds on power-up.
26	8059	8091	8124	8156	Message Count (between Pause Time)	CRM-560 defaults to 4 on power-up.
NA	8060	8092	8125	8157	BID Reply Interval	This value determines the amount of time between successive automatic BIDs.
NA	2103	2135	2167	2199	Number of messages in Command Buffer	Read Only Statistic that displays the number of queued messages waiting in the Command buffer.

Mode 13: RNIM Slave

Several operational parameters of the RNIM Master in the CNOE-800 are adjustable. Table 18-3 displays the control registers in the CNOE-800 and the equivalent registers in the Square D CRM-560. The CNOE-800 retains the previous setup parameters upon power-up while the CRM-560 always returns to the factory default settings.

It is important that the Master and all Slave units on the same network be set for the same parameter values. If CRM-560s are included in the network, it is important to note that the BID response timeout is fixed at two seconds in the CRM-560 while it is adjustable in the CNOE-800.

Bit 9 of the Options Register for a RNIM Slave allows the Command Buffer to be cleared. Set this bit to clear the queued messages. Clear this bit to resume normal operation. The Number of Queued Messages statistic register may be used to determine the number of messages in the Command Buffer.

Table 18-3 RNIM Slave Register Summary

CRM-560 Register	SPE4/CNOE-800 Register				Description	Notes
	Port 1	Port 2	Port 3	Port 4		
18	8041	8073	8105	8137	Identification number.	Must be the same for all RNIMs on the same network. CRM-560 defaults to 0 on power-up.
19	8042	8074	8106	8138	Clear to Send (CTS) Delay (10mS units)	CRM-560 defaults to 500mS on power-up.
20	8043	8075	8107	8139	Message Response timeout (10mS units)	CRM-650 defaults to 20 seconds on power-up. The EPE5 also uses this value for the BID timeout.
24	8062	8094	8126	8158	Clear Command Buffer	Set bit 9 in the SPE4/CNOE-800 options register to clear the Command buffer. Set the CRM-560 register to decimal 210 to remove stored commands from the buffer.
NA	2103	2135	2167	2199	Number of messages in Command Buffer	Read Only Statistic that displays the number of queued messages waiting in the Command buffer.

Driver Mode

Pt to Pt

RNIM Master and Slave modes on ports 1 and 2 offer the ability to operate on RS-485 networks in 4-wire and 2-wire modes. When the port is set to Pt to Pt it is in its normal RS-422 mode for point to point operation. This is the default state for the module and it is the only state available on the RS-232 ports. In Pt to Pt mode, the RS-485 transmit drivers are always enabled. Choose Pt to Pt when the Multidrop port is the master on a 4-wire multidrop network.

Half Duplex

RNIM Master and Slave modes on ports 1 and 2 offers the ability to operate on RS-485 networks in 4-wire and 2-wire modes. Half Duplex mode allows the port to ignore any echo that may be returned from the attached device. The Half Duplex mode is the same as the Pt to Pt mode with the exception that the receiver is disabled when the unit is transmitting. The transmit drivers are always enabled.

NOTE: It is recommended that the Half Duplex mode be used with RNIM Multidrop networks such as when the RM14K is being used.

Two Wire

RNIM Master and Slave modes on ports 1 and 2 offers the ability to operate on RS-485 networks in 4-wire and 2-wire modes. Two wire setting allows the port to operate on a 2-wire RS-485 peer-to-peer network. The transmit driver is normally tri-stated and is dependent upon the state of CTS. The receiver is disabled when the transmitter is enabled. The two wire setting sets bits 7 and 8 of the options register for that port.

RTS/CTS Operation

It is important to note that the RTS/CTS operation of the CNOE-800 RNIM is slightly different than that of the CRM-560. If CTS is not present at the end of the CTS delay, the CRM-560 will post an error message to the originator, while the CNOE-800 will wait for the attached device to assert CTS. This true handshaking feature of the CNOE-800 allows the CTS delay setting to be set to the smallest allowable time for the best throughput while allowing a longer than normal handshake response if required. The CRM-560 must be set to the largest delay possible to avoid excessive timeout errors.

The CNOE-800 handshake sequence is as follows:

- 1 The CNOE-800 asserts the Request to Send (RTS) signal when it has data to send.
- 2 The CNOE-800 will wait for the CTS delay time and for CTS to be asserted before it will send the data. If the CTS delay time is set for zero, the CNOE-800 will just wait for CTS to be asserted.

Transfer Mode

The Transfer mode allows re-routing of SY/MAX messages to the Primary PLC in a redundant system. This feature may be used for re-directing messages through any port but is most useful for Ethernet devices.

NOTE: The Transfer mode is available only on the two serial ports. When a port is in Transfer mode, the actual serial port is disabled and may not be used for external communication.

Incoming command messages routed to the Transfer port have their routes modified by the addition of the Transfer Route to the end of route. The message is then re-routed to the destination directed by the Transfer Route. Reply messages from the destination target have the Transfer Route removed as they are routed through the Transfer port and are then sent back to the original source. The Transfer Route is stored in the Auto-Transfer Route configuration registers for the appropriate serial port.

The "On Ethernet" feature may be used to reduce the number of drops needed in the route.

Transfer Example

Figure 19-1 displays a pair of Model 650 PLCs in a Hot-Backup system, an CNOE-800, and a computer acting as an operator interface. The Model 650s are controlling a critical system and one is the Primary running the system. The other Model 650 is the Secondary (Standby) unit and upon failure of a component in the Primary, it assumes control and becomes the new Primary.

This oscillation of the Primary usually spells trouble for the Operator Interface (OI). The Model 650's E-net address is fixed by dip switches and it is not able to modify it while running. Therefore, the OI must continuously decide which PLC is the Primary by polling additional registers in the PLC and switch between the two E-net addresses on the transfer of control.

With the Transfer mode in the CNOE-800, it is possible to set up the OI (and other devices on the network) to poll a single E-net drop and have the CNOE-800 redirect the messages to the Primary. The OI doesn't care which PLC is the Primary, it always sends its messages to the CNOE-800.

When the transfer occurs the new Primary sends a TWRITE to the CNOE-800 to change the "Transfer Route" within the CNOE-800 to point to its E-net address.

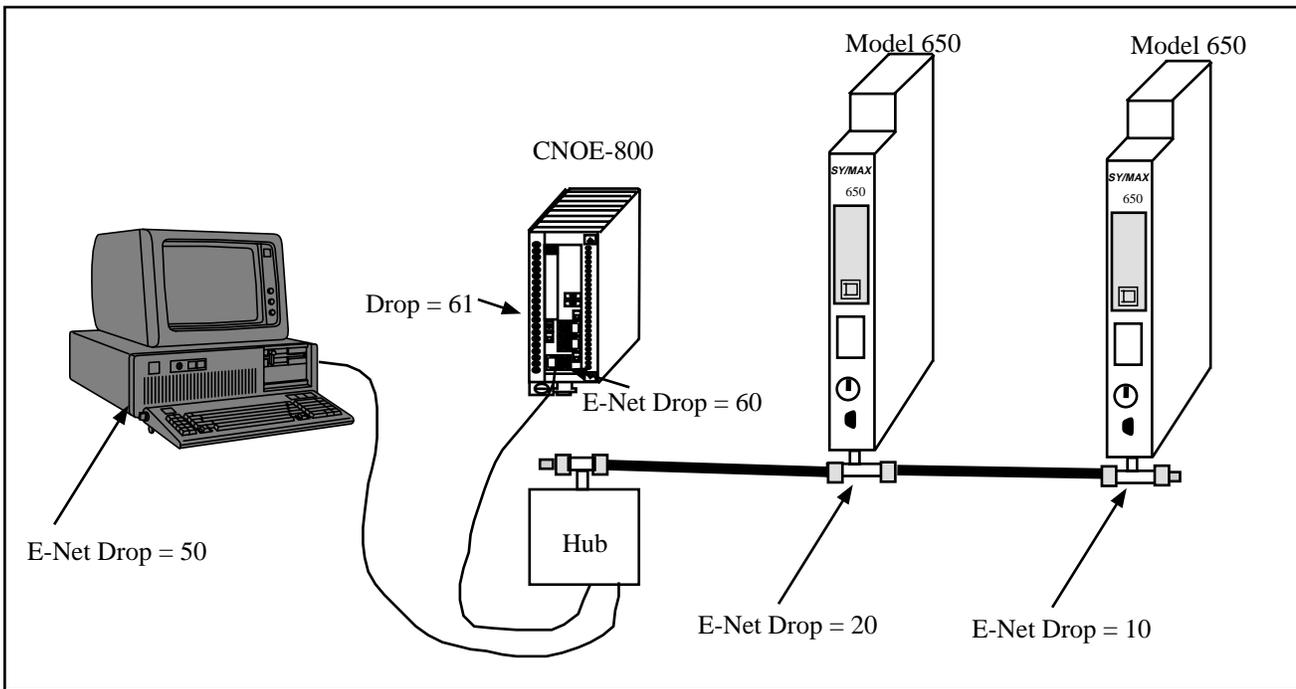


Figure 19-1 Transfer Example 1

The CNOE-800 Port 1 is set for TRANSFER protocol. The "On Ethernet" feature is set to NO. The Transfer Route will be set to 60, 20 when the left Model 650 is Primary and 60, 10 when the right 650 is Primary. The route from the OI will always be 50, 60, 61 to reach the Primary.

The Transfer Route for Port 1 is stored in registers 8046 through 8054 in the CNOE-800. Register 8046 contains the number of drops in the route to the Primary from the Transfer port. The registers following contain the 8 drops of the route.

Table 19-1 Transfer Route Registers

CNOE-800 Register	Description	Settings for 20 as Primary	Settings for 10 as Primary
8046	# of drops in route	2	2
8047	Drop 1	60	60
8048	Drop 2	20	10
8049	Drop 3	0	0
8050	Drop 4	0	0
8051	Drop 5	0	0
8052	Drop 6	0	0
8053	Drop 7	0	0
8054	Drop 8	0	0

When the hot-backup transfer occurs and the old Secondary becomes the new Primary, the new Primary writes its own Ethernet address to CNOE-800 register 8048. It is usually important to write the application in a redundant system such that both PLCs run the exact same program. Register 8093 in the Model 650 contains the 650's Ethernet drop number.

NOTE: The value in CNOE-800 register 8046 sets the number of drops in the Transfer Route for Port 2. Since it is set to 2 in this example, it doesn't matter what the values are in registers 8049 through 8054.

PLC Ladder Rungs

Both Model 650s could have the following ladder rungs in their programs to perform the communications switch.

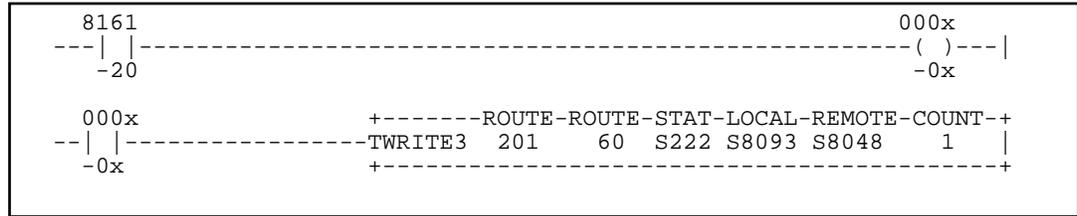


Figure 19-2 Transfer Communication Rungs

As the backup PLC assumes the role of Primary, status bit 8161-20 is set to 1 (ON) by the LTI. This energizes coil 000x-0x. Upon scanning this contact in rung 2, the TWRITE is executed. The first drop in the route is set to the special "don't care" drop number 201. The second drop in the route is set for the QUCM's E-net port, 60. The STAT register is a unique communication status register within the PLC. The LOCAL register contains the Ethernet SY/MAX drop number of the PLC. The REMOTE register is the target in the CNOE-800 for the write. And finally, the COUNT is set to 1 because only one register needs to be sent.

With the use of the 201 route and registers 8093, the above rungs become generic and may be used in both PLCs.

CAUTION

Do not attempt to program the Primary PLC through the Transfer route. A system transfer could occur during the program load and cause the program to load incorrectly. Programming should always be performed directly to the PLC's E-net address.

"On Ethernet" Example

The above example could be changed to use the "On Ethernet" feature of the Transfer port to reduce the number of drops in the routing. The following changes would take place:

- The "On Ethernet" option would be set to YES for Port 1 of the CNOE-800.
- The value in R[8046] would need to be changed to 1 since there will only be one drop in the Transfer Route.
- The remote register in the ladder logic TWRITE would now need to be 8047 to place the target Model 650 address in the first drop of the Transfer Route.
- The Route from the OI is now simply 50, 61.
- Extra care must be used to avoid setting one of the drop numbers of a port in the CNOE-800 to a potential target of the Transfer Route to avoid routing errors.

Chevron Mode

The Chevron mode is a combination of the RNIM Master and Modbus Gate modes to allow the integration of remote SY/MAX and Modbus devices on the same multidrop (RS-485, modem, or radio) network. Incoming messages with the drop number following the Chevron Port's drop number within the range of 0 through 99 are sent out as RNIM packets. Messages with the following drop in the range of 100 through 199 are sent out as Modbus RTU packets where the Modbus slave address is the drop number minus 100.

All SY/MAX messages are supported through the RNIM message structure including PLC programming. Also, all Modbus RTU messages are supported including PLC programming. All RNIM Slave devices may be used in a Chevron network including CRM-560 RNIMs, SPE4s, EPE5s, CNOE-800s, and MEBs. Any Modbus RTU slave device with active RTS/CTS handshaking (or multidrop RS-485 ports) may also be used in a Chevron network as a Slave.

NOTE: The POWERLOGIC PNIM protocol supported by most POWERLOGIC equipment is a subset of the RNIM protocol and thus the CHEVRON mode may be used to integrate POWERLOGIC and MODBUS equipment on the same RS-485 network. Simply set the NETWORK ID to 0 and set the CTS DELAY to 0.

The following restrictions apply to the Chevron mode:

- All devices (RNIM and Modbus) must operate with the same serial parameters. Typically this will be 9600 baud, 8 data bits, 1 stop bit, and EVEN parity.
- All Modbus Slave PLCs must not be in "Bridge" mode if they are also on a Modbus Plus network. The Slave devices must not respond to Modbus messages that are not targeted to their address. PLCs in Bridge mode pass messages onto the Modbus Plus network which may result in multiple replies from different units and/or error replies from non-existent units.
- Modbus address 16 decimal (10 hex) may not be used. It is possible that unit 16 would try to respond to the RNIM messages.
- RNIM repeater features are not allowed. Drop numbers greater than 100 will be sent as Modbus RTU messages and not RNIM repeater routes.
- The Chevron port operates as a Modbus Gate mode master only. The port will not accept messages as a Modbus Slave.
- The values for the CTS timer, Pause Time, and Message Count are used for both Modbus and RNIM messages.
- The Modbus messages do not retry if a response is not received before the Reply Timeout. RNIM messages follow the normal retry mechanism of the standard RNIM Master.
- Like a normal RNIM network, all RNIM devices must use the same Network ID.
- RNIM BIDDing and automatic BIDDing is permitted and operates like a normal RNIM Master port.

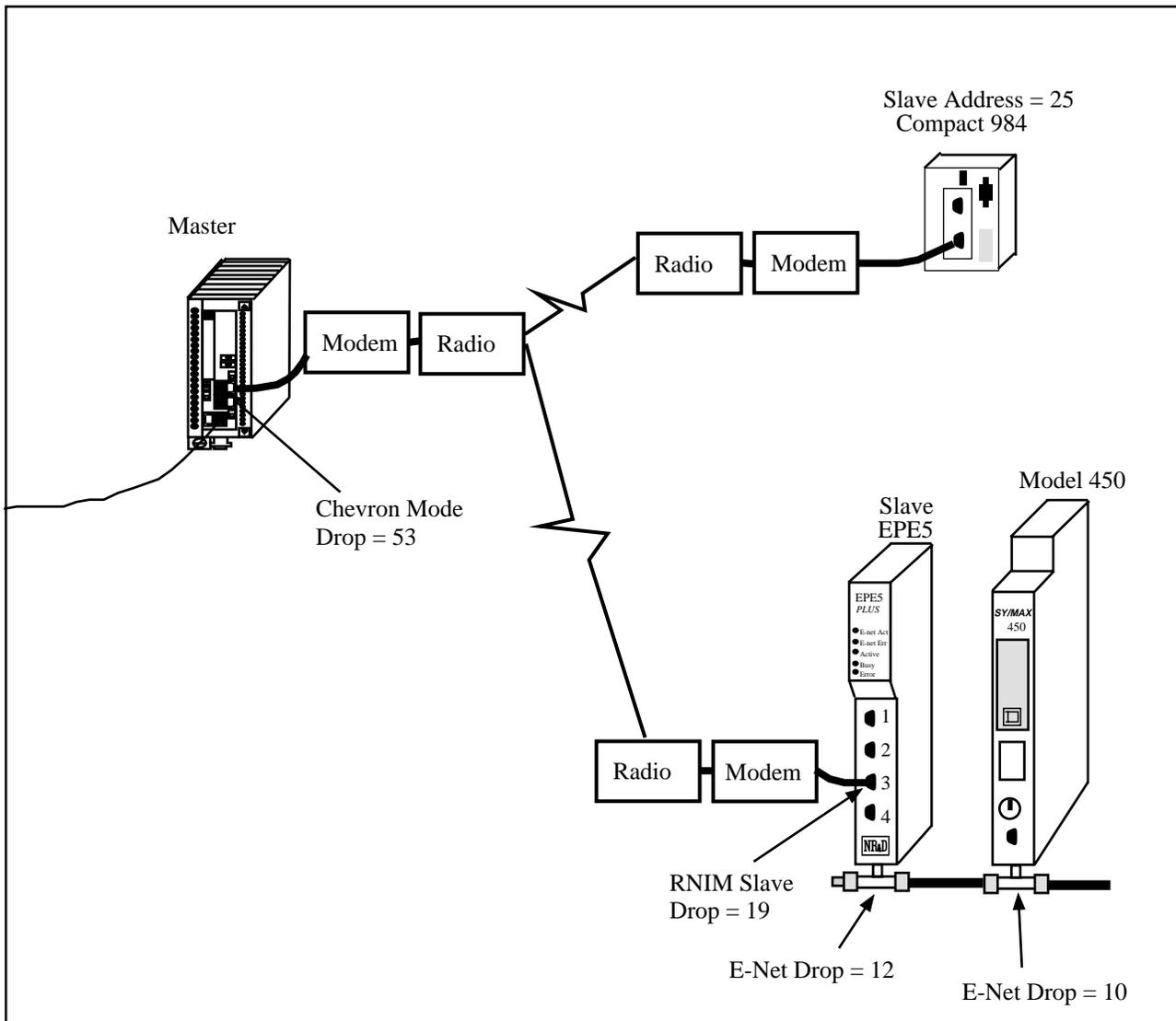


Figure 20-1 Chevron Radio Example

An example application of the Chevron mode is displayed in Figure 20-1. The Master CNOE-800 on the left has Port 2 in Chevron mode with a drop number of 53. This port is connected via radio modems to an EPE5 and a Compact 984 PLC. The remote EPE5 has its Port 3 set for RNIM Slave with a drop number of 19. The Compact 984 is configured for RTU mode with an address of 25.

To route to the Model 450, the portion of the route from the Master CNOE-800 would be:

..., 53, 19, 12, 10

while the route to the Compact 984 from the Master CNOE-800 would be:

..., 53, 125

Notice that the Modbus device was accessed by adding 100 to its slave address.

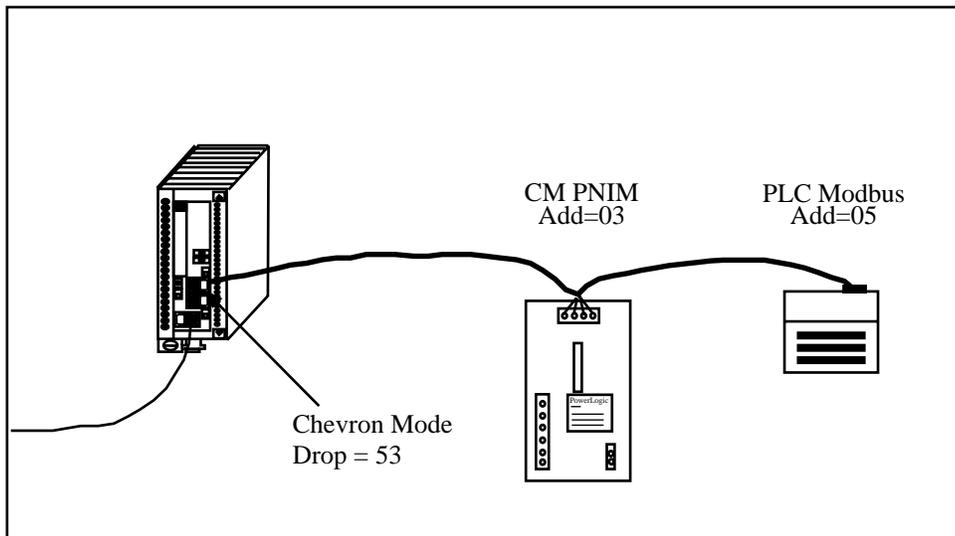


Figure 20-2 Chevron POWERLOGIC Example

An example application of the Chevron mode is displayed in Figure 20-2. The CNOE-800 has Port 2 in Chevron mode with a drop number of 53. This port is wired with a 4-wire RS-485 cable to a POWERLOGIC Circuit Monitor and a Momentum PLC. The CM is configured for PNIM Address 03 while the PLC is at Modbus RTU Address 05. All three devices are configured for the same baud rate, paritye, data bits, and stop bits (9600,EVEN,8,1). The PLC has its 9-pin port configured for RS-485.

The setup for the CHEVRON port is as follows:

Table 20-1 POWERLOGIC CHEVRON Example

Setting	Value
Drop	53
On Ethernet	NO
Protocol	CHEVRON
Baud Rate	9600
Parity	EVEN
Data Bits	8
Stop Bits	1
Buffer Limit	16
Driver Mode	PT TO PT
Network ID	0
CTS Timer	0
Reply Timeout	200
Bid Interval	0
Attempts	1
Pause Time	0
Message Count	0
Bid Address	0

To route to the CM, the portion of the route from the Master CNOE-800 would be:
 ..., 53, 03

while the route to the Momentum PLC from the Master CNOE-800 would be:
..., 53, 105

Notice that the Modbus device was accessed by adding 100 to its slave address.

Dual Slave Mode

The Dual Slave mode is a combination of the Modbus Gate and SY/MAX modes to allow a single-threaded master connected to the port to use either Modbus RTU or SY/MAX to route through the port. This mode is most useful with POWERLOGIC's SMS's "SY/MAX to NIM/PNIM" serial driver, since it will route messages targeted to both POWERLOGIC and MODBUS devices through a single communications port. This mode is also useful when a single connection from a computer is needed for running both SY/MAX and Modicon PLC programming softwares at different times.

There are a few limitations imposed by the Dual Slave Mode:

- The device attached to the port must be the communication Master; it must initiate the communication.
- The connected Master must only issue one message at a time. SY/MAX messages will eventually return either a data reply or an error reply and the Master should wait for that reply. Modbus messages may or may not receive a reply and the Master should wait an appropriate amount of time before generating the next query.
- SY/MAX messages are routed just like a normal SY/MAX port. The first drop in the route should be either the drop number of Dual Mode port or the special "Don't Care" drop of 201. No route will result in local access of the Module.
- The Modbus Routing table is used for routing the Modbus messages just like in Modbus Gate mode. A drop number of 255 will always result in local access of the Module.
- Modbus Slave address 16 (decimal) and 254 (decimal) are not supported and should not be used in the Modbus Routing Table.

SMS Example

POWERLOGIC System Manager Software supports Modbus RTU devices as well as SY/MAX (POWERLOGIC Compatible) devices. When both Modbus and SY/MAX devices are configured within SMS to use the same serial communications port of the PC, SMS will send both the SY/MAX and Modbus messages out the serial port even if the port is configured only for SY/MAX mode. The Dual Mode now allows the CNOE-800 to accept both types of messages on a single serial connection.

NOTE: The "Communications Wiring" setting within SMS must be set for "SyMax to NIM/PNIM" Do not choose "PowerLogic/Modbus/Jbus (4-Wire)" because the SY/MAX routing will not work.

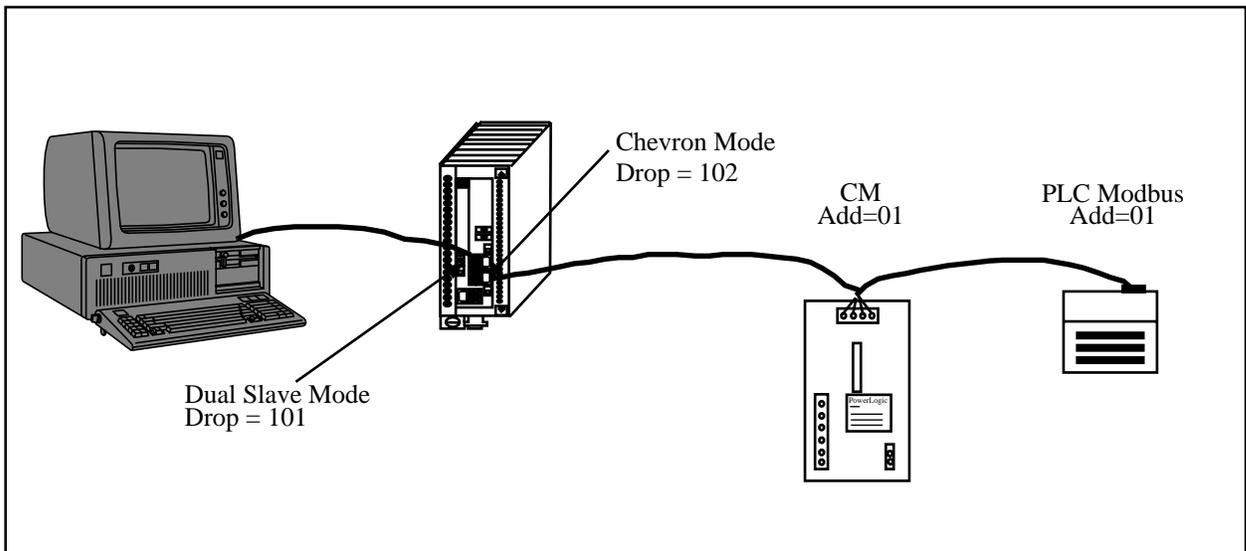


Figure 21-1 Dual Slave SMS Example

An example application of the Dual Slave mode is displayed in Figure 21-1. The CNOE-800 has Port 1 in Dual Slave Mode with the SMS computer connected through an NR&D MM1 cable. Port 2 is in Chevron mode with a Circuit Monitor and a Momentum PLC.

Table 21-1 POWERLOGIC Example DUAL SLAVE Port

Setting	Value
Drop	101
On Ethernet	NO
Protocol	DUAL SLAVE
Baud Rate	9600
Parity	EVEN
Data Bits	8
Stop Blts	1
Buffer Limit	16

Table 21-2 POWERLOGIC Example DUAL SLAVE Port Modbus Routing

ADDR	DEVICE	ROUTE
1	MODBUS	101,102,101

Table 21-3 POWERLOGIC Example CHEVRON Port

Setting	Value
Drop	102
On Ethernet	NO
Protocol	CHEVRON
Baud Rate	9600
Parity	EVEN
Data Bits	8
Stop Blts	1
Buffer Limit	16
Driver Mode	PT TO PT
Network ID	0
CTS Timer	0
Reply Timeout	200
Bid Interval	0
Attempts	1
Pause Time	0
Message Count	0
Bid Address	0

Table 21-4 POWERLOGIC Example SMS Communications Connection - Serial

Setting	Value
Connection Name	Com1
Communications WIring	SyMax to NIM/PNIM
Parity	Even
Using Modem	NO (Not Checked)
Serial Port	COM1
Baud Rate	9600
Attempts	2
Timeout	5000mS
Network Address	30

Table 21-5 POWERLOGIC Example SMS Setup Devices/Routing

Setting	CM 1 on Port 2	PLC 1 on Port 2
Device	CM_1	MOM_1
Connection Name	Com1	Com1
Protocol	PowerLogic	Modbus
Phone Number		
RT 1	30	30
RT 2t	101	1
RT 3	102	
RT 4	1	
RT 5		
Rt 6		
RT 7		
RT 8		

PLC Programming Example

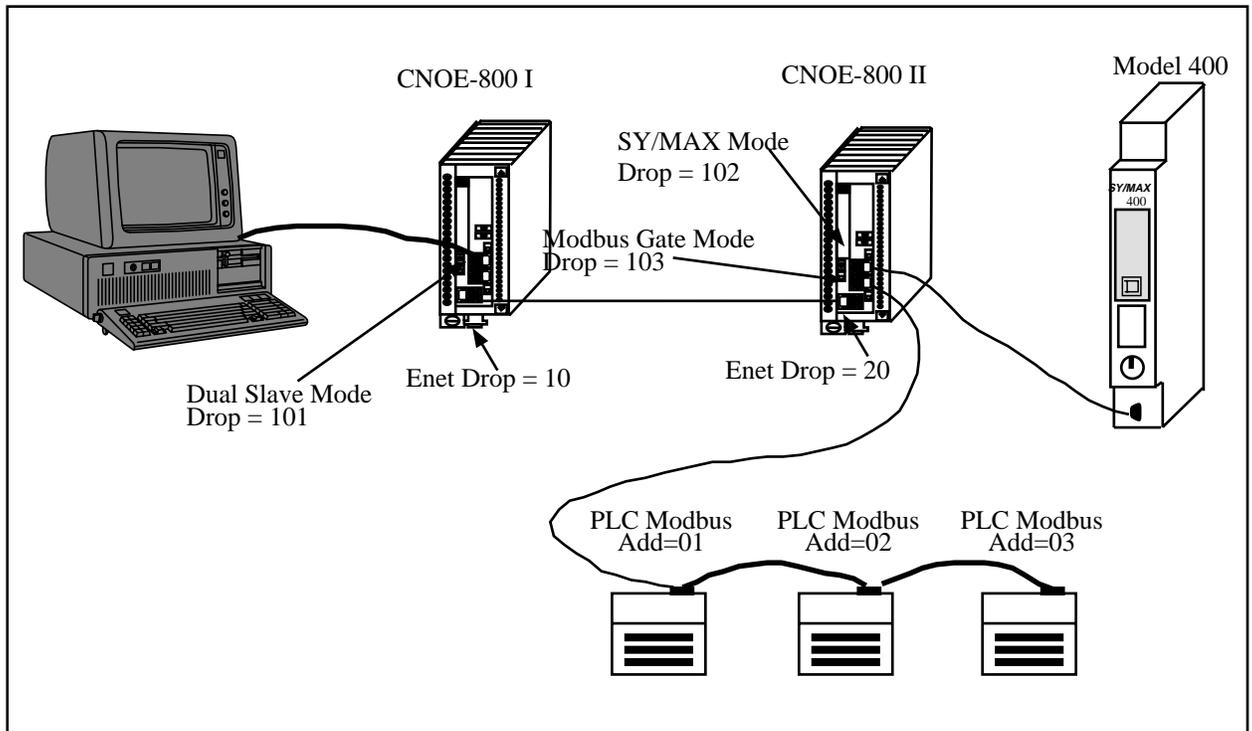


Figure 21-2 Dual Slave PLC Programming Example

Another example application of the Dual Slave mode is displayed in Figure 21-2. CNOE-800 I has Port 1 in Dual Slave Mode with the PLC Programming computer connected through an NR&D MM1 cable. Both CNOE-800s' Enet ports are set for SY/MAX 802.3. CNOE-800 II Port 1 is in SY/MAX mode with a Model 400 PLC. Port 2 is in Modbus Gate Mode with three Momentum PLCs. This setup allows the computer to run either the SY/MATE programming software or a Modicon programming software (Modsoft, ProWorks, Concept) without changing the cabling or CNOE-800 port setup.

Table 21-6 PLC Programming Example DUAL SLAVE Port

Setting	Value
Drop	101
On Ethernet	NO
Protocol	DUAL SLAVE
Baud Rate	9600
Parity	EVEN
Data Bits	8
Stop Bits	1
Buffer Limit	16

Table 21-7 PLC Programming Example DUAL SLAVE Port Modbus Routing

ADDR	DEVICE	ROUTE
1	MODBUS	101,10,20,103,1
2	MODBUS	101,10,20,103,2
3	MODBUS	101,10,20,103,3

Table 21-8 PLC Programming Example SY/MAX and Modbus Gate Ports

Setting	Port 1 Value	Port 2 Value
Drop	102	103
On Ethernet	NO	NO
Protocol	SY/MAX	MODBUS GATE
Baud Rate	9600	9600
Parity	EVEN	EVEN
Data Bits	8	8
Stop Blts	1	1
Buffer Limit	16	16
Error Check	BCC	N/A
Route Appendix	NONE	N/A
Route Replacement	OFF	N/A
Driver Mode	N/A	PT TO PT
Reply Timeout	N/A	200
Transfer Interval	0	0
Transfer Route	NONE	NONE
Read Count	0	0
Read From	0	0
Read To	0	0
Write Count	0	0
Write From	0	0
Write To	0	0

Table 21-9 PLC Programming Example SY/MATE Settings

Setting	Value
Comm. Device	COM1
Resp. Time (sec)	003
Retries	03
Route	101 10 20 102
ASCII ID	
Baud Rate	9600
Parity	EVEN
Error Checking	BCC

Table 21-10 PLC Programming Example Modsoft Settings

Setting	PLC 1	PLC 2	PLC 3
Address	1	2	3
Protocol	Modbus I	Modbus I	Modbus I
Mode	RTU	RTU	RTU
Data Bits	8	8	8
Parity	EVEN	EVEN	EVEN
Stop Bits	1	1	1
Baud	9600	9600	9600
Device	COM1	COM1	COM1

Auto-transfer and Auto-Scan

The CNOE-800 has the ability to originate READ and WRITE messages on a timed interval using the Auto-transfer and Auto-Scan features. The READ messages move information from an external device to the CNOE-800's internal mailbox registers. The WRITE messages move information from the CNOE-800's mailbox registers to an external device.

NOTE: These two features, as well as the Ethernet I/O Scanner, are only useful when the CNOE-800 is being used as an I/O module.

Auto-Transfer

The Auto-transfer is available on the serial ports in the following protocol modes: SY/MAX, NET-to-NET, IDEC, Modbus Host, Modbus Gate, Modbus ASCII, PLOGIC, and PNIM. The use of Auto-transfer in Modbus modes implies that the CNOE-800 port is the Master. The Auto-transfer feature is available on the Ethernet port as long as the E-PEER feature is disabled.

The Auto-transfer has the ability to perform a single READ and/or WRITE with a single fixed route to the target device on a timed interval. Adjustable parameters include:

- **Transfer Interval** - This value sets the amount of time between successive messages in 10mS units. If only READs or only WRITEs are enabled, this interval determines the amount of time between the sending of each messages. If both READs and WRITEs are enabled, the READs and WRITEs are alternated. For example if both READs and WRITEs are enabled and the Transfer Interval is set to 100, then a READ will be sent, one second later a WRITE will be sent, one second later a READ will be sent...etc.

The Transfer Interval should be set to a large enough number to allow a message to be sent and the response to be received before the next message is sent. If the Transfer Interval time has expired and the reply from a previous poll has not been received, that CNOE-800 port will insert a delay of two seconds before the next transfer. It is good practice to allow for at least three times the actual transmission time of the command and reply message for retries and additional network traffic. A Transfer Interval of zero (0) will disable the Auto-transfer.

- **Transfer Route** - The Transfer Route determines the path to the target device. The first drop in the route is usually the drop number of the Auto-transfer port. Additional drops are used to point to the specific target. For example, if a PNIM port has a drop number of 125 and the target of the Auto-transfer is Circuit Monitor 4 then the route would be 125,004.
- **READ Count** - The READ Count determines the number of registers returned by the READ. The maximum Count is 128 for SY/MAX messages. A setting of zero (0) disables the Auto-transfer READ.
- **READ From** - The READ From value is the starting register for the read in the remote device.
- **READ To** - The READ To value is the starting register for where the data from the external device is placed in the CNOE-800's mailbox registers. This value must be within the range of 1 through 2048.
- **WRITE Count** - The WRITE Count value is the number of registers transferred from the CNOE-800's Mailbox registers to the external device. The valid range is 0 through 128 where 0 disables the WRITE transfer.

- **WRITE From** - The **WRITE From** value is the starting register in the CNOE-800's Mailbox from which the data is sent to the external device.
- **WRITE To** - This value is the starting point in the external device where the data is written.

Auto-Scan

The Auto-Scan is an enhancement of the Auto-transfer feature to allow up to 48 independent READs or WRITES to be operated on external devices. Each serial port on the CNOE-800 includes its own Auto-Scan table. The Auto-Scan feature is available on the Ethernet port. via the Ethernet I/O scanner Each entry in the Auto-Scan table is configured for its own local, remote, count, read or write type, and route parameters.

- **TRANSFER INTERVAL** - This value sets the amount of time between successive non-empty messages in 10mS units. The Transfer Interval should be set to a large enough number to allow a message to be sent and the response to be received before the next message is sent. If the Transfer Interval time has expired and the reply from a previous poll has not been received, that CNOE-800 port will insert a delay of two seconds before the next transfer. It is good practice to allow for at least three times the actual transmission time of the command and reply message for retries and additional network traffic. A Transfer Interval of zero (0) will disable the entire Auto-Scan table.
- **LOCAL** - The local value is a pointer to a register in the CNOE-800's mailbox. On READ operations, this register is the starting register where the data from the external device is placed upon completion of the read. On WRITE operations, this is the starting point of the data from the CNOE-800 to the external device. The valid range of this parameter is 1 through 32, and 65 through 2048. A setting of zero will disable an individual Auto-Scan entry.
- **REMOTE** - The remote value is a pointer to a register in the external device. On READ operations, this is the starting register in the remote device. On WRITE operations, this is the starting register for the data from the CNOE-800. The valid range of this parameter is 1 through 65535. A setting of zero will disable an individual Auto-Scan entry.
- **COUNT** - The count value determines the number of registers to be included in the READ or WRITE. The valid range is normally 1 through 128. A setting of zero will disable an individual Auto-Scan entry.
- **DIRECTION** - The direction determines whether the operation will be a READ (from the external device to the Mailbox) or a WRITE (from the Mailbox to the external device).
- **ROUTE** - The Route determines the path to the target device. The first drop in the route is usually the drop number of the Auto-Scan port. Additional drops are used to point to the specific target. For example, if a PNIM port has a drop number of 125 and the target of the Auto-Scan is Circuit Monitor 4 then the route would be 125,004.

Notice: The Auto-Scan feature uses the Timer Interval from the Auto-transfer feature so therefore the Auto-transfer feature is disabled if a valid entry in the Auto-Scan is found by the CNOE-800. In order to be classified as a valid entry, the local, remote, count and route entries must be non-zero and fall within their respective valid ranges.

Notice: The Auto-Scan feature uses the route table from the Modbus Slave Table for a given serial port. If the Auto-Scan feature is enabled on a Modbus mode port, that port will be a Master and Slave operation will not be allowed.

Auto-Scan Status

The Auto-Scan feature includes the option of having a group of three mailbox registers to display the status of each Auto-Scan entry. Each Auto-Scan entry has a status bit which is set if the scanned message has a successful reply and cleared if the scan entry is disabled or an error occurs in the reply. The first Status register is for Scan entries 1 through 16, the second register is for entries 17 through 32, and the third Status register is for entries 33 through 48.

Auto-Scan Watchdog

The Auto-Scan feature includes a watchdog option that can turn off autoscan entries in specific ports when a user-specified timer expires. Two registers control this option: 8189 and 8190. Register 8190 is the bitmask register. The first (least significant) five bits control each of the ports. Bit one (LSB) controls port 0, bit two controls port 1, etc. When any of these bits is set high, the corresponding port is affected by the watchdog timer. The timer register, 8189, can be set by any outside device. The decimal value written will indicate the time in 10 ms increments. The time will immediately begin to count down to 0, unless a new number is rewritten to the timer register. If the timer reaches 0, all autoscans on the specified ports will be discontinued, and the status bits, if any, will be set to zero. Since this option is designed to take effect in the event of a communications loss, the affected ports will also be shut down in the event of a power cycle. When the CNOE-800 reboots, register 8189 will be reset to 0.

Auto-Scan Watchdog Example

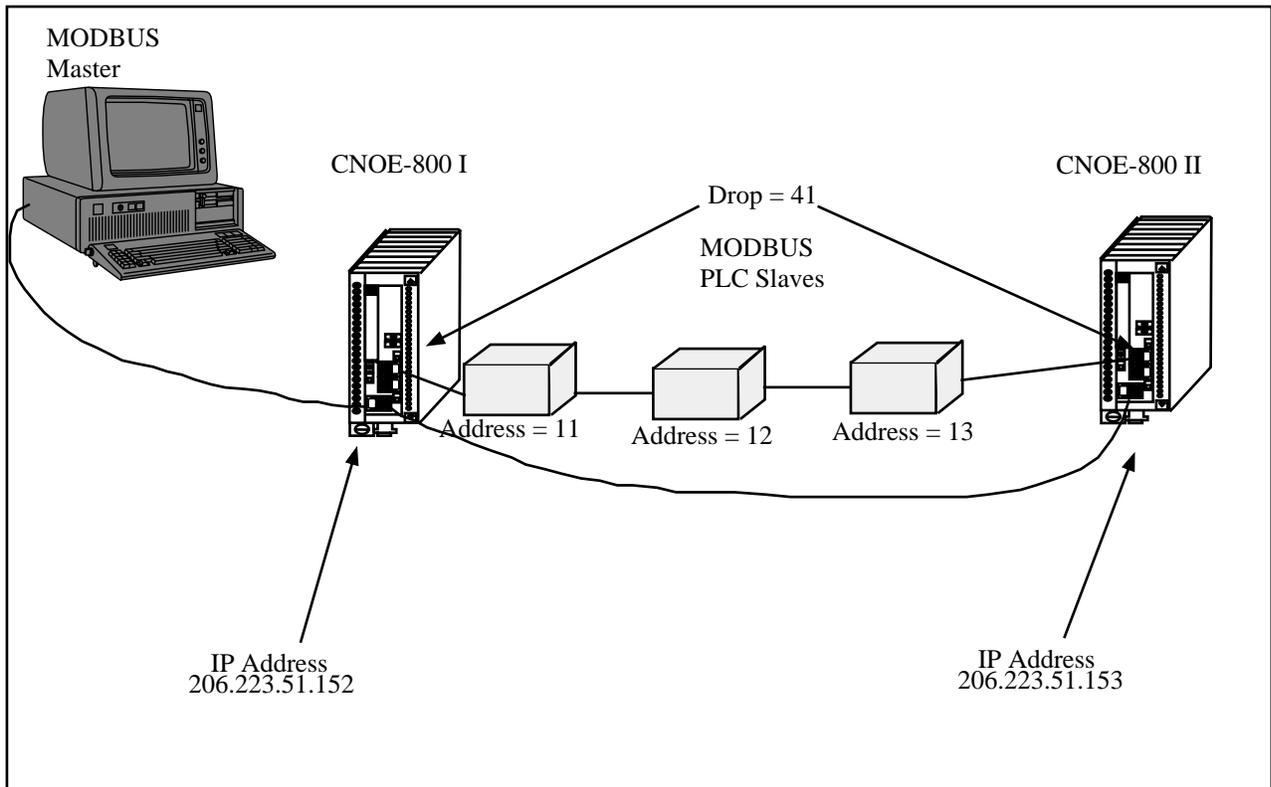


Figure 22-1 Auto-Scan Watchdog Example

In this example, an HMI package is monitoring registers that have been Auto-Scanned by CNOE-800 I. The HMI is constantly writing a decimal value of 500 to register 8189. The HMI is also monitoring the status register for the Auto-Scans. If the value of the status register is ever zero, or if the HMI loses communication to CNOE-800 I, the HMI must wait five seconds, then begin continuously writing decimal 500 to CNOE-800 II. Waiting five seconds will allow the timer in CNOE-800 I to run out, and there will be no conflicting queries on the serial line. As can be seen in the tables below, the Auto-Scan tables for both CNOE-800's are exactly the same, so only one should be Auto-Scanning at any given time.

Note: Since the Auto-Scan table uses the same routing registers as the Modbus Routing table, the programmer must be careful to select slave ID's that will be higher than the last entry in the Auto-scan table. Otherwise, the CNOE-800 not Auto-Scanning would reply to the master's queries.

Table 22-1 Auto-Scan Entries for both CNOE-800's

Entry	Local	Remote	Count	Direction	Route
1	4	1	10	Read	41,11
2	14	1	10	Read	41,12
3	24	1	10	Read	41,13

EPEER Mode

Niobrara CNOE-800 Ethernet port expanders are equipped with a peer-to-peer feature that allows a number of CNOE-800 and EPE5 units to distribute a range of rack-addressed registers among themselves. This feature is similar to the Sy/Peer feature of the Square-D model 600 or the Global Data Peer Cop function of Modicon PLCs. In comparison, Sy/Peer is higher in performance and can synchronize the scan of the linked PLCs but the EPEER is more flexible and uses standard Ethernet protocols so can be mixed with a small amount of ordinary traffic. For instance, PLCs can be programmed over the same cabling that carries the EPE5 peer-to-peer traffic. The CNOE-800 peer mode is faster than ordinary Sy/Net 802 operations because all nodes in the network are updated by a single multicast Ethernet packet instead of individual write transactions.

To design an EPEER peer network, determine how many registers each node will provide (broadcast) to the other nodes, the number of nodes, the total number of registers involved and the required update interval. Unlike Sy/Peer, the EPEER network is not restricted to broadcasting the same number of registers from each node, nor does the number of registers broadcast need to be a power of two. Any number of registers from 1 to 128 can be broadcast by any node. For an example, let us assume a network of eight EPE5 equipped nodes each transmitting 50 registers. This is a total of 400 registers that would be rack-addressed to each CNOE-800 unit.

Each node is assigned a node number, in this case 1 through 8. This node number is not related to the Sy/Net 802.3 drop number of the CNOE-800. For our example, let us imagine that the register map of each CNOE-800 looks like this:

Table 23-1 E-PEER Register List Example

CNOE-800 Registers	Supplying Node
1..50	1
51..100	2
101..150	3
151..200	4
201..250	5
251..300	6
301..350	7
351..400	8

Write the following values to the setup registers in each QUCM:

CNOE-800 Register	Function	Example Value
8026	Number of peer nodes	8
8012	Number of this node	1 through 8
8013	Start of register range to transmit	$(R[8012] - 1) * 50 + 1$
8027	Number of registers to transmit	50
8028	Destination register (in other peers)	same as R[8013]
8011	Update interval in milliseconds	24 (3mS per node)
8030	Bit 6 enables E-PEER operation	32

Rack address 400 registers to the EPE5 in each PLC rack.

The bits of read-only register 3303 correspond to those of the first sixteen nodes in an CNOE-800 peer network which are active. If unit x is active on the network, bit x is set. If node x is powered off, disconnected from the cable, or otherwise disabled, bit x will be cleared. Loss of one node has no effect on the timing of the other nodes. They will detect the absence of the node and clear the corresponding bit in their register 3303. If the peer network has more than sixteen nodes, node numbers 17 and beyond have no associated active bit.

The update interval should be selected depending on system requirements and PLC scan time. As a rule of thumb, don't attempt to update faster than 1 or 2 milliseconds per node. There is no point in updating the peer-to-peer network much faster than the PLC can scan, but bear in mind that there is no synchronization between PLC scanning and peer-to-peer updating. Attempting to update too many registers too fast will result in Ethernet collisions that will reduce the throughput of the network and render it non-deterministic. Check the collision statistics (register 2066 and 2067) to determine if your update rates are too ambitious or consult Niobrara for maximum update rates for a given system design. Use the Ethernet packet counters (registers 2064 and 2065) and a stopwatch to verify that throughput is what you expect. Note that no acknowledge packet is sent for CNOE-800 peer operations and it is your responsibility to avoid overloading the available throughput.

With no other traffic on the cable, the network will operate deterministically. Each node will time its register broadcast to occur in its time slot. Depending on the amount of network bandwidth and processing resources used up by the peer-to-peer transmissions, non-peer traffic (i.e. Sy/Max programming or reads and writes) can cause a temporary loss of deterministic behavior. This is not usually a problem when the network is being used to program the PLCs. Peer operations have priority over other CNOE-800 transactions.

It is possible to set up a CNOE-800 to receive E-Peer broadcasts without transmitting any. Any number (up to Ethernet limits) of CNOE-800 units may listen to one or more broadcasting units. To configure a listen-only E-Peer node, set bit 6 of register 8030 to 1 and set register 8012 (number of this node) to 0. A CNOE-800 with 8030.6 clear will ignore E-Peer broadcasts but, like any IEEE 802 compliant device, can coexist on the Ethernet with E-Peer configured units. A receive-only or non E-Peer unit is not counted in the number of nodes programmed into register 8026 of the E-Peer units.

The E-Peer parameters may be easily configured within MEBSW. See page 148 for more information.

Figure 23-1 displays the timing relationship for an E-peer network with three nodes, A, B, and C. Notice that the Update Interval is based upon the time between broadcasts of the same unit.

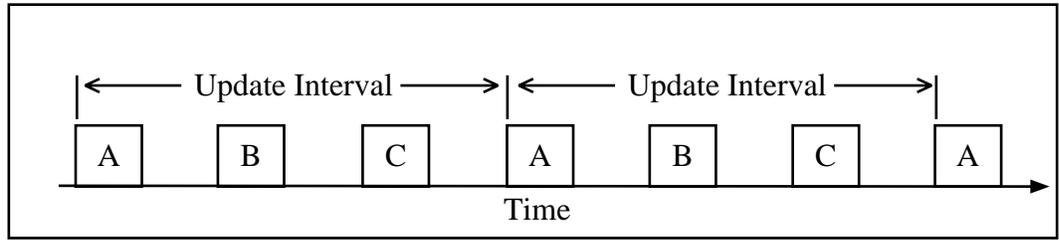


Figure 23-1 EPEER Update Interval Timing

On Ethernet Option

Each of the serial ports have the option of being mapped to the Ethernet as a "Virtual E-Net Node". This feature is called "On Ethernet". By placing the drop numbers of the serial ports on the Ethernet, the number of drops in the Route may be reduced. This may be especially helpful in cases of Net-to-Net, Modbus, and PowerLogic protocol modes.

NOTE: The "On Ethernet" option only applies to the SY/MAX 802.3 Ethernet protocol. The "On Ethernet" setting is ignored in Modbus/TCP protocol.

The CNOE-800 treats ports with the "On Ethernet" option set with the following rules:

- Messages arriving at serial ports have their routes inspected to determine if the next drop in the route is one of the other ports in the CNOE-800. If the next drop number matches another port in the module then the message is routed to that port.
- Messages arriving at serial ports with the next drop number not in the Module are routed out of the Ethernet port as the next drop is assumed to be on the E-Net.
- Ethernet Messages routed to the standard E-Net port are routed as normal.
- Ethernet Messages targeted to an "On Ethernet" port are immediately sent out the appropriate port.
- The SY/MAX Ethernet addresses are limited to the range 00 through 99. "On Ethernet" drop numbers in the range 100 through 199 will appear on the E-Net as the drop number - 100. For example, if drop 154 is placed "On Ethernet" then the CNOE-800 will place the drop number 54 on the Ethernet. Thus messages routed to the E-Net address 54 and 154 will both be processed by the same CNOE-800. This feature may be used to reduce the number of E-Net drop numbers consumed by "On Ethernet" ports.

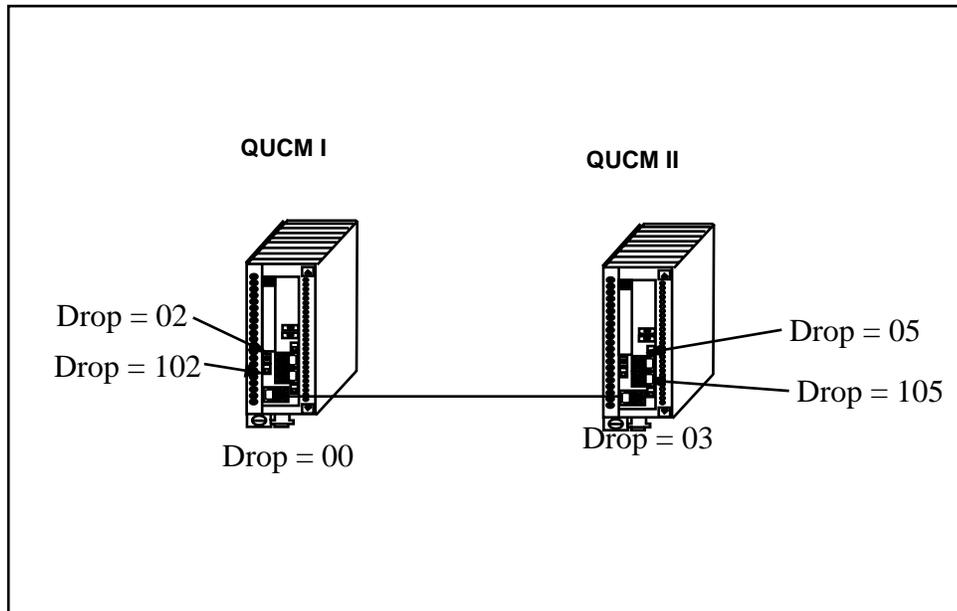


Figure 24-1 On Ethernet Example

In Figure 24-1 if all of the ports are placed on the Ethernet then the CNOE-800's would respond to E-Net messages with target drop numbers of 00, 02, 03, 05, 102, and 105. Therefore none of the other devices on the SY/MAX Ethernet may have these drop numbers or a duplicate drop number error condition will occur.

Consider that all of the serial ports are in SY/MAX mode. Table 24-1 shows several possible routes for communication.

Table 24-1 On Ethernet Routing Examples

Source	Target	Route
CNOE-800 I Port 1	CNOE-800 II Port 1	2, 0, 3, 5
CNOE-800 I Port 1	CNOE-800 II Port 1	2, 0, 5
CNOE-800 I Port 1	CNOE-800 II Port 1	2, 3, 5
CNOE-800 I Port 1	CNOE-800 II Port 1	2, 5
CNOE-800 II Port 2	CNOE-800 I Port 2	105, 3, 0, 102
CNOE-800 II Port 2	CNOE-800 I Port 2	105, 0, 102
CNOE-800 II Port 2	CNOE-800 I Port 2	105, 3, 102
CNOE-800 II Port 2	CNOE-800 I Port 2	105, 102

Configuration Software RPCSW32

RPCSW32

The RPCSW32 software program is provided free of charge to CNOE-800 users. RPCSW32 is a Windows 32-bit console application and may be run under WIN95/98/NT/2000/ME/XP. This software is used to configure the operational parameters of the CNOE-800. It may be operated in either online or offline modes.

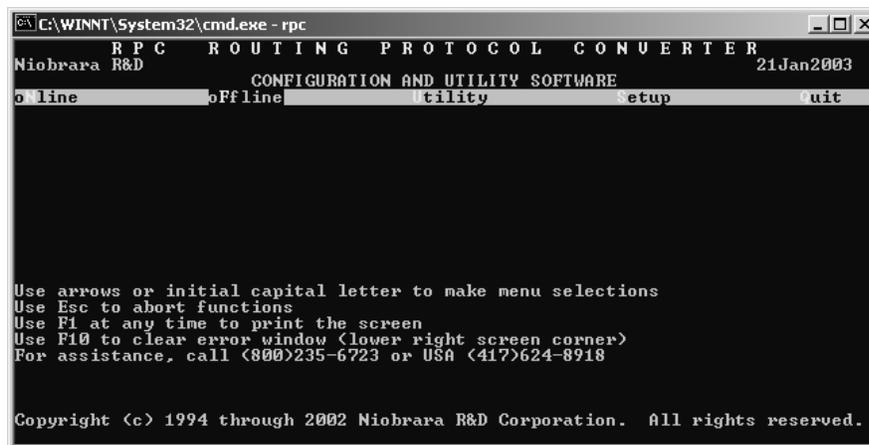
RPCSW32 will use the TCP/IP stack native to WIN95/98/NT/2000/ME/XP for direct MODBUS/TCP connection to the CNOE-800.

In online mode, RPCSW32 presents the user with a screen of data describing the operation of all of the module's ports. The arrow keys are used select the port parameters to be modified and the space bar and + and - keys are used to change the parameters of that port. Changes made in the online mode are transferred to a connected CNOE-800 module and are effective immediately.

In offline mode, RPCSW32 allows a copy of the configuration to be uploaded from the CNOE-800 to an image in offline memory. The offline copy can be edited without affecting the CNOE-800 in real time. The offline copy can be saved to a named disk file for later retrieval, or listed on a hard copy printer. A CNOE-800 need not be connected to perform most offline operations. The offline copy of the configuration parameters may be downloaded to a CNOE-800 module at any time.

Because the CNOE-800 has an internal nonvolatile parameter memory, the configuration parameters normally will not need to be reloaded unless a change has been made.

The startup screen of RPCSW32 is shown in Figure 25-1 on page 144. The operational modes are selected by the highlighted menu bar on the fourth line. Selection can be made by moving the cursor to the desired option using the arrow keys and pressing **ENTER**. A short cut is provided, simply type "N" for online, "F" for offline, "U" for Utility, "S" for setup or "Q" to quit.



```

C:\WINNT\System32\cmd.exe - rpc
RPC ROUTING PROTOCOL CONVERTER
Niobrara R&D 21Jan2003
CONFIGURATION AND UTILITY SOFTWARE
o line  o Ffline  o tility  o Setup  o uit

Use arrows or initial capital letter to make menu selections
Use Esc to abort functions
Use F1 at any time to print the screen
Use F10 to clear error window (lower right screen corner)
For assistance, call (800)235-6723 or USA (417)624-8918

Copyright (c) 1994 through 2002 Niobrara R&D Corporation. All rights reserved.

```

Figure 25-1 RPCSW32 Startup Screen

If offline mode is selected, a second menu appears as shown in Figure 25-2. This menu presents the available functions for manipulating the offline image of the configuration parameters and for transfer of configuration data to and from the CNOE-800 module. Use the up and down arrows to move the highlight, **ENTER** to select the highlighted choice, or the initial capital letter to quickly select an option.

The online and offline parameter editing screens are nearly identical. The difference is in operation. Every time a change is made in the online mode, the modified parameter is transmitted to the CNOE-800. In offline mode, changes are made to the parameter image in offline memory. Changes made in the online screen affect only the configuration stored in the attached CNOE-800, not the offline copy. Likewise, changes made in offline mode have no effect on a connected CNOE-800 until they are explicitly sent to it using the "Send memory to module" function.

RPCSW32 also contains several convenient utilities for general use: a SY/MAX Register Viewer, and a Statistics Viewer. These features use the same setup as the oNline and oFfline functions.

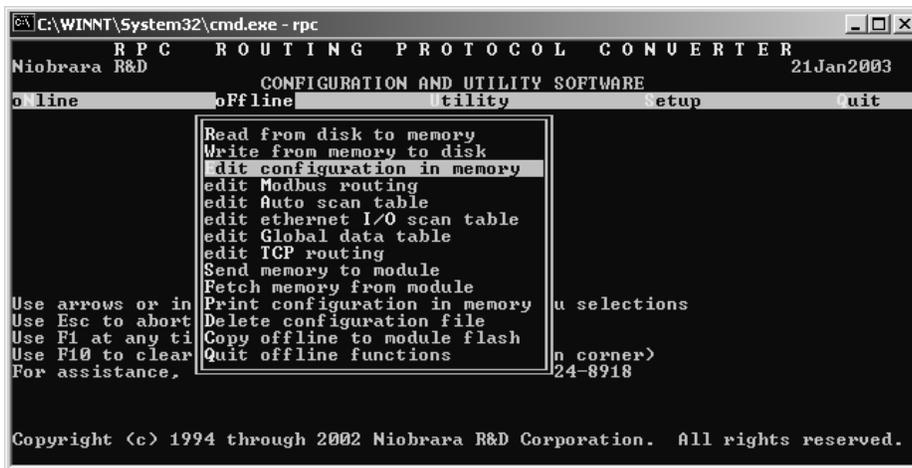


Figure 25-2 RPCSW32 offline Menu

Data Entry Keys

Whenever data entry is allowed by the program, certain keys can be used to facilitate data entry. They are:

BACKSPACE	Move cursor left and remove character there
LEFT ARROW	Move cursor to the left one character
RIGHT ARROW	Move cursor to the right one character
DEL	Remove the character under the cursor
INS	Change between insert and overstrike modes of entry
HOME	Move cursor to the left edge of the field
END	Move cursor to the end of the data
Control-F	Move cursor right (Forward) one word
Control-R	Move cursor left (Reverse) one word
Control-D	Delete from the cursor to the end of the field
Control-U	Delete from cursor to the beginning of the field

Control-Y	Delete all characters in the field
ESC	Exit the field without modifying it
ENTER	Accept the contents of the field

When a field is opened for input, the cursor is positioned at the left side of the field. If data is already present in the field, typing any character other than those listed above will cause the field to be blanked allowing entry of new data without first deleting the old. If it is desired to retain the previous data for editing, make sure the first key you type is an editing key such as a left or right arrow.

Most data fields in RPCSW32 do not allow direct entry of the parameter, instead a series of choices is presented. The following keys are used:

GRAY +	Increments options to the next available choice
GRAY -	Decrements options to the previous choice
SPACE BAR	Increments options and rolls back to first option after last

The arrow keys are used to maneuver between fields.

Online and Offline Editing Screen

In either the online or offline mode, parameters are changed by moving the highlighted cursor to the desired field using the arrow keys and by pressing the +, -, or space bar to toggle through available parameters.

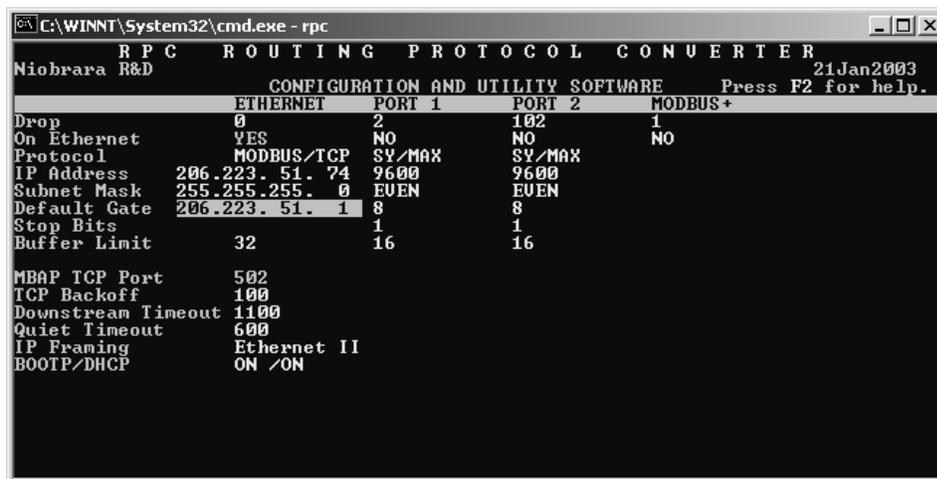


Figure 25-3 RPCSW32 oNline Edit Screen

(All ports)The oNline Edit (and oFfline Edit) screen is presented as a matrix of parameters, see Figure 25-3. Each column represents one of the ports of the CNOE-800. The lower half of the screen will change to present the available parameters for each protocol mode. The parameters are described below.

Drop Number

(Ethernet and Backplane) This value determines the drop number of the port. All ports must have unique drop numbers within the module. The drop number of the Ethernet port must be unique for the entire Ethernet network. The Ethernet drop number must fall within the range of 00 through 99. The drop number for the backplane port must fall within the range 000 through 199. The default drop number for the Ethernet port is 0, and backplane is port is 1.

On Ethernet

(Ports 1 and 2) This setting allows the CNOE-800 to place the drop number of the port on the Ethernet as a virtual Ethernet SY/NET address. No other device on the E-Net may have the same drop number

or drop number - 100 as the port. This option is valid in SY/MAX 802 Ethernet mode only and is ignored in TCP/IP protocols.

Protocol

(Ports 1,2) This value determines the mode of the individual communication port. Possible values are SY/MAX, Net-to-Net, Peripheral, Transparent, Share, PLogic, Idec, Gateway, Multidrop, Modbus Host, Modbus Gate, PNIM, RNIM Master, and RNIM Slave. The default modes for Port 1 and Port 2 are Dual Slave and Modbus ASCII, respectively.

(E-net) The QUCM modules support SY/MAX 802, Modbus/TCP, and MBTCP+SY/MAX. The default is Modbus/TCP.

Baud Rate

(Ports 1,2) Controls the baud rate of the individual port. This value should be set to match the baud rate of the device attached to the port. The default value is 9600.

Parity

(Ports 1,2) Controls the parity of the individual port and should be set to match the attached device. Available choices are EVEN, ODD, and NONE. The default value is EVEN.

Data Bits

(Ports 1,2) Set to 7 or 8 to match the data bits transmitted by the connected device. The default values for Port 1 and Port 2 are 8 and 7, respectively.

Stop Bits

(Ports 1,2) Set to 1 or 2 to match the stop bits used by the connected device. The default value is 1.

Buffer Limit

(E-net, Ports 1,2) The buffer limit sets the maximum amount of available buffers for each port. The default value is 16 with a minimum value of 2 and a maximum value of 16. Then E-net port has a maximum value of 32. It is not recommended to alter the number of buffers available unless the equipment requires a small number of buffers.

Mode Specific Sub-menus

Certain mode values require additional parameters and other fields will appear in the middle area of the screen. Only the parameters listed in this manual are used by the CNOE-800. These parameters are explained as follows:

Driver Mode

(Peripheral, Share, Multidrop, Modbus Host, Modbus Gate, RNIM Master, RNIM Slave, Chevron) These settings control the action of the transmit driver and receiver action of the RS-485 port. Possible settings include **Pt to Pt** for Point to Point (RS-422 operation), **FOUR WIRE** for 4-wire RS-485 slave operation, **HALF DUPLEX** for 4-wire Pt to Pt half duplex operation, and **TWO WIRE** for 2-wire half duplex operation.

IP Address

(E-net Port only, Modbus/TCP and MBTCP+SY/MAX protocol only) The IP Address is entered in dotted-decimal notation. This address should be provided by the Network Administrator of your corporate Ethernet. Each IP device on the network must have a unique IP Address. The default IP Address for the RPC will be 0.0.0.0.

Subnet Mask

(E-net Port only, Modbus/TCP and MBTCP+SY/MAX protocol only) The Subnet Mask is entered in dotted-decimal notation. This address should be provided by the Network Administrator of your corporate Ethernet. The default mask is 0.0.0.0.

Default Gate

(E-net Port only, Modbus/TCP and MBTCP+SY/MAX protocol only) The Default Gate is the IP address of the default gateway for the subnet that the CNOE-800 is located on. The Default Gate is entered in dotted-decimal notation with the factory default as 0.0.0.0.

MBAP TCP Port

(E-net Port only, Modbus/TCP and MBTCP+SY/MAX protocol only) The TCP Port number for Modbus TCP/IP is fixed at 502. This is the TCP Port number that the RPC-TCP Server listens on for accepting new connections.

TCP Backoff

(E-net Port only, Modbus/TCP and MBTCP+SY/MAX protocol only) The TCP Backoff is the amount of time that TCP will wait for an acknowledgment of a transmitted message. When this amount of time has passed after transmitting a message, TCP will retry the message and reset its timeout timer to twice this value. After this timer expires without an acknowledgment, the value is quadrupled, etc., until the Downstream timeout expires. This value is expressed in units of 1/100th of a second. The default value is 100 (1 sec.).

Downstream Timeout

(E-net Port only, Modbus/TCP and MBTCP+SY/MAX protocol only) The Downstream Timeout determines the amount of time that the CNOE-800 will wait for a reply from the remote device. Upon the expiration of this timer, a timeout error reply is generated to the source of the message and the TCP layer is instructed to give up on the message. This value is expressed in units of 1/100th of a second and the default value is 500 (5 sec.).

Quiet Timeout

(E-net Port only, Modbus/TCP and MBTCP+SY/MAX protocol only) The Quiet Timeout determines the amount of time that the CNOE-800 will keep a TCP connection open without receiving or transmitting a new message on the connection. This value is expressed in units of 1 second and the default value is 600 (10 minutes).

Server Operation: The CNOE-800 will send a keep-alive TCP message to the client after the Quiet Timeout expires. If the Client responds, then the connection is left open. If the Client doesn't respond, the CNOE-800 will retry once a second for 10 seconds and then close the connection.

Client Operation: If the timeout expires on a connection that the CNOE-800 originated, the CNOE-800 will send a FIN on that connection to close it down.

NOTE: The "keep alive" message sent by another Niobrara server will be recognized by the CNOE-800 client and the CNOE-800 will shut down the connection. So if the client and server have different timeout values, the shortest of the two will cause the connection to close.

IP Framing

(E-net Port only, Modbus/TCP and MBTCP+SY/MAX protocol only) The CNOE-800 may use Ethernet II (DIX) or 802.3 (SNAP) framing. The most common network IP setting is Ethernet II.

MAC Address

(E-net Port only)The "Online, Edit port parameters" screen will display the MAC Address for the module in hexadecimal notation.

E-Peer

(E-Net Port only, SY/MAX 802.3 only) The E-Peer item allows the enabling of the CNOE-800's Peer-to-Peer mode. If set to OFF the E-Peer is disabled on this CNOE-800 and the Auto-Transfer settings for the E-Net port are displayed. If set to ENABLE, the Auto-Transfer settings for the E-Net port change to show the settings for the E-Peer.

Error Check

(SY/MAX, Net-to-Net, PLOGIC, Multidrop, PNIM) The Error Check item allows the selection of the standard BCC error check or the CRC error check. Normal SY/MAX operation requires the BCC error check. The SY/MATE PLUS software provides the CRC checksum as an option for use with no parity, thus allowing 10 bit modem programming. The CRM-512 NIM also uses the CRC checksum.

Route Appendix

(SY/MAX) The Route Appendix allows SY/MAX devices with limited network capabilities, such as the EATON PanelMate operator interface, to increase the number of drops available. SY/MAX packets arriving at the port with the last drop in the route being 205 will have the Route Appendix attached to the incoming route in place of the 205 drop number. To disable the Route Appendix feature, set the Route Appendix to NONE by deleting all drops in the route field.

Route Replacement

(SY/MAX) The Route Replacement is an extension of the Route Appendix feature. If the Route Replacement is ON, any incoming SY/MAX packet on the port will have its route ignored and the route described in the Route Appendix will be used instead. The replies from sent messages will have their original route reversed and inserted as they leave the port. The default value is OFF.

The Route Replacement/Appendix may be enhanced to include up to 128 eight-drop routes by using Options bit 2. When this Options bit is set for the SY/MAX mode port, incoming route of the form 205,X will have the route located in the Modbus Slave Address Table entry X used for the replacement. The reply will be returned to the sender with the reversed route X,205. This feature may only be used on single-threaded SY/MAX ports and is primarily intended to be used with the PanelMate operator interface.

Packet size limit

(Transparent, Share, Gateway) This value determines the number of characters which will accumulate without receiving an ASCII carriage return or exceeding the Packet time limit, and result in the formation of a SY/MAX packet being formed. Setting the packet size to 1 will cause each character entering the port to be transmitted without delay but will result in slow throughput because of the large overhead of sending each character as a packet. The default value is 128 characters.

Packet time limit

(Transparent, Share, Gateway) This integer value determines the number of hundredths of a second which will pass between characters before a packet is formed of the characters already received. The default value is 100.

Target Route

(Transparent, Share, Gateway) The route should consist of the drop number of the originating port, any Net-to-Net drops, and the drop number of the receiving port. For two-way communication, the receiving port should be programmed with the same drops in reverse order. In Gateway mode, the route may be easily modified by using the Address command. The default value is NONE.

Control Character

(Transparent, Share, Gateway) The Control Character field determines whether control characters (carriage return, line feed, etc.) will be used to terminate the message before the packet time limit or packet size limit is met. The default value is ON.

Echo

(Transparent, Share, Gateway) The Echo field determines whether the port will echo all characters received back to the sending device. This may be useful in applications involving terminals. The default value is OFF.

Highlight

(Gateway) The Highlight field determines whether the Gateway port provides the ANSI highlight control characters before and after each message returned from the Gateway port. The default value is OFF.

Node Priority

(Multidrop) This value determines the priority for the port within the multidrop scheme. Each port on the multidrop circuit should have its own unique priority value and should fall within the range of 1 to the number of nodes.

Number of Nodes

(Multidrop) This value should be set to equal the number of multidrop CNOE-800, QUCM, MEB, EPE5 or SPE4 ports included within the network. This value must be at least equal to 2.

Time Slice

(Multidrop) The time slice value determines the amount of time that each unit will wait from the receipt of the last character on the network before transmitting a new request. This value is expressed in units of n/100 seconds.

READ command

(MODBUS Host) This value is required in the MODBUS Host mode. SY/MAX read requests are translated to the MODBUS function code defined in the MODBUS READ register for that port. Possible values are 1, 2, 3, or 4. The default value is 4.

WRITE command

(MODBUS Host) This value is required in the MODBUS Host mode. SY/MAX write requests are translated to the MODBUS function code defined in the MODBUS WRITE register for that port. Possible values are 5, 6, 15, or 16. The default value is 16.

Retry timeout

(MODBUS Host and Gateway) This value expressed in units of n/100 seconds determines the delay time between retries for failed transmissions from a MODBUS mode port. The default value is 100.

Register Bias

(MODBUS Host) Since it is not possible to read or write MODBUS registers outside of the legal SY/MAX range of 1 through 8192., an offset value has been added. This offset value allows the translation from the SY/MAX range to another valid range in MODBUS. The MODBUS register addressed will the result of the following formula:

$$\text{MODBUS value} = \text{SY/MAX register} + \text{Offset value} - 1$$

If the offset value equals 0 then reading the SY/MAX register 1 will translate to reading the MODBUS register 0. If the offset value equals 20001 then reading the SY/MAX register 10 will translate to reading the MODBUS register 20010. The default value for the offset is 1.

Transfer Interval

(Auto-transfer) This value determines the periodic interval between Auto-transfer READS/Writes. The value is expressed in units of n/100 seconds (i.e. 100 = 1 sec). Some consideration must be taken in selecting the interval. Too small of a value will result in the filling of the buffers and possible rejection of reads/writes. If the application is time critical, this value should be set to a value slightly longer

than the transmission + reception time of the largest expected packets. If both read and write are selected, the transmission time must be calculated for each worst case and added together for the final interval.

Transfer Route

(Auto-transfer) The route describes the path that any Auto-transfer reads and/or writes will require to reach the desired peripheral device. Two drops are required. The first must be the drop number of the CNOE-800 port, the second must be the unit number of the attached device.

READ Count

(Auto-transfer) This value determines whether the Auto-transfer read will operate. A value of zero will disable the Auto-transfer read. A value of one will cause a read to occur at the time interval. A value greater than one will cause a multiple register read to occur starting at the READ From register.

READ From

(Auto-transfer) This is the register number located within the peripheral device that is of interest. On multiple register reads, READ Count > 1, this is the starting register of the multiple register read.

READ To

(Auto-transfer) This is the register number in the mailbox where the data from the peripheral device will be stored. On multiple register reads, this is the first register of the multiple registers.

WRITE Count

(Auto-transfer) This value determines whether the Auto-transfer WRITE will operate. A value of zero will disable the Auto-transfer write. A value of one will cause a write to occur at the time interval. A value greater than one will cause a multiple register write to occur starting at the WRITE From register.

WRITE To

(Auto-transfer) This is the register number located within the peripheral device that is of interest. On multiple register writes, this is the starting register of the multiple register write.

WRITE From

(Auto-transfer) This is the register number in the mailbox where the data for the peripheral device is stored. On multiple register writes, this is the first register of the multiple registers.

Total E-Peer Nodes

(E-Peer) This value determines the total number of CNOE-800/EPE5/MEB/QUCM modules on the E-Peer. This value must be in the range of 2..100 and must be the same for all CNOE-800/EPE5/MEB/QUCM modules using the E-Peer.

E-PEER devices with This Node's Number set to zero are not included in the total E-PEER nodes count.

This Node's Number

(E-Peer) This value sets this CNOE-800's E-Peer number. This number must be unique among the E-Peer members and must also fall within the range of the Total E-Peer Nodes.

NOTE: This value has no relationship to the SY/NET drop number of the E-Net Port.

A special case of This Node's Number is when it is set for zero. When This Node's Number is set to zero and the E-PEER is enabled, this CNOE-800 will accept E-PEER messages, but will not transmit any data. This allows E-Peer devices to listen to all of the data on the network but not consume any of the available bandwidth because they have nothing to transmit. E-PEER devices with This Node's Number set to zero are not included in the total E-PEER nodes count.

Start Register

(E-Peer) This is the register number in the mailbox where the data for the other E-Peer members is stored. On multiple register writes, this is the first register of the multiple registers.

Register Count

(E-Peer) This value determines the number of registers broadcasted from this CNOE-800 to the other members of the peer. The register count is not required to be the same among the members of the peer.

Destination Reg

(E-Peer) This is the register number in the other members of the peer where the data from this CNOE-800 will be transferred. This value is commonly the same as the Start Register.

Update Interval

(E-Peer) The amount of time in milliseconds allotted for a complete cycle of the peer. It is recommended that the Update Interval be an integer multiple of the total number of units where the multiple has a minimum value of 2. For example, if there are 8 nodes in the peer and 3mS is allowed for each node, set the Update Interval to 24.

Network Id

(RNIM Master and Slave) This number must be the same for all RNIM devices on the same Remote Network. The Network Id allows multiple Remote Networks to operate within close range on the same frequency. RNIM devices only respond to messages that match their own Network Id. The Valid data range is 0 through 255.

NOTE: The Square D CRM-560 always defaults to a Network Id of 0 upon power-up.

CTS Timer

(RNIM Master and Slave) The CTS timer provides a minimum amount of time to wait for the Clear to Send hardware handshake line to become active after the Request to Send (RTS) line has been asserted. The unit of time is 10mS. A value of 50 provides a 500mS delay. The valid data range is 0 through 65535 (655.35 seconds max).

NOTE: The Square D CRM-560 CTS timer has units of 50mS and defaults to a value of 10 (for a delay of 500mS) upon power-up.

Packet response

(RNIM Master and Slave) This value sets the message response timeout in 10mS units. This value determines the amount of time that the RNIM port will wait for a response before a message is retransmitted. (The number of retries is governed by the Retries setting.) This value also covers the response time allotted to a BID. The valid data range is 0 through 65535 (0 sec to 655.35 sec).

NOTE: The Square D CRM-560 Message response timeout is in 1 second units and defaults to 20 seconds upon power-up. Also the CRM-560 has the BID response fixed at 2 seconds.

Bid interval

(RNIM Master) This value sets the interval between successive automatic BIDs in 10mS units. This value determines the amount of time that the RNIM Master port will wait between sending one BID and sending the next after the Message response timeout has elapsed. During this interval any queued NORMAL messages are sent. The valid data range is 0 through 65535 (0 sec to 655.35 sec).

NOTE: The Square D CRM-560 does not allow this parameter to be adjusted. It is fixed at 2 seconds.

Retries

(RNIM Master) This value sets the number of retries by the Master (without a valid reply from the Slave) before an error message is returned to the originating device. The valid range is 0 through 65535 for Masters and 0 for Slaves.

NOTE: The Square D CRM-560 Number of Retries has a valid range of 0 through 3 for Masters and 0 for Slaves and defaults to 3 upon power-up.

Pause time

(RNIM Master) This value determines the amount of time that will be inserted after a specific number of messages or BIDs have been sent to rest the transmitter. Valid data range is 0 through 65535.

NOTE: The Square D CRM-560 Pause time is in 1 second units and defaults to 15 upon power-up.

Message Count

(RNIM Master) The Message Count is the number of messages and/or BIDs that will be transmitted by the Master before the Pause Time will be inserted to give the transmitter a chance to rest. Valid range is 0 through 65535.

NOTE: Most modern transmitters will operate at 100% duty so set this value to 0 if your transmitter can handle it.

NOTE: The Square D CRM-560 defaults this value to 4 upon power-up.

Bid Address

(RNIM Master) This number determines the type of BID operation.

1 to 99 - If the value falls within the range of 1 through 99, the RNIM Master will issue a single BID to that Slave address. The Slave has the amount of time set by the Message response setting to respond to the BID.

NOTE: To send a single BID to Slave 00, use the value 100.

100 to 199 - If the value falls within the range of 100 through 199, the RNIM Master will issue a BID to the Slave address that corresponds to the number minus 100. The Slave has the amount of time set by the Message response setting to respond to the BID. After the Message response timeout has occurred (regardless if a response was sent), the Master will wait for the BID Interval delay. After the BID Interval delay, the Master will subtract 1 from the address and issue a BID to that new Slave address minus 100. This new address will be displayed in the BID Address register in the Master. The address will be automatically decremented at the end of the Bid response timeout (or reply) until the address 00 BID has been issued. All addresses between the starting address and 00 will be BID. It is not possible to skip any addresses. NORMAL messages received while performing an automatic BID take precedent over the automatic BID and will be inserted during the next BID Interval delay.

200 to 299 - If the value falls within the range of 200 through 299, the RNIM Master will issue continuous BIDs to that address minus 200. After sending the BID, the Master will wait for the Message response timeout before processing any other messages. After the Message response timeout, the Master will wait for the BID Interval time before sending the next BID. During the BID Interval delay, all queued NORMAL messages will be sent over the remote network.

300 to 399 - If the value falls within the range of 300 through 399, the RNIM Master will issue continuously decrementing automatic BIDs from that address minus 300 to address 00. After the BID for address 00 is sent, the BID resumes at the starting address. This works just like the 100 to 199 that automatically resets itself when it gets to zero.

NOTE: Unlike the 100 to 199 operation, the value displayed in the BID address register always stays at the 300 range value. This is to allow the automatic BID to resume upon power loss.

Transfer Route

(Transfer) The route should consist of the route from the Transfer port to the Primary PLC.

Backplane Port Mode

(Backplane Port) Selects whether the CNOE-800 will be seen by the PLC as an option module or an I/O module. As an option module, the user has full control to the PLC. As I/O only, the CNOE-800 can only manipulate the registers assigned to it by the PLC.

Note: This feature is only read by the PLC at power up. If it is changed, the rack's power must be cycled for the change to take effect.

MSTR Message Reply Timeout

(Backplane Port) Specifies the amount of time the CNOE will wait before sending back an error to the PLC that the downstream device did not respond. This value is set in increments of 1/100th of a second. The default is 1000 (10 seconds).

Programming Channel idle timeout

(Backplane Port) Specifies the amount of time the CNOE will keep a programming connection open without a message being sent or received. The value is set in increments of 1 minute. The default is 16 minutes.

Ethernet I/O Scanner

(Backplane Port) Determines whether the Ethernet I/O Scanner is enabled. If enabled, the CNOE-800 will read its I/O scan table, and begin issuing messages from the Ethernet port. More details will follow. Default is disabled.

Ethernet I/O Entries Per Socket

(Backplane Port) Specifies the span of entries in the I/O scanning table the CNOE-800 will compare for a common IP address. All entries in that span to a single IP address will be sent in a single socket before opening another socket to that device. Valid entries are 1-32. The current default is 4.

HOTKEYS

F1 Print Screen hotkey

Pressing the F1 key at any time will allow for printing of the screen to a printer or text file. Pressing the F1 key will produce a window similar to Figure 25-4.

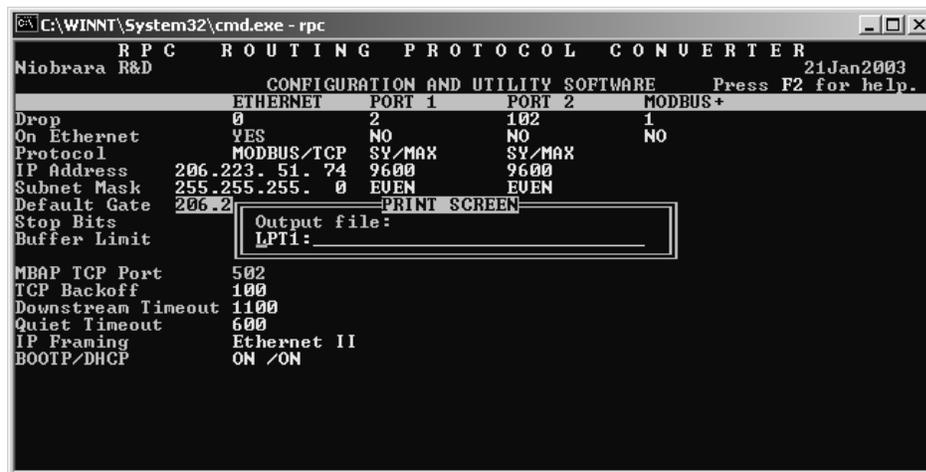


Figure 25-4 F1 Print Screen

The new window prompts for an output filename. The default is PRN which prints to the DOS default printer. If a valid DOS filename is typed into the field, RPCSW32 will print the information to that filename as an ASCII text file.

F2 Help Window

Pressing the F2 key will present the help window shown in Figure 25-5. Pressing any key will return to the previous location.

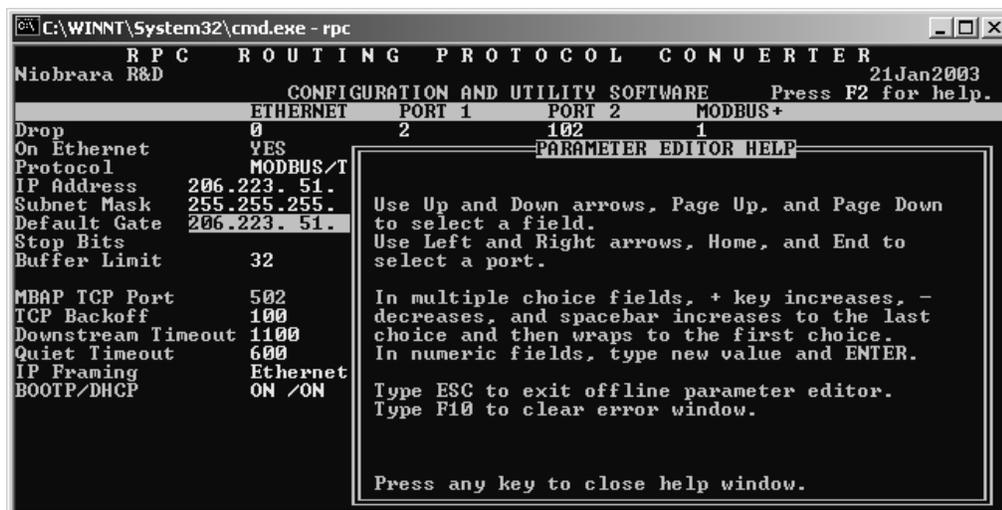


Figure 25-5 F2 Help Window

F3 Statistics Viewer

Pressing the F3 key while on a port will invoke the statistics register viewer. This window will display the statistical registers for a specific port. The port selection may be changed by pressing the space bar or the + or - keys. Pressing the 0 (zero) or the z key will result in the clearing of all of the statistical parameters for the selected port. Press the ESC key to exit back to the main screen.

The Ethernet port has its own set of statistics as shown in Figures 25-6, 25-7, and 25-8.

Pressing the Page Down key will advance the statistic viewer to a new page of statistics. Pressing the Page Up key will return to the first page. Pressing the left arrow key, right arrow key, - key, + key, or space bar will change the port displayed. Pressing the F9 key will provide a shortcut to the SY/MAX setup window for changing the route, etc.

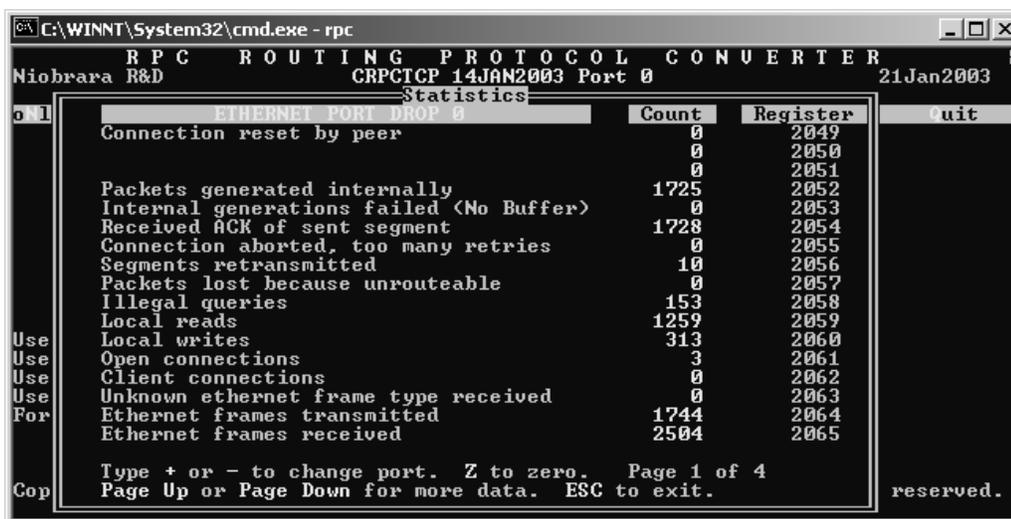


Figure 25-6 Ethernet Port Statistical Screen (Page 1)

```

C:\WINNT\System32\cmd.exe - rpc
RPC ROUTING PROTOCOL CONVERTER
Niobrara R&D CRPCTCP 14JAN2003 Port 0 21Jan2003
Statistics
-----
ETHERNET PORT DROP 0 Count Register
-----
Last route received --- 2076
--- 2076
--- 2077
--- 2077
--- 2078
--- 2078
--- 2079
--- 2079
--- 2079
Use Buffers in internal queue 0 2071
Use Ethernet collisions 0 2066
Use Packets lost because excess collisions 0 2067
Use Receive packets lost for CRC error 0 2068
Use Receive packets lost for framing error 0 2069
For Sequence error, NAK TRANS 0 2070
Cop Buffers currently in use 1 2080

Type + or - to change port. Z to zero. Page 2 of 4
Page Up or Page Down for more data. ESC to exit. reserved.

```

Figure 25-7 Ethernet Port Statistical Screen (Page 2)

```

C:\WINNT\System32\cmd.exe - rpc
RPC ROUTING PROTOCOL CONVERTER
Niobrara R&D CRPCTCP 14JAN2003 Port 0 21Jan2003
Statistics
-----
ETHERNET PORT DROP 0
-----
Socket IP Socket IP
-----
0 0.0.0.0 16 0.0.0.0
1 206.223.51.52 17 0.0.0.0
2 206.223.51.200 18 0.0.0.0
3 0.0.0.0 19 0.0.0.0
4 0.0.0.0 20 0.0.0.0
5 0.0.0.0 21 0.0.0.0
6 0.0.0.0 22 0.0.0.0
7 0.0.0.0 23 0.0.0.0
8 0.0.0.0 24 0.0.0.0
9 0.0.0.0 25 0.0.0.0
Use 10 0.0.0.0 26 0.0.0.0
Use 11 0.0.0.0 27 0.0.0.0
Use 12 0.0.0.0 28 0.0.0.0
Use 13 0.0.0.0 29 0.0.0.0
For 14 0.0.0.0 30 0.0.0.0
Cop 15 0.0.0.0 31 0.0.0.0

Type + or - to change port. Page 3 of 4
Page Up or Page Down for more data. ESC to exit. reserved.

```

Figure 25-8 Ethernet Port Statistical Screen (Page 3)

Below is a list of the currently active registers for the Ethernet Port and the conditions which cause them to be incremented. For a complete table of these registers see page 179. When one of the error registers is incremented, the RED and GREEN FAULT lights on the module will be lit for one second.

- **Packets generated internally.** This register is incremented when the port generates a message to be transmitted from the port to the attached device. This will occur when the CNOE-800 sends a message out the Ethernet port.
- **Internal generations failed (No buffer).** Check the Auto-transfer interval and slow it down. (increase the value).
- **Received ACK of sent segment.** A valid transmission has occurred to the attached Ethernet device.
- **Connection aborted, too many retries.** When the downstream timeout expires, the CNOE-800 will close the connection.
- **Segments retransmitted.** Incremented when a negative acknowledgment or the failure of a positive acknowledgment has occurred after a transmission.

- **Packets lost because unroutable.** Check the route of the sending devices routed to the port. Use the *Last route received* statistics to determine the route incoming on the port.
- **Illegal queries.** Check the command being sent to the port.
- **Local reads.** Incremented when a read request has been received on the port from an external device. This means that the read was routed to the module and operated on the setup register, mailbox register, or statistics registers.
- **Local writes.** Incremented when a write request has been received on the port from an external device. This means that the write was routed to the module and operated on the setup register, mailbox register, or statistics registers.
- **Open connections.** Displays the number of Ethernet devices currently connected to the CNOE-800.
- **Client connection.** Number of open connections for which the CNOE-800 is a client.
- **Unknown Ethernet frame type received.** Incremented when packets that are not Modbus/TCP or SY/MAX 802.3 are transmitted to the CNOE-800.
- **Ethernet frames transmitted.** Incremented when a command, reply, ACK, NAK, or BUSY frame has been transmitted to the Ethernet.
- **Ethernet frames received.** Incremented when a command, reply, ACK, NAK, or BUSY frame has been received from the Ethernet.
- **Last route received.** These eight fields display the route of the last incoming message received by the port. If fewer than eight drop numbers are included in the route, --- will be displayed for each location after the last drop. If messages are received with no route --- will be displayed in all eight locations. If a port has not received any messages, all locations may display 0. When several messages arrive with different routes, this display may jump back and forth between the routes.

It should be noted that since the CNOE-800 is a multitasking system, it may be possible for it to be updating the Last route received while the personal computer is reading those values. The result may be that a route is displayed that is a combination of two or more routes and is therefore not valid. The Last route received is intended for troubleshooting systems where it is unsure what the route is from a particular device.

- **Ethernet collisions.** Incremented when the CNOE-800 has detected a collision between a packet it is sending and other traffic on the network.
- **Buffers in internal cue.** Displays the number of messages waiting in the cue to be processed.
- **Packets lost because excess collisions.** When the collision limit of 16 collisions on a single packet has been exceeded the CNOE-800 will report an error and stop sending the packet.
- **Receive packets lost for CRC error.** Incremented when a receive packet has an error in the checksum.
- **Receive packets lost for framing error.** Incremented when a packet received from the Ethernet has an error in the framing.
- **Sequence error, NAK TRANS.** The CNOE-800 keeps a table of the SY/NET Ethernet Sequence numbers from every active SY/NET Ethernet unit on the network. If the CNOE-800 port receives a packet with an incorrect Sequence number from another device this register is incremented and a NAK TRANS is sent to the offending device.
- **Buffers currently in use.** This number displays the number of buffers that this port is currently using. This number should remain low (0-3). If the Buffers currently in use climbs to near the Buffer limit, the system should be inspected because there is a bottle neck somewhere.
- **Connected IP addresses.** Pages 3 and 4 of the Ethernet statistics show the socket number and IP address of each Ethernet device connected to the CNOE-800.

The backplane port has different types of statistics which are shown in Figures 25-9, 25-10, and 25-11.

C:\WINNT\System32\cmd.exe - rpc

RPC ROUTING PROTOCOL CONVERTER
 Niobrara R&D CRPCTCP 14JAN2003 Port 0 21Jan2003

Statistics

	Count	Register	Quit
BACKPLANE DROP 1			
Replies received from backplane	0	2145	
Error Responses Generated	0	2146	
Replies to MSTR discarded	0	2147	
Messages generated by backplane	0	2148	
Port unable to get buffer	0	2149	
Memory access messages sent to PLC	0	2150	
No context available for new MSTR	0	2151	
Count of active MSTR blocks	0	2152	
Message discarded	0	2153	
Bad Message Format	0	2154	
Backplane MB Channel message w/logon	0	2155	
Backplane MB Channel message w/o logon	0	2156	
PLC memory access message serviced	1	2157	
MSTR operation initiated	0	2158	
Port expired the programming connection	0	2159	
Unsupported MSTR opcode	0	2160	
MSTR operation finished	0	2161	

Type + or - to change port. Z to zero. Page 1 of 3
 Page Up or Page Down for more data. ESC to exit. reserved.

Figure 25-9 Backplane Port Statistical Screen (Page 1)

C:\WINNT\System32\cmd.exe - rpc

RPC ROUTING PROTOCOL CONVERTER
 Niobrara R&D CRPCTCP 14JAN2003 Port 0 21Jan2003

Statistics

	Count	Register	Quit
BACKPLANE DROP 1			
Backplane MB channel message serviced	0	2162	
Error response generated-no rack comms	0	2163	
Last route received	0	2172	
	0	2172	
	0	2173	
	0	2173	
	0	2174	
	0	2174	
	0	2175	
	0	2175	
End-of-scan hooks	4110	2165	
User Logic Hooks	0	2166	
Power up Hooks	1	2169	
Exit Dim Hooks	1	2170	
Programming logon claimed	0	2168	
Buffers in internal queue	0	2167	
Buffers currently in use	0	2176	

Type + or - to change port. Z to zero. Page 2 of 3
 Page Up or Page Down for more data. ESC to exit. reserved.

Figure 25-10 Backplane Port Statistical Screen (Page 2)

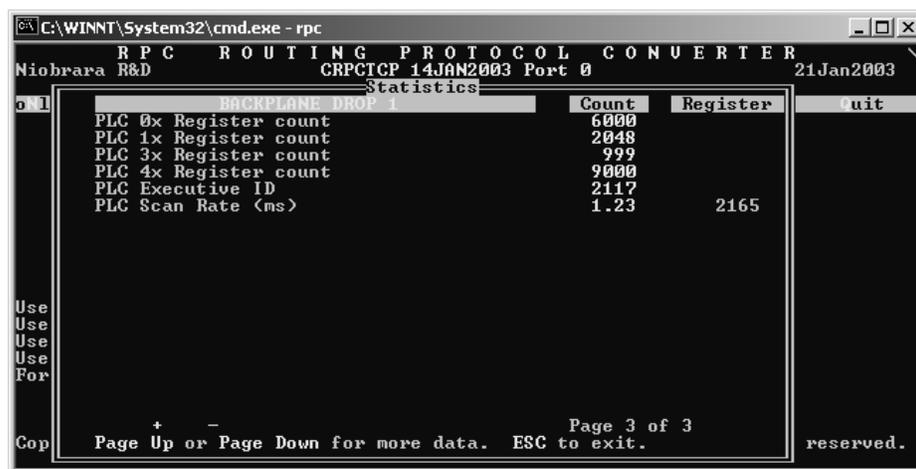


Figure 25-11 Backplane Port Statistical Screen (Page 3)

Below is a list of the currently active registers for the BackplanePort and the conditions which cause them to be incremented.

For a complete table of these registers see page 182. When one of the error registers is incremented, the RED and GREEN FAULT lights on the module will be lit for one second.

- **Replies received from backplane.** This register is incremented when a reply is received from the PLC on the backplane.
- **Error Responses Generated.** This increments each time an error is created by the CNOE-800 on the backplane.
- **Replies to MSTR discarded.** Increments when a message is out of context. The timeout may be too short.
- **Messages generated by backplane.** Increments each time the CNOE-800 generates a message on the backplane.
- **Port unable to get buffer.** This will happen if the CNOE-800 runs out of buffers on the backplane. This should never happen. If it does, please call Niobrara tech support.
- **Memory access messages sent to PLC.** This is incremented when there is a message sent to a queue to be serviced by the PLC.
- **No context available for new MSTR.** Incremented when a fifth MSTR has been activated by the ladder logic. The MSTR can't go active until another MSTR releases the resources.
- **Count of active MSTR blocks.** Running count of the number of currently active MSTR's.
- **Message discarded.** Increments if a message coming from the Ethernet device was untranslatable to the PLC.

- **Bad message format.** Any bad message (bad checksum, framing error, etc.) will increment this count.
- **Backplane MB Channel message w/logon.** When multiple masters are connected to the PLC, only one can be "logged on." This count increments when the logged on master sends a message.
- **Backplane MB Channel message w/o logon.** Increments when any master that is not logged on sends a message to the PLC.
- **PLC memory access message serviced.** Increments when a message in the queue gets serviced by the PLC.
- **MSTR operation initiated.** Increments when the PLC issues an MSTR instruction.
- **Port expired the programming connection.** Increments when the programming channel idle timer expires. For more details, see page 153
- **Unsupported MSTR opcode.** Increments when an MSTR is issued with an unsupported opcode.
- **MSTR operation finished.** Increments when an MSTR is completed.
- **Backplane MB channel message serviced.** Increments when a message is serviced by the PLC on the backplane Modbus channel.
- **Error response generated-no rack comms.** The CNOE-800 boots much faster than the PLC. This register will increment if a master tries to issue a message to the PLC before it has booted, and begun talking to the CNOE-800. This could also increment if the CNOE-800 is in a rack with no PLC, or a PLC with the wrong exec.

Note: The error generated will be x0A, which is "Gateway Path Unavailable."

- **Last route received.** These eight fields display the route of the last incoming message received by the port. If fewer than eight drop numbers are included in the route, --- will be displayed for each location after the last drop. If messages are received with no route --- will be displayed in all eight locations. If a port has not received any messages, all locations may display 0. When several messages arrive with different routes, this display may jump back and forth between the routes.

It should be noted that since the CNOE-800 is a multitasking system, it may be possible for it to be updating the Last route received while the personal computer is reading those values. The result may be that a route is displayed that is a combination of two or more routes and is therefore not valid. The Last route received is intended for troubleshooting systems where it is unsure what the route is from a particular device.

- **End-of-scan hooks.** Increments each time the PLC sends an end of scan hook.
- **User Logic Hooks.** Increments each time the PLC scans an MSTR that has the enable input energized.
- **Exit Dim Hooks.** Increments as the PLC is powering up.
- **Programming logon claimed.** Remains 0 if there is no master logged into the PLC.
- **Buffers in internal queue.** Displays the number of messages waiting in the queue to be processed.
- **Buffers currently in use.** This number displays the number of buffers that this port is currently using. This number should remain low (0-3). If the Buffers currently in use climbs to near the Buffer limit, the system should be inspected because there is a bottle neck or inefficient ladder code somewhere.
- **PLC 0x Register count.** The count of 0x registers configured in the PLC.
- **PLC 1x Register count.** The count of 1x registers configured in the PLC.
- **PLC 3x Register count.** The count of 3x registers configured in the PLC.
- **PLC 4x Register count.** The count of 4x registers configured in the PLC.
- **PLC Executive ID.** Displays the Executive ID reported by the PLC to the backplane.

- **PLC Scan Rate (ms).** This number is calculated by RPCSW32. The CNOE-800 keeps track of the time between end of scan hooks. Each time RPCSW32 reads this value, it adds it to the total, and averages the scan time. If there is an unreasonable number in this register, the user should zero the count by pressing "0" or "z." Keep in mind that pressing one of these keys will reset all statistics for this port.

Ports 1 and 2 have the same types of statistics which are shown in Figures 25-9 and 25-10.

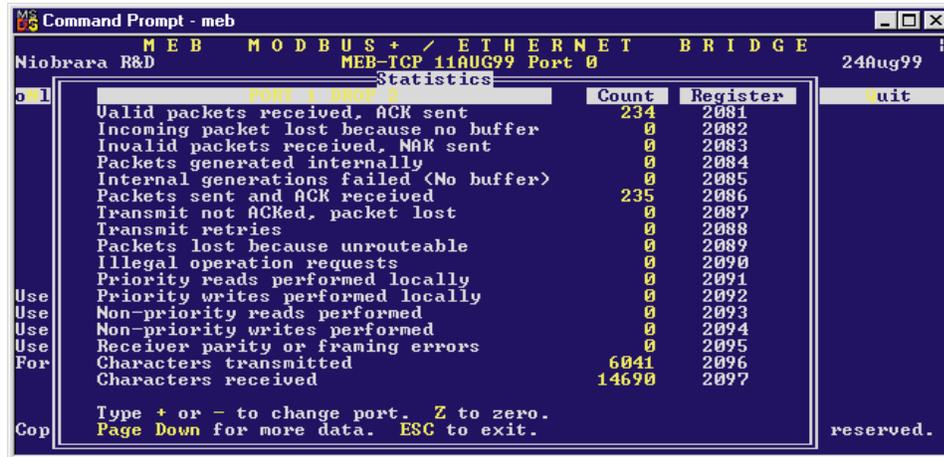


Figure 25-12 Port 1..2 Statistical Screen (Page 1)

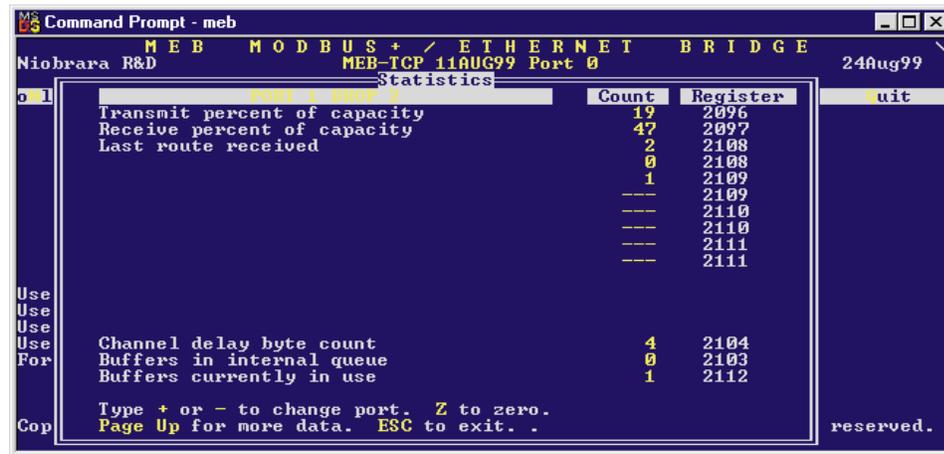


Figure 25-13 Port 1,2 Statistical Screen (Page 2)

Below is a list of the currently active registers for Ports 1 and 2 and the conditions which cause them to be incremented.

For a complete table of these registers see page 182. When one of the error registers is incremented, the RED and GREEN FAULT lights on the module will be lit for one second.

- **Valid packets received, ACK sent.** This register is incremented when a valid packet is received from an external source connected to the port.
- **Incoming packet lost because no buffer.** If this register increments, check the cabling on that port or the target port for the routed message. If CTS is not properly jumpered, the port will not be able to transmit and the buffers will fill. Use the *Utility, CTS Monitor* to check the state of CTS it should be ON.

This register may also be incremented as a result of trying to exceed the throughput of the port. This may happen if several high baud rate sources are routed to a low baud rate target. Try slowing down the polling of the high baud rate sources. Check the *percent of capacity* on the transmit and receive lines on the ports that the message is routed through. Also check the buffer limit setting. The default value is 16. If this setting is set to a lower value, A burst of a few messages may fill the available allocated buffers. Check the *Buffers currently in use* statistic to see how many buffers are full.

- **Invalid packet received, NAK sent.** If this register increments, check the parity settings, or the BCC/CRC settings on the module and the attached devices. Telephone line interference or flow control settings (XON/XOFF) on a modem might cause NAKs to be sent.
- **Packets generated internally.** This register is incremented when the port generates a message to be transmitted from the port to the attached device. This may occur from an Auto-transfer READ or WRITE or by a translation like IDEC or MODBUS.
- **Internal generations failed (No buffer).** Check CTS wiring. Check the Auto-transfer interval and possibly slow it down (increase the value).
- **Packet sent and ACK received.** A valid transmission has occurred to the attached device.
- **Transmit retries exhausted, packet lost..** If errors occur on the transmission, eventually the retries will be exhausted and the transmission will fail. Check the cabling, and communication parameters (baud rate, parity, data bits, stop bits, mode).
- **Transmit retries.** Incremented when a negative acknowledgment or the failure of a positive acknowledgment has occurred after a transmission.
- **Packets lost because unrouteable.** Check the route of the sending devices routed to the port. Use the *Last route received* statistics to determine the route incoming on the port.
- **Illegal operation request.** Check the command being sent to the port.
- **Priority reads performed locally.** Incremented when a Priority read has been received on the port from an external device. This means that the read was routed to the module and operated on the setup register, mailbox register, or statistics registers.
- **Priority writes performed locally.** Incremented when a Priority write has been received on the port from an external device. This means that the write was routed to the module and operated on the setup register, mailbox register, or statistics registers.
- **Non-Priority reads performed.** Incremented when a Priority read has been received on the port from an external device. This means that the read was routed to the module and operated on the setup register, mailbox register, or statistics registers.
- **Non-Priority writes performed.** Incremented when a Non-Priority write has been received on the port from an external device. This means that the write was routed to the module and operated on the setup register, mailbox register, or statistics registers.
- **Receiver parity or framing.** Check the baud rate, parity, data bits, and stop bits.
- **Characters transmitted.** Incremented when a BYTE of information is transmitted from the port.
- **Characters received.** Incremented when a BYTE of information is received to the port.
- **Transmit percent of capacity.** This is a time averaged calculation of the percent of theoretical throughput of the port. This calculation is based upon the Characters transmitted within a certain time and takes into account the baud rate, number of data bits, stop bits, and parity bits.

This average is reset each time page 2 of the statistics is entered, when the port monitored is changed, or when the z or 0 key has been used to zero the statistics fields. Due to the latency between the personal computer performing the read and the reply returning, it is possible to witness values greater than 100%. Since each reading by the personal computer is included in the average allowing this statistic to run for a few minutes will report a more accurate value.

- **Receive percent of capacity.** This is a time averaged calculation of the percent of theoretical throughput of the port. This calculation is based upon the Characters received within a certain time and takes into account the baud rate, number of data bits, stop bits, and parity bits.

This average is reset each time page 2 of the statistics is entered, when the port monitored is changed, or when the z or 0 key has been used to zero the statistics fields. Due to the latency between the personal computer performing the read and the reply returning, it is possible to witness values greater than 100%. Since each reading by the personal computer is included in the average allowing this statistic to run for a few minutes will report a more accurate value.

- **Last route received.** These eight fields display the route of the last incoming message received by the port. If fewer than eight drop numbers are included in the route, --- will be displayed for each location after the last drop. If messages are received with no route --- will be displayed in all eight locations. If a port has not received any messages, all locations may display 0. When several messages arrive with different routes, this display may jump back and forth between the routes.

It should be noted that since the QUCM is a multitasking system, it may be possible for it to be updating the Last route received while the personal computer is reading those values. The result may be that a route is displayed that is a combination of two or more routes and is therefore not valid. The Last route received is intended for troubleshooting systems where it is unsure what the route is from a particular device.

- **Channel Delay byte count.** This value displays the number of bytes including PADs and ENQs sent after the checksum of a SY/MAX message and before an acknowledgment is received. This value is quite helpful in fine-tuning modem applications as it displays the delay time in the modem circuit. Pressing the "T" key on the keyboard will take the reading from the Channel Delay byte count register, add 10 to this value, and write this new value to the PAD count control register for that serial port.
- **Buffers in internal Queue.** This value displays the number of messages in queue waiting to be sent out of this port. On a single-threaded protocol mode such as PNIM, PLOGIC, RNIM, Modbus Host or Gate, or Chevron, this value will show how many messages are waiting to be sent out the port and a value larger than 0 or 1 may appear.
- **Buffers currently in use.** This number displays the number of buffers that this port is currently using. This number should remain low (0-3). If the Buffers currently in use climbs to near the Buffer limit, the system should be inspected because there is a bottle neck somewhere. Use the percent of throughput statistic on the ports included in the route statement to see if any are near 100%. If so try to increase the throughput by increasing the baud rate on that section, lowering the baud rate or polling interval of the previous sections, or routing through alternate paths.

Modbus Slave Routing

CNOE-800 serial ports in Modbus Host, Modbus Gate, or Modbus ASCII modes are capable of operating as a MODBUS RTU (or ASCII) Slave as well as a Master. As a Slave, the CNOE-800 port will respond to Modbus messages based upon a look-up table. Each entry of the look-up table is indexed off of the Modbus Slave address of the incoming message. If the entry in the look-up table is non-empty, the CNOE-800 will translate the Modbus message into a SY/MAX message with the SY/NET route from the entry in the table. If the entry is empty, the CNOE-800 port will ignore the message. Each CNOE-800 port has a Modbus address look-up table with 128 possible entries. These entries consist of a SY/MAX route that may have up to 8 drops and for each Modbus Slave address.

When the oNline, edit Modbus routing screen or the oFfline, edit Modbus routing screen is selected, the Modbus Slave look-up table may be easily edited. Figure 25-14 displays an example of this screen for

serial port 1 of the CNOE-800. This screen allows the editing of the table for each CNOE-800 port, the range of Modbus address that the table covers, and the entries for each of the covered addresses.

```

MS Command Prompt - meb
MEB MODBUS + / ETHERNET BRIDGE
Niobrara R&D MEB-TCP 11AUG99 Port 0 24Aug99
CONFIGURATION AND UTILITY SOFTWARE
oNline o fline tility etup Quit
MODBUS ROUTING FOR PORT 1, START ADDRESS = 1
ADDRESS ROUTE
1 OTHER 101,5,2
2 OTHER 101,5,14
3 OTHER NONE
4 OTHER NONE
5 OTHER NONE
6 OTHER NONE
7 OTHER NONE
8 OTHER NONE
9 OTHER NONE
10 OTHER NONE
11 MODBUS 101,5,12,41,1
12 OTHER NONE
13 OTHER NONE
14 OTHER NONE
15 OTHER NONE
16 OTHER NONE
Type digits to enter route. F4 to edit start address.
Use + and - to select port. Escape to exit.

```

Figure 25-14 Edit Modbus Slave Routing

Port Number

Each CNOE-800 serial port has its own Modbus Slave look-up table. The + and - keys are used to select the CNOE-800 port table for editing.

Starting Address

The CNOE-800 Modbus port look-up table covers a range of 128 consecutive addresses. The starting point of this range may be adjusted with the Starting Address value. The Home key is used to edit the Starting Address. The lowest setting allowed is 0 and the highest setting should be 129. Normally this value will be set for 1 or 129.

Address

The Address column displays the Modbus Address for which the entry corresponds. The starting and ending point of this column is governed by the Starting Address setting.

Target TYPE

The target type may be set to MODBUS or OTHER. If the device is a SY/MAX device then set it to OTHER.

ROUTE

The Route column determines the SY/NET route to the target device. The entries are separated by commas. The first entry should be the SY/NET drop number of this Slave port.

In Figure 25-14 above, incoming Modbus messages to slave #1 will be translated to SY/MAX messages with the route 101, 5, 2. Modbus messages to slave #2 will be sent out as SY/MAX messages with the route 101, 5, 14 while messages to Slave 11 will have the route 101, 5, 104, 41, 1. Messages to addresses 2, 3, 4...10 and 12, 13, 14, 15 and 16 will be ignored by the CNOE-800.

Modbus Server Routing for Ethernet Port

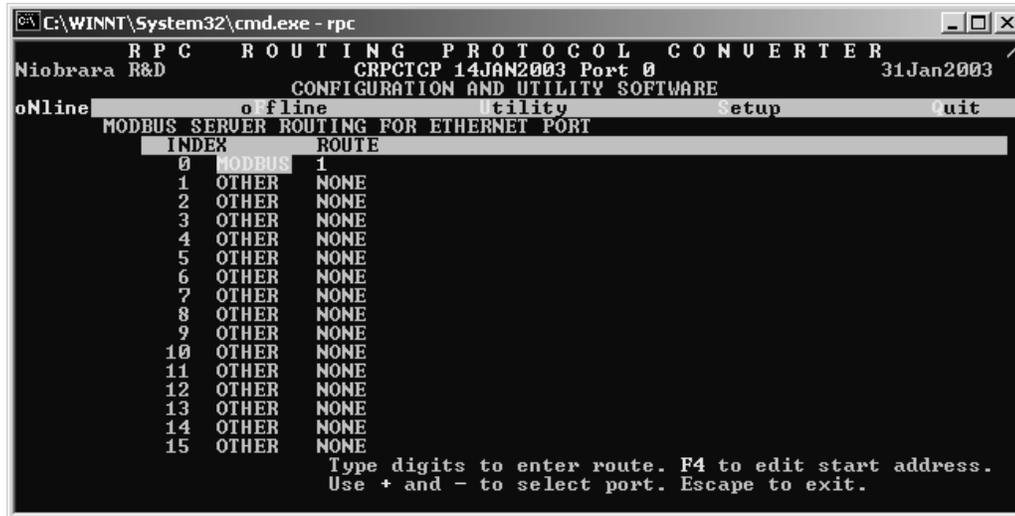


Figure 25-15 Modbus Server Routing for Ethernet Port

(Modbus/TCP only) The CNOE-800 can act as a Server as well as a Client for Modbus TCP/IP protocols. As a Server, incoming Modbus TCP/IP messages are handled in relation to the Modbus Routing table. The Destination Index of the incoming message is checked for an entry in the Modbus Routing table for the Ethernet port and if present, routes the message appropriately. This screen is selected by "edit Modbus routing" and pressing the "-" key until the Ethernet port is displayed.

NOTE: Since the IP address of the CNOE-800 is unique, there is no possibility that incoming messages are intended for another device. Therefore, all incoming messages with Index values that have empty entries will be acted upon locally by the CNOE-800.

Index

The Index column displays the Modbus Destination Index for which the entry corresponds. The Destination Index is a single byte of routing information with a valid range of 0-255. The CNOE-800 supports all 255 entries for this index. Index 255, which would be the 256th entry, is a special drop that always refers to the CNOE-800. Messages with empty Index values will be treated as local operations.

Target TYPE

The target type may be set to MODBUS or OTHER. If the device is a SY/MAX device then set it to OTHER.

ROUTE

The Route column determines the SY/MAX route to the target device. The entries are separated by commas. The first entry should be the SY/MAX drop number of the outgoing port of the CNOE-800 (Enet or backplane).

In Figure 25-15 above, incoming Modbus TCP/IP messages to Index #0 will be sent to the PLC. This is the default setting. The route may be changed, but must be the drop number of the backplane port in order to send messages to the PLC. Messages to any other index will be handled by the CNOE-800.

Auto-Scan Table

The CNOE-800 serial port modes which may be used with Auto-Scan may also be configured for Auto-Scan. The Auto-Scan entries include pointers to the Local (CNOE-800 mailbox register), Remote (peripheral device register), Count, type of operation (READ or WRITE), and the Route to the peripheral.

Up to 48 entries may be include per port. Figure 25-17 displays an example of the Auto-Scan edit screen.

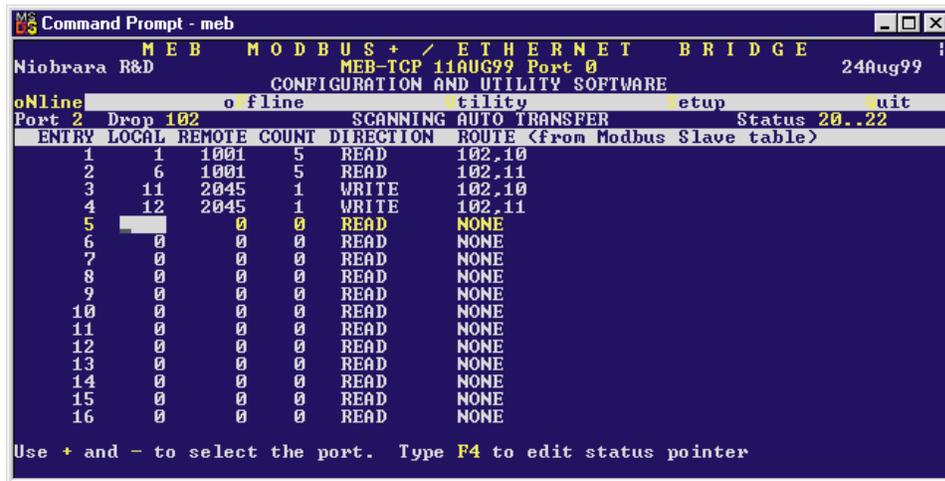


Figure 25-16 Edit Auto-Scan Table

Local

This value determines the mailbox register in the CNOE-800 that is the starting register for the operation. The valid range is 1 through 2048. A value of 0 disables the Auto-Scan entry.

Remote

This value determines the register in the Peripheral device that is the starting register for the operation. The valid range is 1 through 8192. A value of 0 disables the Auto-Scan entry.

Count

The Count field determines the number of consecutive registers moved in the operation. The valid range is 0 through 128. A value of 0 disables the Auto-Scan entry.

Operation

This setting is set to READ or WRITE depending on the operation desired. READ operations copy data from the peripheral device to the CNOE-800's mailbox. WRITE operations copy data from the CNOE-800's mailbox to the peripheral device.

ROUTE

The Route column determines the SY/NET route to the target device. The entries are separated by commas. The first entry should be the SY/NET drop number of this Slave port.

Ethernet I/O Scanner

The CNOE-800's Ethernet port can be set up to automatically poll other Ethernet devices. The I/O scan entries include pointers to the Remote IP address, ID (Index), Timeout (in ms), Scan Rate (in ms), Read Register space (0x, 1x, 3x, 4x) and offset for Master (CNOE-800) and slave (downstream device), Write Register space (0x, 1x, 3x, 4x) and offset for Master (CNOE-800) and slave (downstream device), Count, and value retention (Hold, or 0). Up to 128 entries may be specified. Figure 25-17 displays an example of the Auto-Scan edit screen.

#	IP Address	ID	Time-out	Scan rate	Master	Slave	Cnt	H/O	Master	Write	Slave	Cnt
1	0.0.0.0	0	0	0	4x000001	4x000001	0	HLD	4x000001	4x000001	4x000001	0
2	0.0.0.0	0	0	0	4x000001	4x000001	0	HLD	4x000001	4x000001	4x000001	0
3	0.0.0.0	0	0	0	4x000001	4x000001	0	HLD	4x000001	4x000001	4x000001	0
4	0.0.0.0	0	0	0	4x000001	4x000001	0	HLD	4x000001	4x000001	4x000001	0
5	0.0.0.0	0	0	0	4x000001	4x000001	0	HLD	4x000001	4x000001	4x000001	0
6	0.0.0.0	0	0	0	4x000001	4x000001	0	HLD	4x000001	4x000001	4x000001	0
7	0.0.0.0	0	0	0	4x000001	4x000001	0	HLD	4x000001	4x000001	4x000001	0
8	0.0.0.0	0	0	0	4x000001	4x000001	0	HLD	4x000001	4x000001	4x000001	0
9	0.0.0.0	0	0	0	4x000001	4x000001	0	HLD	4x000001	4x000001	4x000001	0
10	0.0.0.0	0	0	0	4x000001	4x000001	0	HLD	4x000001	4x000001	4x000001	0
11	0.0.0.0	0	0	0	4x000001	4x000001	0	HLD	4x000001	4x000001	4x000001	0
12	0.0.0.0	0	0	0	4x000001	4x000001	0	HLD	4x000001	4x000001	4x000001	0
13	0.0.0.0	0	0	0	4x000001	4x000001	0	HLD	4x000001	4x000001	4x000001	0
14	0.0.0.0	0	0	0	4x000001	4x000001	0	HLD	4x000001	4x000001	4x000001	0
15	0.0.0.0	0	0	0	4x000001	4x000001	0	HLD	4x000001	4x000001	4x000001	0
16	0.0.0.0	0	0	0	4x000001	4x000001	0	HLD	4x000001	4x000001	4x000001	0

Figure 25-17 Edit Auto-Scan Table

IP Address

This is the IP address of the device or bridge to be polled.

ID

This is the device address or bridge index of the device to be polled.

Timeout

This value determines the timeout, in milliseconds, before the CNOE-800 expires the operation.

Scan Rate

This value determines how often, in milliseconds, the CNOE-800 will poll the device.

Register Space

This column precedes the Master and Slave columns for both Read and Write. Although this column has no heading, it allows the user to choose the register space in the device to be polled. Valid choices are 0x, 1, 3x, and 4x. Default is 4x. Press the space bar to toggle, or press 0, 1, 3, or 4 to select.

Master (Under Read or Write)

This value determines the mailbox register in the CNOE-800 that is the starting register for the operation. The valid range is 1 through 2048. A value of 0 disables the I/O scan entry.

Slave (Under Read or Write)

This value determines the register in the Peripheral device that is the starting register for the operation. The valid range is 1 through 8192. A value of 0 disables the I/O scan entry.

Cnt (Under Read or Write)

The Count field determines the number of consecutive registers moved in the operation. The valid range is 0 through 120. A value of 0 disables the Auto-Scan entry.

H/O

This setting is set to HLD or 0, depending on the desired function. If set to HLD, the CNOE-800 will hold the value of the last read when the next read times out. If set to 0, the CNOE-800 will reset the register to 0 if a timeout occurs.

NOTE: If a read and a write are configured in the same I/O scan entry, the CNOE-800 will use

Modbus opcode 23, or x17, to issue a read/write in the same message. If the downstream device does not support this opcode, the the user must configure the reads and writes in separate entries.

Outgoing TCP Routing

(Modbus/TCP and MBTCP+SY/MAX only) The "edit Tcp routing" screen allows editing of the table that maps SY/MAX drop numbers (0-199) to IP addresses. The drop in the route following that of the Ethernet port of the CNOE-800 is used as an index in this table to point to a specific IP device.

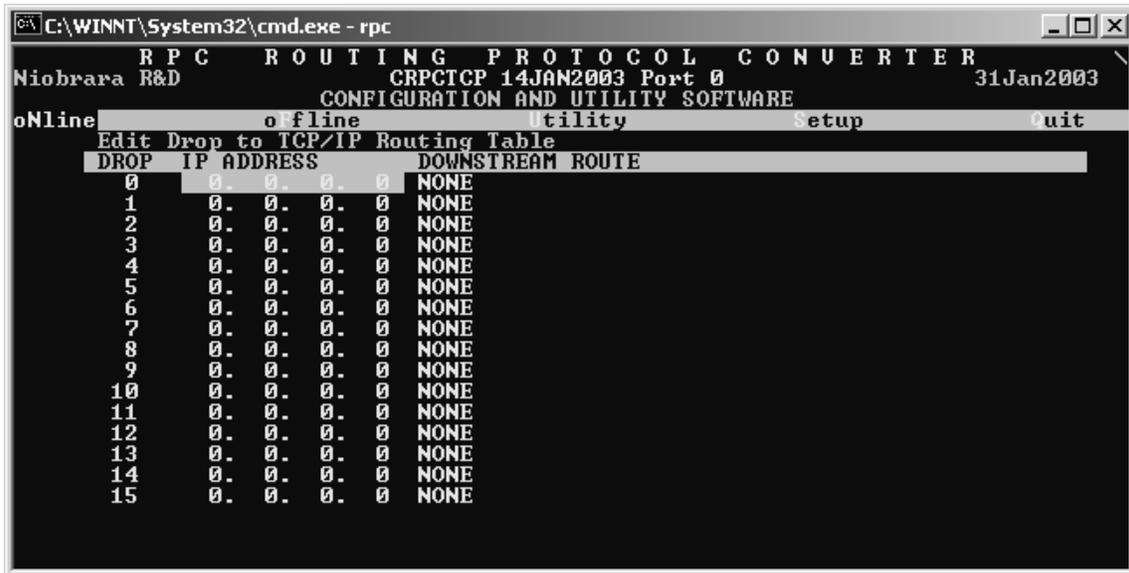


Figure 25-18 Edit TCP Routing

Drop

The Drop entry refers to the SY/MAX drop number 0 through 199.

IP Address

The IP Address is the dotted decimal representation for the target server.

Downstream Route

The Downstream Route is an optional additional route that is added after the index drop number and may be up to one layer deep in Modbus/TCP.

Offline Functions

"Read from disk to memory"

This function reads an CNOE-800 configuration file into the offline memory. The file should have been created by the "Write from memory to disk" function described below and must have a .RPC extension. When "Read from disk to memory" is selected, a window will open and ask for the name of the file to read. The bottom part of the screen will show a list of all files with the extension .RPC in the current directory. Any subdirectories will be shown in square brackets. Any drive names will also be shown in square brackets, [b:]. The parent directory (of which the current directory is a subdirectory) is shown by the word "parent" in square brackets. You may either type the name of the file to read or you may use the arrow keys to move the highlight to the desired filename. Pressing **ENTER** with the highlight on a filename will select that file for reading. Pressing **ENTER** with the highlight positioned on a directory (drive) name (either a subdirectory or [parent]) will change the current directory (drive) to that directory (drive) and will show the .RPC files in the new directory (drive). If there are more

files than will fit on the screen, pressing the right arrow with the highlight at the right edge of the screen will scroll the display sideways to show more files. Typing the **ESC** key will return to the offline function menu without loading a file or otherwise modifying offline memory.

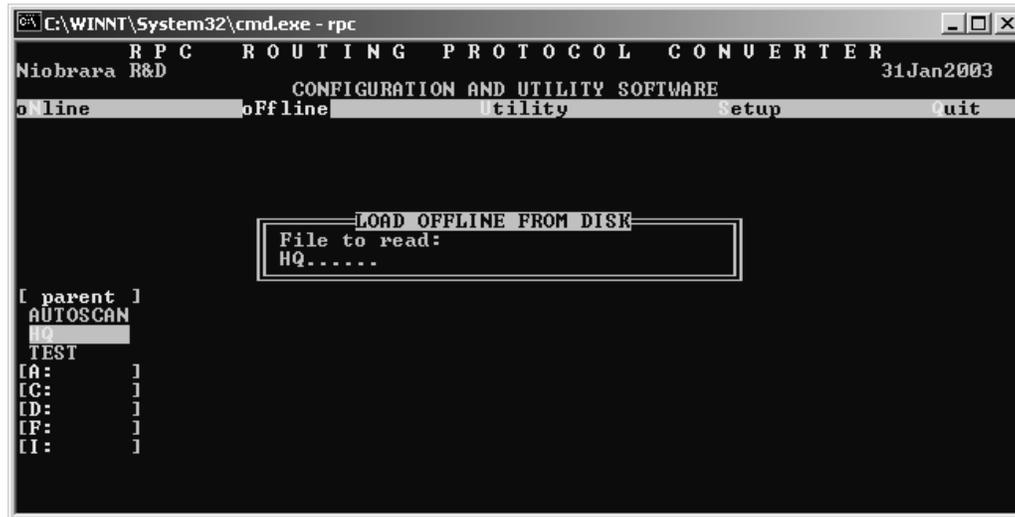


Figure 25-19 oOffline Read from Disk to Memory

"Write from memory to disk"

This function saves a copy of the two ports, the I/O scan table, and global configuration parameters from the offline memory to a disk file. "Write from memory to disk" uses the same point and shoot file selection described for "Read from disk to memory" above. To create a new file you must type the name. The name should be a valid MS/DOS filename (containing no more than eight characters, and no spaces) but should not include any path name or extension. The program will append an extension of .RPC to the name and the file will be placed in the directory which is shown in the bottom half of the screen. To create a file in a directory other than the current one, use the arrow and **ENTER** keys to traverse the directory tree until a listing of the desired directory is shown in the bottom half of the screen. Then type in the file name and press **ENTER**. If you specify (either by typing or by pointing) a file that already exists, you will be prompted for approval before that file is overwritten.

"Edit configuration in memory"

Just like the online portion of the program, this function displays a screen with the parameters for a CNOE-800's ports. As described above, changes here effect the offline memory and not any attached CNOE-800.

"edit Modbus routing"

Just like the online portion of the program, this function displays a screen with the parameters for a CNOE-800's Ethernet port's routing. As described above, changes here effect the offline memory and not any attached CNOE-800.

"edit Ethernet I/O scan table"

Because it would not be desirable to inadvertently change an I/O scan entry in the middle of the scan, all editing of the I/O scan table is done offline. The editing is as described above.

"edit TCP routing"

Just like the online portion of the program, this function displays a screen with the parameters for a CNOE-800's Ethernet port's TCP routing. As described above, changes here effect the offline memory and not any attached CNOE-800.

"Send memory to module"

This function will send the configuration in memory to the CNOE-800 module by way of the serial setup parameters. In order to send the configuration to the CNOE-800 it is necessary for the personal computer to communicate with the CNOE-800. Try going oNline before sending a configuration.

Be cautious when sending a configuration. Go oNline and notice IP Address and protocol the module's Ethernet port. Examine the configuration before sending to make sure that the IP address and protocol not change from the current settings, otherwise communication may be lost during the send.

"Fetch memory from module"

Use this function when you wish to copy the configuration parameters from a connected CNOE-800 module to the offline memory for editing, printout, or saving on disk.

"Print configuration in memory"

This function will produce a report showing the settings of all parameters in offline memory. When this function is selected, you will be prompted for an output filename with the default value of PRN shown. To send the report to the PRN device (normally the parallel printer port), simply press **ENTER**. To send the report to a different port or to a file, type the name and then press **ENTER**. Online configurations may be printed with the **F1** print screen key.

"Delete configuration file"

This function will show a point and shoot menu of the available .RPC configuration files. Select the file to be deleted and press **ENTER**.

"Quit offline functions"

Selecting the quit item will cause a return to the main menu bar. Pressing the **ESC** key will have the same effect.

Utilities

The Utilities menu provides access to useful maintenance and testing functions of the RP-CSW32software.

View registers

Selecting the View registers menu item will invoke a SY/MAX register data viewer/modifier. This viewer continuously performs a block read of 20 registers and displays the contents of those registers in hex, unsigned integer, signed integer, and binary. The status register associated with the data register is also displayed in hex. Like any other oNline or oFfline function involving communication, the register viewer is dependent on the values located in the **SETUP** Serial menu. Mode, IP address, etc. must be properly set for proper communication.

REGSTR	HEX	UNSIGN	SIGNED	BINARY				STAT
8173	0000	0	0	0000	0000	0000	0000	
8174	0001	1	1	0000	0000	0000	0001	
8175	0000	0	0	0000	0000	0000	0000	
8176	8000	32768	-32768	1000	0000	0000	0000	
8177	4352	17234	17234	0100	0011	0101	0010	
8178	5043	20547	20547	0101	0000	0100	0011	
8179	5443	21571	21571	0101	0100	0100	0011	
8180	5020	20512	20512	0101	0000	0010	0000	
8181	3134	12596	12596	0011	0001	0011	0100	
8182	4A41	19009	19009	0100	1010	0100	0001	
8183	4E32	20018	20018	0100	1110	0011	0010	
8184	3030	12336	12336	0011	0000	0011	0000	
8185	3320	13088	13088	0011	0011	0010	0000	
8186	2020	8224	8224	0010	0000	0010	0000	
8187	0003	3	3	0000	0000	0000	0011	
8188	9990	39312	-26224	1001	1001	1001	0000	
8189	0000	0	0	0000	0000	0000	0000	
8190	0000	0	0	0000	0000	0000	0000	
8191	0000	0	0	0000	0000	0000	0000	
8192	0000	0	0	0000	0000	0000	0000	

Figure 25-20 View Registers

The Up and Down arrow keys are used to move from register to register.

The Page Up and Page Down keys move in increments of 10 registers.

The Left and Right arrows move from column to column on the same register.

Pressing the F9 key will present the Serial setup window. This is useful for changing the route or other parameters without returning to the main menu.

This register viewer is highly useful in that it allows easy editing of the data in the register being viewed. By pressing 0..9 in the decimal fields or 0..9, or A..F in the hex field, an editing mode is entered. New data may be entered at this time. Pressing the Enter key or moving to a new field with the arrow keys will cause the new data to be written to the edited register. If the cursor is located in the REGISTER column the block of registers being viewed may be adjusted by entering a new register number. To edit the binary values, press HOME when on the binary field. Move the cursor to the desired bit and enter a '0' or a '1' and press enter to accept.

Pressing Esc will exit from the Register viewer and return to the main menu. Pressing Esc while editing a data field will result in canceling the edit and the modified data will not be written to the register.

Terminal Emulator

Selecting the Terminal emulator from the Utilities menu will invoke a terminal emulator according to the setup selected in the Setup menu. The terminal emulator opens as shown in Figure 25-21.

```
Type ctrl-End to exit terminal. Type F7 to begin capture to a file.
Type F9 to change terminal communication setup.
To send hex sequence, type INSERT key, enter hex codes, type ENTER.
r1<0D>
0<0D>
r1,10<0D>
0 0 32768 0 0 0 0 4660 65278 1234<0D>
w12,55,67<0D>
<0D>read12<0D>
55<0D>
s12.1<0D>
<0D>r12<0D>
55<0D>
s12.16<0D>
<0D>r12<0D>
32823<0D>
c12.1<0D>
<0D>r12<0D>
32822<0D>
Enter hex codes to send: 10 05
<10><05>█
```

Figure 25-21 Terminal Emulator

The terminal sends the ASCII code for the alpha-numeric characters out the selected COM port. Functions keys F1 through F4 and the keypad arrows send ANSI (i.e. VT100) codes. F7 is reserved for starting a file capture. F8 will close the capture file. The backspace key sends ASCII BS (08 hex). The Delete key sends and ASCII DEL (7F hex). The Insert key allows the transmission of ASCII hexadecimal characters directly from the hex numbers separated by spaces.

The terminal displays printable ASCII characters which are received on the port. Non-printable characters are displayed as the hexadecimal value enclosed in <>, such as <0D><0A> indicates the carriage return, line feed characters. The terminal is always in this "monitor" mode and therefore ANSI output emulation is not provided.

Pressing F9 will invoke the Terminal Emulator Setup window. This is useful for changing the port parameters without returning to the main menu.

SETUP

The setup menu accesses the setup parameters for the personal computer to enable it to communicate with the CNOE-800. The parameters chosen will depend on the exact equipment involved in making the connections. Since the CNOE-800 will most likely be configured directly over Ethernet, we will focus on those parameters.

Serial SETUP

The connection type is mainly determined by the method of connection to outside world and may be broken into two groups: the personal computer's COM: port, and the Network Interface Card.

Personal Computer COM: port

If the connection from the personal computer is made through one of its serial ports then the Connection type should be one of the following:

- Sy/Max COM:
- Net-to-Net COM:
- Gateway COM:
- Modbus RTU COM:
- Modbus ASCII COM:

Sy/Max COM: is the default and most likely will be the one used. In this mode the personal computer will communicate through one of its COM: ports as though it were a SY/MAX device such as a PLC. The full SY/MAX protocol is supported including routing so SY/MAX COM: may be used through SY/MAX mode ports on NIMs and Niobrara Routing Modules with appropriate routing. This mode is to be used when a direct connection from the personal computer COM: port is made to the CNOE-800.

Net-to-Net COM: is used when connecting to a NIM, SY/LINK, CNOE-800, MEB, EPE5, or SPE4 that is set to Net-to-Net mode. The first drop number in the route will be that of the address of the Net-to-Net port.

Gateway COM: is used when connecting to an SPE4/MEB/CNOE-800/EPE5 port that is in Gateway mode. For more information about Gateway mode see on page 99.

Modbus RTU COM: is used when connecting to a port in MODBUS GATE or MODBUS HOST or a Modicon PLC or BM85 Bridge Mux. Only a single drop of routing information is allowed. Use drop 255 when connecting to a CNOE-800 port directly. Modbus RTU mode has strict inter-character timing requirements and may not be suitable for use under Windows NT; try MODBUS ASCII instead.

Modbus ASCII COM: is used when connecting to a port in MODBUS ASCII mode or a Modicon PLC or BM85 Bridge Mux. Only a single drop of routing information is allowed. Use drop 255 when connecting to a CNOE-800 port directly.

Port - When one of the COM: connection types is selected a particular port of the personal computer must be selected. Available choices are: COM1:, COM2:, COM3:, and COM4:. Select the port which will be used to connect to the CNOE-800.

Baud rate - The Baud rate selected here is the baud rate of the personal computer serial port selected. This value should be set to match the device connected to the personal computer. A CNOE-800 has a default baud rate of 9600 and if a direct connection is made to the CNOE-800 this is the setting that should be made on the personal computer. If the baud rate of the port of the CNOE-800 has been changed this value may need to be adjusted.

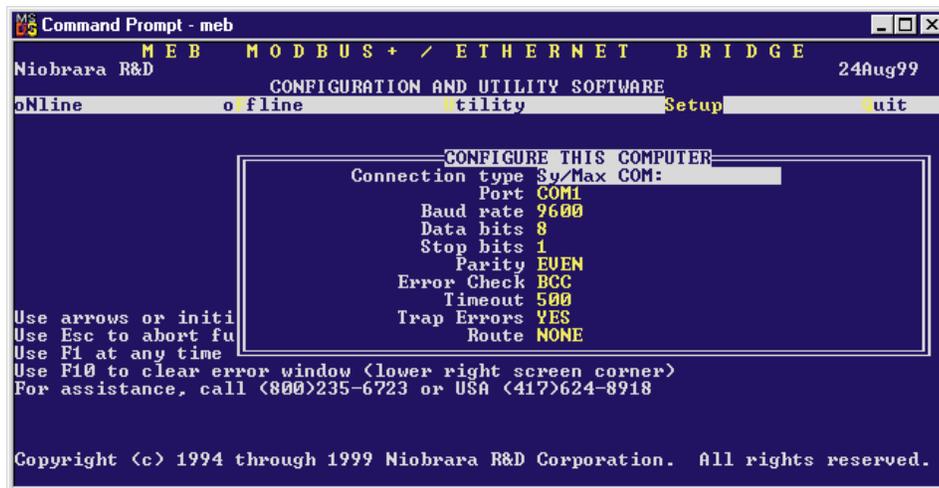


Figure 25-22 SY/MAX Setup Screen

Data bits - When in SY/MAX or Net-to-Net modes the data bits is required to be 8 and may not be changed. The SY/MAX protocol requires 8 data bits. The Gateway and MODBUS ASCII modes use ASCII messages which do not require the full 8 data bits and may be set to 8 or 7 depending on the attached device.

Stop bits - The stop bits are normally set to 1 but may be adjusted to 2 for some particular application. The communication ports of the CNOE-800 are normally set for 1 stop bit.

Parity - SY/MAX, Net-to-Net, Modbus RTU, and Modbus ASCII modes normally use EVEN parity and that is the default for the communication ports on the CNOE-800. Other choices are ODD and NONE.

Route - The route is used to determine the path from the personal computer to the CNOE-800. If a direct connection is made from the personal computer to the CNOE-800, i.e. without going through a SY/NET network, an Ethernet network, another CNOE-800, or an SPE4, this value is set to NONE by pressing the Delete key. If a SY/MAX connection is made to a SY/MAX mode port on an NIM or SPE4 the first drop will be that of the drop number of the NIM or SPE4 port. If any Net-to-Net drops are included between the port connected to the personal computer and the port connected to the CNOE-800, they must be included in order of occurrence from the personal computer to the CNOE-800. The last drop number listed will be that of the NIM or SPE4 SY/MAX mode port that is connected to the CNOE-800. Up to 8 total drops are supported by the SY/MAX protocol.

If the personal computer is in Net-to-Net mode the first drop will be that of the Net-to-Net port of the NIM, SY/LINK, EPE5, or SPE4 that the personal computer is connected to. Subsequent drops will be included as above.

The Gateway mode route will include the Gateway port on the CNOE-800, EPE5 or SPE4 that the personal computer is connected and any subsequent Net-to-Net and SY/MAX drops to reach the CNOE-800.

Modbus/TCP Connection

RPCSW32 provides support of Modbus/TCP via Ethernet directly using the TCP/IP stack of the Windows 95/98/NT/2000/ME/XP operating system.

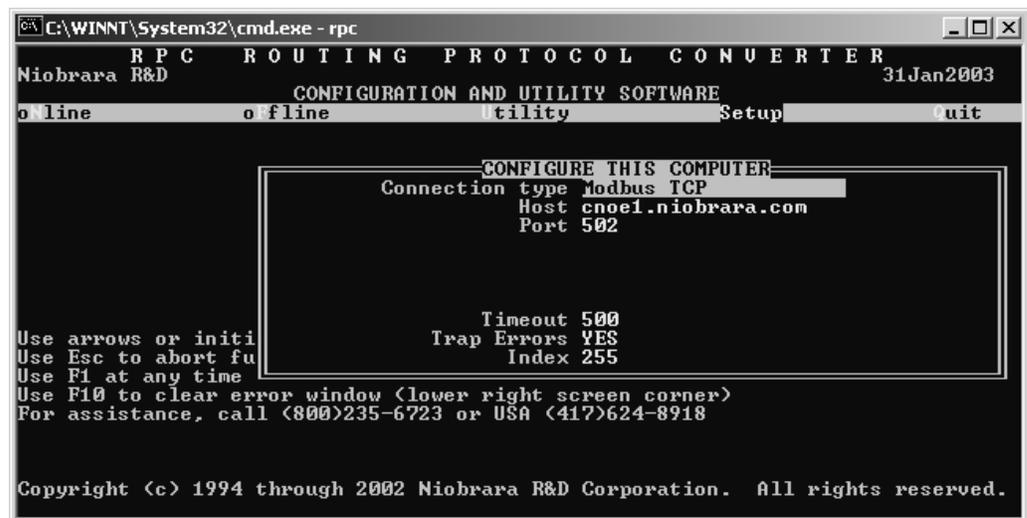


Figure 25-23 MODBUS/TCP Setup Screen

HOST - Enter the dotted-decimal IP address of the CNOE-800 such as 206.223.51.154. If the CNOE-800 has been assigned a name by a DNS server then the name may be entered such as cnoe1.niobrara.com.

PORT - Enter the TCP/IP Port number used by the server. Normally this is 502.

TIMEOUT - Enter the timeout value that RPCSW32 waits for a reply in 1/10 second intervals. 500 means 5 seconds.

TRAP ERRORS - When set to yes RPCSW32 will stop on all errors and wait for the user to press F10 before continuing.

DROP - Enter the Destination Index value to determine the target device. Use 255 when attempting to communicate with the CNOE-800 itself.

Terminal Emulator SETUP

The Terminal Emulator setup allows an individual setup for the operation of the terminal emulator. For instance, this separate setup will allow COM1 to be used for the CNOE-800 SY/MAX connection and COM2 to be used for a terminal emulator connection.

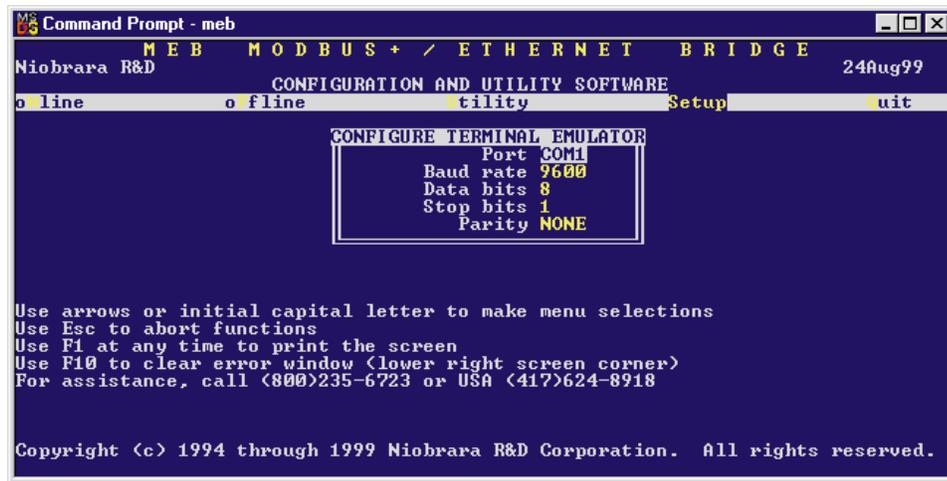


Figure 25-24 Terminal Emulator Setup Screen

Port - Available choices are: COM1:, COM2:, COM3:, and COM4:. Select the port which will be used to connect to the external device.

Baud rate - The Baud rate selected here is the baud rate of the personal computer serial port selected. This value should be set to match the device connected to the personal computer.

Data bits - Selects the number of data bits for the message packet. Choices are 8 or 7 depending on the attached device.

Stop bits - The stop bits are normally set to 1 but may be adjusted to 2 for some particular application.

Parity - Choices are EVEN, ODD, and NONE.

Register Viewer Setup

The Register Viewer Setup allows an individual setup for the operation of the Utility Register Viewer.

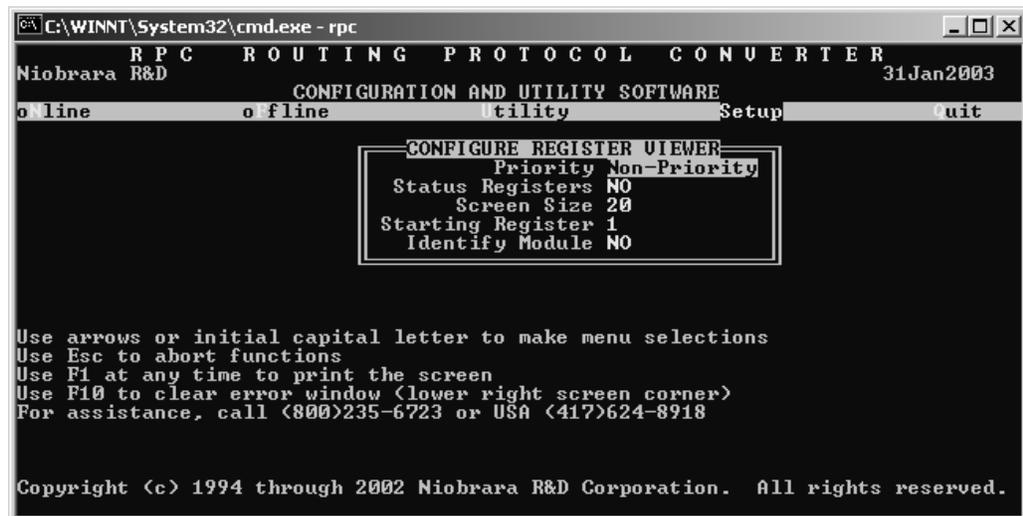


Figure 25-25 Terminal Emulator Setup Screen

Priority - This setting has no effect when connecting Modbus/TCP.

Status Registers - This setting is not useful for the CNOE-800.

Screen Size - Selects the number registers to be read per operation and displayed on the screen. The valid range is 1 through 20 inclusive. The default value is 20.

Starting Register - The starting register value determines the first register polled when the register viewer is entered. The valid range is 1 through 8192 inclusive with the default value of 1.

Identify Module - This option determines if the register 8188 is read in the target device to determine the SY/MAX ID of the target. This setting is not very useful, as all NR&D products return a value of x9990. The default value is NO.

Load from File

The Load from File option allows the user to select from multiple SY/MAX setups. Simply enter the filename of the setup desired and RPCSW32 will use that setup. RPCSW32 always saves the current setup as RPCSW.STP regardless if a new setup has been loaded. The idea is that you configure the setup as you like, save it to RPCSW.STP by selecting Y for yes when prompted, quit RPCSW32 to DOS, and copy RPCSW.STP to a new filename with the extension .STP. The following DOS command copies the RPCSW.STP to a new name RPC01.STP:

```
C:\RPC> copy mebsw.stp meb01.stp
```

Command Line Parameters

RPCSW32 may be started from the DOS command line with a sequence of letters which represent the keystrokes necessary to perform any operation. This allows batch processing of various commands such as downloading of stored setup files. The special characters /R, /D, and /E refer to the Return key, Delete key, and Escape key respectively. The parameters are not case sensitive. The following example loads a new SY/MAX setup RPC01.STP, to perhaps change the route to the RPC, loads the configuration file TEST.RPC into a CNOE-800, then quits. It is assumed that the CNOE-800 is connected to the computer and the rest of RPCSW32 setup is correct.

```
>RPCSW32 SLmeb01/RFRtest/RFSQ
```

The S selects Setup, the L selects Load setup file, meb01 is the filename of the setup, /R is the return to accept the filename, the F is for oFfline, the R is to Read a configuration file, test is the filename, /R is the return to accept the filename, F selects oFfline again, S sends the configuration to the module, and finally Q for Quit.

Local Registers

The CNOE-800 configuration is controlled by writing to a set of processor equivalent registers local to the CNOE-800 module. These registers may be read or written by sending Modbus RTU or Modbus/TCP read and write messages to the module itself. These messages may be generated by any device capable of generating Modbus read and write messages, including the RPCSW32 program provided with the module. In order for the module to know that a message is for the module itself and not to be routed to another port, the index should be 255. The Register Viewer located in the Utility section of the RPCSW32 program is a convenient interface to the module's registers.

Module Register Overview

Table 26-1 represents an overview of the local 4x registers present within the CNOE-800. Notice that, as an I/O module, only registers 1..64 may be rack addressed by the PLC. As an option module, no registers will be rack addressed. All registers must be read or written through MSTR's or via the Ethernet I/O scanner.

Table 26-1 Module 4x Register Overview

Register	Function
1..2048	Mailbox registers for user applications
2049..2176	Statistics Registers (See Table 26-2)
2177..2899	Reserved for future use, do not modify
2900..2995	TCP/IP Address Table
2996..2999	TCP/IP Tuning Parameters
3000..3302	Ethernet Addresses (See Table 26-7)
3303	E-Peer Active Nodes Register
3304	Ethernet Address Poll Register
3410..3699	Auto-Scan Tables
4640..7199	Modbus Slave Address Look-up Tables (See Table 26-2)
7200..7999	TCP/IP Routing Table
8001..8162	Setup and Configuration (See Tables 26-13, 26-14, 26-22)
8176..8188	Module identification (See Table 26-25)

Mailbox Registers

The CNOE-800 contains 2048 Mailbox registers numbered 1...2048. Each of these registers may be written or read from the Ethernet port.

As an I/O module, the first 64 (4x 33-64 are 3x 1-32) of these registers may be rack addressed by the PLC. The mailbox registers correspond to the registers in the PLC by the following formula:

$$\text{PLC Register} = \text{Rack Start Address} + \text{Mailbox Register}$$

For example, if a CNOE-800 is rack addressed to PLC register 4x1050, then PLC register 4x1050 is CNOE register 1, PLC register 4x1051 is CNOE register 2, etc.

It should be noted that any Mailbox registers that are not rack addressed are still available to the external devices for Mailbox use, they just are not scanned by the PLC.

Statistics Registers

Ethernet Port Statistics

The Ethernet port has its own group of 32 statistics registers to give the user an idea of the activity on the Ethernet connection of the CNOE-800. These registers may be cleared by writing a zero. The group of registers for SY/MAX 802 mode is shown in Table 26-2 while TCP/IP is shown in Table 26-3.

Table 26-2 SY/MAX Ethernet Port Statistics Registers

Register	Incremented when the following occurs:
2049	SY/MAX Ethernet commands/replies received.
2050	Incoming E-Net SY/MAX packet lost because no available buffer.
2051	Retry packets received.
2052	Packets generated locally. (Auto-transfer)
2053	Packet generation failed because no available buffer.
2054	Packet transmitted successfully.
2055	Transmission failed.
2056	Transmission retry.
2057	Packet lost because of unrecognized or illegal drop or bad route.
2058	Illegal SY/MAX operation request on local registers.
2059	Priority read received and performed upon local registers.
2060	Priority write received and performed upon local registers.
2061	Non-Priority read received and performed upon local registers.
2062	Non-Priority write received and performed upon local registers.
2063	Non-SY/MAX Ethernet packet received.
2064	Ethernet packets transmitted.
2065	Ethernet packets received.
2066	Ethernet collisions.
2067	Ethernet transmit packets lost to excess collisions.
2068	Ethernet receive packets with CRC error.
2069	Ethernet receive packets with framing error.
2070	Ethernet NAK TRANS sent (Sequence error).
2071	Reserved for future use.
2072	Reserved for future use.
2073	Reserved for future use.
2074	Reserved for future use.
2075	Reserved for future use.
2076	Last route received (drops 1,2).
2077	Last route received (drops 3,4).
2078	Last route received (drops 5,6).
2079	Last route received (drops 7,8).
2080	Buffers in use. Number indicates the buffers in use by this port.

Table 26-3 TCP/IP Ethernet Port Statistics Registers

Register	Incremented when the following occurs:
2049	TCP/IP RESET received..
2050	SNIC ran out of Ring Buffers.
2051	Reserved.
2052	TCP Buffer pulled from Free Queue.
2053	Free Queue is Empty (out of buffers).
2054	Packet transmitted successfully and acknowledged by peer.
2055	Connection abandoned.
2056	Retransmitted un-ACKed packet.
2057	Packet lost because of unrecognized or illegal drop or bad route.
2058	Illegal TCP/IP Query request on local registers.
2059	Incoming TCP/IP Read performed upon local registers.
2060	Incoming TCP/IP Write received and performed upon local registers.
2061	Total number of TCP connections open.
2062	Total number of Client TCP connections open.
2063	Non-Modbus TCP/IP Ethernet packet received.
2064	Ethernet packets transmitted.
2065	Ethernet packets received.
2066	Ethernet collisions.
2067	Ethernet transmit packets lost to excess collisions.
2068	Ethernet receive packets with CRC error.
2069	Ethernet receive packets with framing error.
2070	Ethernet NAK TRANS sent (Sequence error).
2071	Reserved for future use.
2072	Reserved for future use.
2073	Reserved for future use.
2074	Reserved for future use.
2075	Reserved for future use.
2076	Last route received (drops 1,2).
2077	Last route received (drops 3,4).
2078	Last route received (drops 5,6).
2079	Last route received (drops 7,8).
2080	Buffers in use. Number indicates the buffers in use by this port.

Data Port Statistics

Each of the four data ports has its own group of 32 statistics registers. These are displayed in Table 26-4.

Table 26-4 Ports 1 and 2 Statistics Registers

Port 1	Port 2	Incremented when the following occurs:
2081	2113	Receipt of a packet on the port. In SY/MAX mode, packet was valid.
2082	2114	Incoming packet rejected (SY/MAX) or lost (other) because no available buffer.
2083	2115	Invalid SY/MAX packet received and negative acknowledge sent.
2084	2116	Message generated internally. (translation, Auto-transfer)
2085	2117	Internal message generation failed because no available buffer.
2086	2118	Packet transmitted (SY/MAX packet acknowledged by recipient.)
2087	2119	Transmission failed (SY/MAX retries exhausted).
2088	2120	Transmission retry.
2089	2121	Message lost because of unrecognized or illegal drop or bad route.
2090	2122	Illegal operation request for local command or translation.
2091	2123	Priority read received and performed upon this port.
2092	2124	Priority write received and performed upon this port.
2093	2125	Non-Priority read received and performed upon this port.
2094	2126	Non-Priority write received and performed upon this port.
2095	2127	Character receive error (parity, framing, etc.)
2096	2128	Characters transmitted
2097	2129	Characters received.
2098	2130	Reserved for future use.
2099	2131	Reserved for future use.
2100	2132	Reserved for future use.
2101	2133	Reserved for future use.
2102	2134	Reserved for future use.
2103	2135	Number of queued messages.
2104	2136	Number of bytes transmitted between SY/MAX checksum and ack returned.
2105	2137	Reserved for future use.
2106	2138	Reserved for future use.
2107	2139	Reserved for future use.
2108	2140	Last route received (drops 1,2).
2109	2141	Last route received (drops 3,4).
2110	2142	Last route received (drops 5,6).
2111	2143	Last route received (drops 7,8).
2112	2144	Buffers in use. Number indicates the buffers in use by this port.

Backplane Port Statistics

The backplane port has its own group of 32 statistics registers to give the user an idea of the activity on the backplane of the Compact rack in relation to the CNOE-800. These registers may be cleared by writing a zero. The group of registers is shown in Table 26-5.

Table 26-5 Backplane Port Statistics Registers

Register	Incremented when the following occurs:
2145	Replies received from backplane.
2146	Error responses generated.
2147	Replies to MSTR discarded.
2148	Messages generated by backplane.
2149	Port unable to get buffer.
2150	Memory access messages sent to PLC.
2151	No context available for new MSTR.
2152	Indicates current count of active MSTR blocks.
2153	Message discarded.
2154	Bad message format.
2155	Backplane Modbus Channel message with logon.
2156	Backplane Modbus Channel message without logon.
2157	PLC memory access message serviced.
2158	MSTR operation initiated.
2159	Port expired the programming connection.
2160	Unsupported MSTR opcode.
2161	MSTR operation finished.
2162	Backplane Modbus channel message serviced.
2163	Error response generated-no rack communications.
2164	Rack scanned by CNOE-800.
2165	End-of-scan hooks.
2166	User logic hooks.
2167	Buffers in internal queue.
2168	Indicates programming logon claimed.
2169	Power-up hooks received.
2170	Exit Dim Awareness hooks received.
2171	I/O scan idle executions.
2172	Last route received (drops 1,2)
2173	Last route received (drops 3,4).
2174	Last route received (drops 5,6).
2175	Last route received (drops 7,8).
2176	Buffers in use. Number indicates the buffers in use by this port.

IP Routing Table

The CNOE-800 includes an internal IP router which is configured by a table with sixteen 12 byte entries including the IP addresses, subnet masks, and gateways. This table is held in registers 2900 through 2995.

The first two registers of each entry contain the IP address. For local IP address, an explicit address is set here and the Flag entry is set to 1 for KEEP. For subnet gateways, the masked IP address of the subnet should appear here.

The next two registers provide the Subnet Mask (or Default Gateway IP address.)

A subnet route has a Subnet Address in the first two registers and the full IP address for a gateway in the next two registers. Failing an exact match, the destination of the packet is ANDed with the local subnet mask and the resulting subnet address is searched for in the table.

A network route is treated the same as a subnet route, except that the subnet mask can be determined by whether the destination is a Class A, B, or C address.

A default route is a network route with a network address of all 0's. This will also serve to mark the end of the table.

The Port Number entry only allows the value 0 for the Ethernet port at this time. When serial IP protocol modes are added to the CNOE-800, other port numbers will be allowed.

The Flag entry tells the router what to do with the incoming/outgoing IP packets. If set to 0, the router discards the packet. If set to 1, the router keeps the message and hands it up the protocol stack. If set to 2, the router forwards the IP packet to the port determined by the Port Number entry.

Table 26-6 below shows an example of the IP router table with the IP Address of the Ethernet port set to 199.186.195.20 and a Subnet Mask of 255.255.255.0 and a Default Gateway of 199.186.195.1.

Table 26-6 IP Router Table

Register	Description	Example (hex)	Notes	Entry
2900	IP Address MSW	C7BA	199.186	IP Table Entry 1 This entry sets the IP address of the Ethernet port to 199.186.195.20 and the Subnet Mask to 255.255.255.0
2901	IP Address LSW	C314	195.20	
2902	Subnet Mask MSW	FFFF	255.255	
2903	Subnet Mask LSW	FF00	255.0	
2904	Port Number	0	Ethernet Port	
2905	Flag	1	Keep	
2906	IP Address MSW	0000	0.0	IP Table Entry 2 This entry sets the Default Gateway to 199.186.195.1 so other packets not matching the subnet mask are sent to the gateway.
2907	IP Address LSW	0000	0.0	
2908	Subnet Mask MSW	C7BA	199.186	
2909	Subnet Mask LSW	C301	195.1	
2910	Port Number	0	Ethernet Port	
2911	Flag	2	Forward	
...
2990	IP Address MSW	0		IP Table Entry 16
...	
2995	Flag	0		

TCP/IP Port Number

Modbus/TCP servers listen on port 502 and this value is fixed and not adjustable.

TCP/IP Step Size for Incremental Backoff

Register 2997 contains the decimal value in 100ths of a second, the step size for the TCP incremental backoff timer. If a TCP packet is transmitted on an open connection, it will expect an acknowledgment from the other device within this time value. If an ACK is not received, the message will be retransmitted and the incremental timer value is doubled. This will continue until an ACK is received or the downstream timer expires. The default value is 100 decimal (1 second) which will result in the following retransmit times: 1 sec, 2 sec, 4 sec, 8 sec, 16 sec...

TCP/IP Downstream Timeout

Register 2998 contains the setpoint for the amount of time a client waits for a response from a server (or further downstream device). This value is expressed in 100ths of a second and the default is 1100 (11 seconds). When this timer expires, a Modbus error x0B is returned.

TCP/IP Quiet Timeout

Register 2999 contains the setpoint for the amount of time a socket will remain open with no traffic. The units are seconds with the default equal 600 (10 minutes).

Ethernet Addresses of Known Drops Registers

The IEEE 802.3 protocol requires each physical device on the Ethernet to have a unique address. (This address is the address of the Ethernet controller and is not to be confused with the SY/MAX drop number 00..99.) This address is a 6 byte number and its value is governed by the IEEE. Each company that makes Ethernet devices is assigned a block of addresses by the IEEE. All NR&D Ethernet products will have addresses with the form 00-20-BD-XX-XX-XX.

The CNOE-800 provides a listing of the physical Ethernet 802.3 address of each known active SY/MAX device on the network (See Table 26-7). These values are placed in Registers 3000..3302 with three registers allocated for each address. The Ethernet address requires six bytes of data and this data is split into two bytes per register. The following formulas will provide the registers containing the Ethernet address of each of the 100 possible devices on the SY/MAX network:

$3000 + \text{Drop} * 3 = \text{First two bytes of Ethernet Address}$

$3001 + \text{Drop} * 3 = \text{Middle two bytes of Ethernet Address}$

$3002 + \text{Drop} * 3 = \text{Last two bytes of Ethernet Address}$

Registers 3300..3302 give the Ethernet address of the CNOE-800.

Table 26-7 Ethernet Physical Address Registers

Register	E-Net Address Bytes	SY/MAX Drop Numbers
3000	First	Drop 00
3001	Middle	
3002	Last	
3003	First	Drop 01
3004	Middle	
3005	Last	
3006	First	Drop 02
3007	Middle	
3008	Last	
3009	First	Drop 03
3010	Middle	
3011	Last	
...
3297	First	Drop 99
3298	Middle	
3299	Last	
3300	First	Address of this RPC
3301	Middle	
3302	Last	

If the CNOE-800 recognizes another device on the Ethernet with the same SY/MAX Ethernet drop, it will go into Duplicate Drop mode and place the offending devices MAC in the table entry corresponding to the drop number of the CNOE-800's port. This state is easily recognized by the Ethernet Error light flashing at a constant rate of 2 flashes per second.

IP Addresses of Connected Devices

The CNOE-800 provides a listing of the IP address of each connected device on the network (See Table 26-8). These values are placed in Registers 2701..2828 with two registers allocated for each address. The IP address requires four bytes of data and this data is split into two bytes per register. The following formulas will provide the registers containing the IP address of each of the 64 possible sockets in the CNOE-800

$$2701 + \text{Socket Number} * 2 = \text{MSW of IP Address on connected socket}$$

$$2702 + \text{Socket Number} * 2 = \text{LSW of IP Address on connected socket}$$

Table 26-8 IP Address of connected Sockets Registers

Register	IP Address Bytes	Connected Socket
2701	First	Socket 0
2702	Last	
2703	First	Socket 1
2704	Last	
2705	First	Socket 2
2706	Last	
2707	First	Socket 3
2708	Last	
...
2827	First	Socket 63
2828	Last	

E-Peer Active Register

The bits of read-only register 3303 correspond to those of the first sixteen nodes on an CNOE-800 peer network which are active. If unit x is active on the network, bit x is set. If node x is powered off, disconnected from the cable, or otherwise disabled, bit x will be cleared. Loss of the node has no effect on the timing of the other nodes. They will detect the absence of the node and clear the corresponding bit in their register 3303. If the peer network has more than sixteen nodes, node numbers 17 and beyond have no associated active bits.

E-Net Search

Register 3304 provides a mechanism for causing the CNOE-800 to send out connect messages to SY/MAX 802.3 units on the Ethernet in order to build a complete table of all devices on the network. When the value 100 is written to register 3304, connect messages from unit 0 through 100 will be sent onto the network. RPCSW32 uses this technique to develop a complete listing of all of the possible nodes on the network.

Auto-Scan Table Registers

Each serial port has registers reserved for up to 48 entries in the Auto-Scan table. Registers 3410 through 3999 along with the Modbus Slave Address Tables are used to define the Auto-Scan table.

Table 26-9 Auto-Scan Configuration Registers

Port 1 Register	Port 2 Register	Data Bytes		Description
		MSB	LSB	
3410	3555			Status Pointer
3411	5281	Flag	Count	Drop 1 Flags/Count
3412	5282			Drop 1 Local Pointer
3413	5283			Drop 1 Remote Pointer
3414	5284	Flag	Count	Drop 2 Flags/Count
3415	5285			Drop 2 Local Pointer
3416	5286			Drop 2 Remote Pointer
...
3554	5915			Drop 48 Remote Pointer

Modbus Slave Address Tables

There is a table of translations for the Ethernet port in Modbus/TCP mode. There are two tables, each 640 registers long that comprise 128 entries with 5 registers each. The LSB of the first register in each entry is the number of drops in the entry or zero to indicate the entry is unassigned. Each of the remaining four registers of the entry contains two drops, one in each byte in MSB and LSB order. Up to eight drops may be included in the route. The table entries correspond to Modbus addresses in the range of N through N+255 where N is the Modbus address base value for that port and is programmed in another register. The default is 0 and the Ethernet port uses the tables for Port 0 and Port 4 giving it the full 256 possible Destination Indexes.

When a message is received from a Modbus master, the module checks the table entry associated with the address byte in the message. If the entry is unused (the drop count register is zero), the CNOE-800 replies with its own registers. If a valid route is found, the Modbus message is translated (or encapsulated) to SY/MAX and processed locally or forwarded according to the route from the table.

The port retains the original Modbus address from the received slave command and uses it to format the reply to the attached Modbus master. Modbus is a single threaded protocol and only one request at a time may be outstanding from the port through the router.

Translation of commands received on the slave port depends on the settings of the same configuration registers that select the opcodes associated with Modbus Master operations. If the entry in the routing table is set to "OTHER," and the incoming packet has an opcode of 1, 2, 3, or 4 then the Modbus message is translated into a SY/MAX priority READ. If the incoming packet has an opcode of 5, 6, 15, or 16 then the message is translated into a SY/MAX priority WRITE. The register offset is not applied to the incoming packet. If the entry in the table is set to "MODBUS," then all opcodes are held intact, and redirected to the next port.

If the incoming message is not in the above list, it is encoded as a SY/MAX network PRINT and sent to the target device. The target port decodes the network print as a Modbus master and the Modbus reply is returned as a SY/MAX Network Print reply to be emitted at the slave port as the Modbus reply.

The table registers occupy addresses in the 4640 through 5919 range in the CNOE-800.

Table 26-10 Modbus Slave Address Table

E-net Entry 0-127	Port 1 Register	Port 2 Register	E-net Entry 128-255	Data Bytes		Modbus Drop Numbers
				MSB	LSB	
4000	4640	5280	6560	Not Used	Number of Drops	Address Base + 0
4001	4641	5281	6561	Drop 1	Drop 2	
4002	4642	5282	6562	Drop 3	Drop 4	
4003	4643	5283	6563	Drop 5	Drop 6	
4004	4644	5284	6564	Drop 7	Drop 8	Address Base + 1
4005	4645	5285	6565	Not Used	Number of Drops	
4006	4646	5286	6566	Drop 1	Drop 2	
4007	4647	5287	6567	Drop 3	Drop 4	
4008	4648	5288	6568	Drop 5	Drop 6	
4009	4649	5289	6569	Drop 7	Drop 8	...
...
4635	5275	5915	7195	Not Used	Number of Drops	Address Base + 127
4636	5276	5916	7196	Drop 1	Drop 2	
4637	5277	5917	7197	Drop 3	Drop 4	
4638	5278	5918	7198	Drop 5	Drop 6	
4639	5279	5919	7199	Drop 7	Drop 8	

The Modbus address base register is in the normal setup register area. (Table 26-11) The E-net port should always have its starting value set to zero.

Table 26-11 Modbus Slave Starting Address Register

RPC Port	Modbus Slave Starting Add. Reg.
E-net	8031
1	8063
2	8095

TCP/IP Routing Table

Outbound Ethernet TCP/IP messages are routed to the appropriate IP addresses by means of a 200 entry table that maps SY/MAX drop numbers 0 through 199 to IP addresses. Additionally, a downstream route drop may be added to the IP address to extend the functionality of the IP routing. This table starts at register 7900 and includes 8 bytes (4 registers) per entry. The first four bytes (2 registers) hold the

destination IP address. The last four bytes (2 registers) hold the downstream route. The route is held in 1 drop per byte and is terminated by a hex FF value. The CNOE-800 will use the drop immediately preceding the xFF for the Device Index.

Table 26-12 Outbound TCP/IP Routing Table

Register	Description	Example (hex)	Notes	Entry
7900	IP Address MSW	C7BA	199.186	Entry 0 Routes to IP address 199.186.195.21 with no additional route.
7901	IP Address LSW	C315	195.21	
7902	Downstream Rt	FF00	NONE	
7903	Downstream Rt	0000		
7904	IP Address MSW	C7BA	199.186	Entry 1 Routes to IP address 199.186.195.22 with the additional drop of 10
7905	IP Address LSW	C316	195.22	
7906	Downstream Rt	0AFF	10	
7907	Downstream Rt	0000		
7908	IP Address MSW	C7BA	199.186	Entry 2 Routes to IP address 199.186.195.23 with a device index of 1
7909	IP Address LSW	C317	195.23	
7910	Downstream Rt	9A11	154,17	
7911	Downstream Rt	01FF	1	
7912	IP Address MSW	C7BA	199.186	Entry 3 Routes to IP address 199.186.195.23 with device index of 2
7913	IP Address LSW	C317	195.23	
7914	Downstream Rt	9A11	154,17	
7915	Downstream Rt	02FF	2	
...	Entries 4 ... 198
7996	IP Address MSW	B670	182.112	Entry 199 Routes to IP address 182.112.204.7 with no additional route
7997	IP Address LSW	CC07	204.7	
7998	Downstream Rt	FFFF	NONE	
7999	Downstream Rt	FFFF		

Setup and Configuration Registers

Registers 8001..8130 are provided for the setup and configuration for the ports of the CNOE-800. Each Port of the CNOE-800 uses 32 registers to control its operational parameters. The first two registers concern the entire module and are shown in Table 26-13.

Table 26-13 Module Setup Identification Registers

Register	Legal Values	Function
8001	5001(hex)	Setup identification constant.
8002		Reserved for future use. Do not modify.

Ethernet Port Control Registers

Registers 8003 through 8034 control the parameters of the Ethernet port on the QUCM. Table 26-14 provides a list of these registers.

Table 26-14 Ethernet Port Control Registers

Port 0	Legal Values	Function
8003	0..99	Ethernet SY/MAX drop number.
8004...8007		Reserved for future use. Do not modify.
8008	2, 260, 272	Protocol Mode 2 = SY/MAX 802.3, 260 = Modbus/TCP, 272 = MBTCP+SY/MAX
8009	1..8192	Auto-transfer Read Source Register (Peripheral)
8010		Reserved for future use. Do not modify.
8011	0..32767	Auto-transfer Interval in 10mS units
		E-Peer Update Interval in 1mS units
8012	1..2048	Auto-transfer Read Destination Register (Mailbox)
	0..100	Number of this E-Peer Node
8013	1..2048	Auto-transfer Write Source Register (Mailbox)
		Start of register range to transmit from this E-Peer Node.
8014	0..8	Number of drops in target route (Auto-transfer)
8015	0..255	Target Route Drop 1 (Auto-transfer)
8016	0..255	Target Route Drop 2 (Auto-transfer)
8017	0..255	Target Route Drop 3 (Auto-transfer)
8018	0..255	Target Route Drop 4 (Auto-transfer)
8019	0..255	Target Route Drop 5 (Auto-transfer)
8020	0..255	Target Route Drop 6 (Auto-transfer)
8021	0..255	Target Route Drop 7 (Auto-transfer)
8022	0..255	Target Route Drop 8 (Auto-transfer)
8023		Reserved
8024		Reserved
8025	1..32	Buffer Limit
8026	0..128	Auto-transfer Read Count
	2..100	Number of E-Peer Nodes
8027	0..128	Auto-transfer Write Count
		Number of E-Peer register to transmit
8028	1..8192	Auto-transfer Write Destination register (Peripheral)
		Destination Register in other E-Peers
8029		Reserved for future use, do not modify
8030		Options (See Table 26-23 on Page 196)
8031		Reserved for future use, do not modify
8032		Reserved for future use, do not modify
8033		Reserved for future use, do not modify
8034		Reserved for future use, do not modify

Data Port Control Registers

Each of the Data Ports may have independent settings for Drop Number, Baud Rate, Parity, Data bits, Stop bits, Mode, Auto-transfer, etc. These are controlled by register values listed in Table 26-22.

Table 26-15 Ports 1 and 2 Configuration Registers

Port 1	Port 2	Legal Values	Function
8035	8067	0..199	Drop Number
8036	8068	0..14	Baud Rate (See Table 26-17 on Page 193)
8037	8069	0,1	Data Bits (See Table 26-18 on Page 194)
8038	8070	0,1,2	Parity Bits (See Table 26-19 on Page 194)
8039	8071	0,1	Stop Bits (See Table 26-20 on Page 194)
8040	8072	1..19	Protocol Mode (See Table 26-21 on Page 194)
8041	8073	0..256	Packet size limit (Modes 4, 5, and 8)
		1..8192	Auto-transfer Read Source Register (Peripheral)
		0..65535	RNIM Identification Number
8042	8074	0..32767	Time limit (Modes 4, 5, and 8)
		0..32767	MODBUS Host mode retry timeout
		0..65535	RNIM CTS Delay
8043	8075	0..32767	Multidrop window interval
		0..32767	Auto-transfer Interval
		0..65535	RNIM Message Response Timeout
8044	8076	0..200	Priority in Multidrop mode
		1..2048	Auto-transfer Read Destination Register (Mailbox)
		0..65535	RNIM BID Address
8045	8077	0..200	Number of nodes in Multidrop mode
		1..2048	Auto-transfer Write Source Register (Mailbox)
		0..65535	RNIM Number of Retries
8046	8078	0..8	Number of drops in target route (Modes 4,5,8 and Auto-transfer)
8047	8079	0..255	Target Route Drop 1 (Modes 4,5,8 and Auto-transfer)
8048	8080	0..255	Target Route Drop 2 (Modes 4,5,8, and Auto-transfer)
8049	8081	0..255	Target Route Drop 3 (Modes 4,5,8, and Auto-transfer)
8050	8082	0..255	Target Route Drop 4 (Modes 4,5,8, and Auto-transfer)
8051	8083	0..255	Target Route Drop 5 (Modes 4,5,8, and Auto-transfer)
8052	8084	0..255	Target Route Drop 6 (Modes 4,5,8, and Auto-transfer)
8053	8085	0..255	Target Route Drop 7 (Modes 4,5,8, and Auto-transfer)
8054	8086	0..255	Target Route Drop 8 (Modes 4,5,8, and Auto-transfer)
8055	8087	1,2,3,4	MODBUS Host equivalent READ command
8056	8088	5,6,15,16	MODBUS Host equivalent WRITE command
8057	8089	1..16	Buffer Limit

Table 26-16 Ports 1 and 2 Configuration Registers (Continued)

Port 1	Port 2	Legal Values	Function
8058	8090	0..128	Auto-transfer Read Count
		0..65535	RNIM Pause Time
8059	8091	0..128	Auto-transfer Write Count
		0..65535	RNIM Message Count
8060	8092	1..8192	Auto-transfer Write Destination register (Peripheral)
		0..65535	RNIM BID Reply Interval
8061	8093	0..65535	MODBUS Host Offset (Register Bias)
8062	8094		Options (See Table 26-23 on Page 196)
8063	8095	0..127	Modbus Slave Starting Address
8064	8096	0..65525	PAD Count in SY/MAX, N-T-N or CTS Delay in 10mS units for Modbus
8065	8097	0..65535	Modbus RTU inter-character timing in mS. (default is 4 characters)
8066	8098		Reserved for future use, do not modify

The above tables make reference to baud rate values, stop bit values, parity values, and mode values. The following tables define these values.

Table 26-17 Baud Rate Values

Baud Register	Baud Rate	Notes
0	50	(A)
1	75	(B)
2	110	
3	134.5	
4	150	(B)
5	300	
6	600	
7	1200	
8	1800	(B)
9	2400	
10		Illegal, but sets 9600
11	4800	
12	7200	(A)
13	9600	
14		Illegal, but sets 9600
15	19200	(B)

Notice: The two RS-422 ports on the QUCM have mutually incompatible baud rates. If one port is set to any of the baud rates marked (A), the other port cannot be set to any of the rates marked (B). Before panicking, note that with either port set to 9600 (or other unmarked rate), the other port can be set to any supported rate. The most common combinations 9600 and 9600, 9600 and 19200, or 19200 and 19200 are among those allowed.

Table 26-18 Data Bits Values

Data Register	Data Bits
0	7
1	8

Table 26-19 Parity Values

Parity Register	Parity
0	None
1	Odd
2	Even

Table 26-20 Stop Bits Values

Stop Register	Stop Bits
0	1
1	2

Table 26-21 Port Mode Values

Mode Register	Protocol
1	SY/MAX
2	Net-to-Net
3	Peripheral
4	Transparent
5	Share
6	PLogic
7	Idec
8	Gateway
9	Multidrop
10	Modbus Host
11	PNIM
12	RNIM Master
13	RNIM Slave
14	Modbus Gate
15	Transfer
16	Chevron
17	Reserved
18	Modbus ASCII
19	Dual Slave

Backplane Port Control Registers

The backplane port may have independent settings for Drop Number, Mode, etc. These are controlled by register values listed in Table 26-22.

Table 26-22 Backplane Port Configuration Registers

Register	Legal Values	Function
8099	0..199	Drop Number
8100...8104		Reserved for future use. Do not modify.
8105	1...32	Span of I/O scan entries per socket.
8106	0...65535	MSTR reply timeout in 1/100ths of a second.
8107...8120		Reserved for future use. Do not modify.
8121	0...65535	Programming channel idle timeout in minutes.
8122...8125		Reserved for future use. Do not modify.
8126		Options (See Table 26-23 on Page 196)
8127...8130		Reserved for future use. Do not modify.

Table 26-23 Options Register Values

Option Bit	Function when Bit CLEAR (Default)	Function when Bit SET
1	Backplane: CNOE-800 is option module Serial: SY/MAX Block Check is single byte checksum (BCC)	Backplane: CNOE-800 is I/O module Serial: SY/MAX Block Check is two byte cyclic redundancy check (CRC)
2	Backplane: Ethernet I/O scanner disabled Ethernet: Telnet enabled. Serial: Gateway, Share, and Transparent do echo.	Backplane: Ethernet I/O scanner enabled Ethernet: Telnet disabled. Serial: Gateway, Share, and Transparent do echo.
3	BOOTP Enabled on Ethernet port in TCP/IP Modes. Gateway mode replies are terminated by CR only.	Disable BOOTP on Ethernet Port in TCP/IP Modes. Gateway mode replies are terminated by CR/LF and are highlighted.
4	DHCP Enabled on Ethernet port in TCP/IP Modes. Gateway, Share, and Transparent messages are terminated by any control character as well as the time and count settings.	Disable DHCP on Ethernet Port in TCP/IP Modes. Gateway, Share, and Transparent messages are terminated only by time and count termination settings. All characters are treated the same.
5	Normal routing. (Route Replacement OFF)	Route Appendix replaces any existing incoming packet (Route Replacement ON).
6	Auto-Transfer Enabled for E-Net Port. Normal Routing for Ports 1..3	E-Peer Enabled for E-Net Port. On Ethernet Enabled for Ports 1..3
7	Multidrop False	Multidrop True
8	Full Duplex (For 4-Wire)	Half Duplex (For 2-Wire)
9	RNIM Master or Slave normal. Normal Modbus Host R[8188] reply.	RNIM Master Disabled. RNIM Slave buffer clear. SMS Register 8188 spoofing on Modbus Host.
10	Reserved.	If bit 10 and bit 9 are set, the value in R[options+1] is used as the remote register polled in SMS read of 8188.
11	Reserved.	Reserved.
12	Reserved.	Reserved.
13	Reserved.	Reserved.
14	Reserved.	Reserved.
15	Reserved.	Reserved.
16	Reserved.	Reserved.

Options

The Options Register allows the modification of the normal operation of several features of the CNOE-800.

- Bit 1 controls the backplane mode of the CNOE-800.

Bit 1 controls the error checksum used by SY/MAX, Net-to-Net, and Multidrop mode ports. If this bit is clear then the default single byte BCC is used. If set, the two byte CRC checksum is used. Normal SY/MAX messages use the BCC while the CRC is normally used on modem connections when the parity is disabled.

- Bit 2 determines whether the Ethernet I/O scanner is enabled. On the Ethernet, it determines whether Telnet is enabled.

Bit 2 determines whether the Gateway, Transparent, and Share ports echo all characters received.

This may be useful when using a terminal on a Gateway port to see what is being typed. This feature is also useful when transparently programming Model 50 PLCs with an Idec Port.

Bit 2 also controls the enhanced Route Appendix operation for use with Eaton PanelMate Operator Interfaces and other devices capable of only two drop routes. When Bit 2 is set on a SY/MAX mode port, if a command message is received with a route of 205,X the QUCM will use the X entry in the Modbus Slave Routing table for the new route. The message will be routed according to this new route. When the reply from the new route is received at this SY/MAX port, the reversed route X,205 will be sent back to the PanelMate.

- Bit 3 determines whether BOOTP is enabled.

Bit 3 determines whether the Gateway Mode terminates its messages (output) with a carriage return or with a carriage return and line feed and the reply is highlighted on ANSI terminals.

- Bit 4 determines whether DHCP is enabled.

Bit 4 determines whether Gateway, Transparent, and Share modes are terminated by control characters such as a carriage return or line feed.

- Bit 5 enables the Route Replacement feature on a SY/MAX mode port. When set, the incoming route is saved and is instead replaced by the route stored in the Target Route Registers. The reply message has the original route reversed and replaced to send back to the originator.
- Bit 6 Enables the E-Peer function on the Ethernet port. If this bit is cleared, then the normal Auto-transfer functions are enabled on the Ethernet port.

Bit 6 also controls the "On Ethernet" status of the two serial ports.

- Bit 7 sets the Multidrop status of the serial port RS-485 driver. When clear, the TX driver is always enabled (i.e. RS-422). When set, the TX driver is controlled by the CTS signal. When CTS is enabled (ON), the transmit driver is enabled and when CTS is not enabled (OFF), the transmit driver is tri-stated and allowed to "float" thus allowing other devices on the multidrop network to transmit.
- Bit 8 sets the full/half-duplex mode of the serial port RS-485 receiver. When clear, the receiver is always enabled which allows full duplex operation. When this bit is set, the receiver is disabled whenever the port is transmitting. This feature is used on two-wire systems and on devices which echo to prevent the QUCM port from hearing its own message.
- Bit 9 controls the disabling of the RNIM Master port. Only one RNIM Master may be active on a given RNIM network at a time. Redundant RNIM Masters may be placed on the system but disabled by setting this bit for the Master's port.

Bit 9 also may be used in the RNIM Slave mode ports to clear the buffer of queued messages waiting for BIDDing.

Bit 9 also is used on Modbus Host ports to provide spoofing of PowerLogic System software. All PowerLogic softwares send a SY/MAX read to register 8188 to determine if the device is online. Not all Modbus devices may be configured to have an address within this range. When this bit is set, the Modbus Host port intercepts a single register SY/MAX read of register 8188 and translates that message to a Modbus Report Slave ID (opcode 17 decimal) message. The Slave ID and the Run/Halt status of the Modbus device are returned as the data to the register 8188 read. The Slave ID byte is returned as the LSB of register 8188. Bit 14 of 8188 will always be set to indicate that this translation has occurred. And Bit 15 of 8188 will be set if the Modbus device is in RUN and clear if the device is in Halt.

- Bit 10 may be used in conjunction with bit 9 to have SMS poll non-PLC devices that don't support opcode 17. When bits 10 and 9 are both set, the value in R[options+1] is used as the remote register to poll in the Modbus Slave when a read of register 8188 is received on the port. For example, if Port 2 of the QUCM is in Modbus Host mode, bits 9 and 10 of register 8094 in the QUCM are set,

and register 8095 has the decimal value of 10, then Holding register 10 in the Modbus slave will be read when SMS performs its health check of register 8188.

Clear Function Register

Register 8174 is the module clear register. When a specific bit pattern is written to it, the module clears the register after performing the requested operation.

Table 26-24 Clear Function bit-map

Bit Number	Description
1	Set all rack addressed registers to PLC outputs.
2	Clear all rack addressed inputs to zero.
3	Clear all rack addressed outputs to zero.
4	Clear all non-rack addressed mailbox registers.
5	Load factory default setup. (does not affect mailbox)
6	Reserved, must be zero if not supported.
7	Must be zero.
8	Must be one.

NOTE: Bits 9 through 16 must be the same as bits 1 through 8 respectively.

For example, the CNOE-800 may be reset to factory default settings, clear all mailbox registers, and set all rack addressable mailbox registers to PLC outputs by writing the value 9F9F hex (-24673 decimal) to register 8174. When the CNOE-800 has finished resetting, it will return register 8174 to its original value.

Module Identification Registers

All NR&D modules contain a group of registers, 8176..8188, which may be used to determine the module type, the port being used to access the module, and certain operational parameters of the module. Table 26-25 provides an overview of these registers.

Table 26-25 Module Identification Registers

Register	Legal Values	Definition
8176	Bit 16, Bits 1..5	Port number (not drop number) that is being used to communicate with the module. Bit 16 is always set. Bits 1..5 indicate port number.
8177		Packed ASCII module identification. Space Padded.
8178		Packed ASCII module identification. Space Padded.
8179		Packed ASCII module identification. Space Padded.
8180		Packed ASCII module identification. Space Padded.
8181		Packed ASCII module identification. Space Padded.
8182		Packed ASCII module identification. Space Padded.
8183		Packed ASCII module identification. Space Padded.
8184		Packed ASCII module identification. Space Padded.
8185		Packed ASCII module identification. Space Padded.
8186		Packed ASCII module identification. Space Padded.
8188	9990 (hex)	Constant 9990(hex). Indicates NR&D module with name starting at Reg. 8177.

For example, if the CNOE-800 has a revision of 14JAN03, Registers 8177..8186 would have the values in Table 26-26.

Table 26-26 Module ID Example

Register	Values (hex)	Packed ASCII Values
8177	4352	CR
8178	5043	PC
8179	5443	TC
8180	5020	P
8181	3134	14
8182	4A41	JA
8183	4E32	N2
8184	3030	00
8185	3320	3
8186	2020	

Global Options Register (Register 8190)

All CNOE-800's come equipped with a global options register.

Table 26-27 Global Options Register Values

Option Bit	Function when Bit CLEAR (Default)	Function when Bit SET
1	Reserved	Reserved.
2	No Auto-Scan watchdog control for Port 1.	Gives control of Auto-Scans in Port 1 to timer in register 8189.
3	No Auto-Scan watchdog control for Port 2.	Gives control of Auto-Scans in Port 2 to timer in register 8189.
4	Reserved	Reserved
5	Reserved	Reserved
6	Reserved	Reserved
7	Reserved	Reserved
8	Reserved	Reserved
9	All rack addressable registers will be zeroed during power cycle.	All rack addressable registers will hold their values during power cycle.
10	All rack addressed 3x and 4x registers are in normal Modicon bit order.	All rack addressed 3x and 4x registers are bit-swapped(bit 1 becomes bit 16, 2 becomes 15, etc.).
11	Reserved.	Reserved.
12	Reserved.	Reserved.
13	Reserved.	Reserved.
14	Reserved.	Reserved.
15	Reserved.	Reserved.
16	Reserved.	Reserved.

Global Options

The Options Register allows the modification of the normal operation of several features of the CNOE-800.

- Bits 2 and 3 turn control of the Auto-Scans in Ports 1 and 2 over to the timer set in register 8189. For more information, see the Chapter on Auto-Scan.
- Bit 9 will cause all rack addressable registers to hold their values when power is cycled.
- Bit 10 will bit-swap all rack addressable 3x and 4x registers. Bit 1 becomes bit 16, bit 2 becomes 15, etc.

Connector Pinouts

RS-232 ports on CNOE-800 (RJ45 socket)

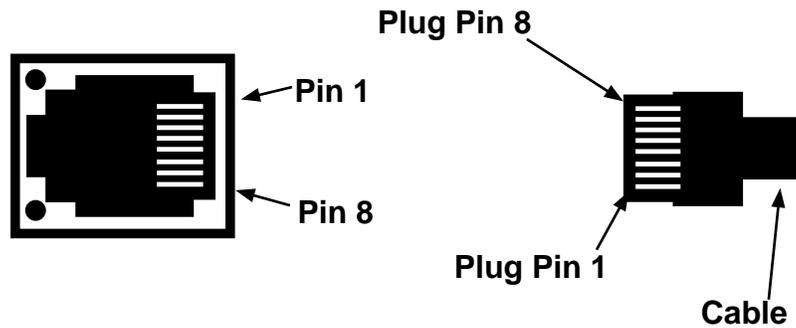


Figure 27-1 Ports 1 and 2 RJ45

Table 27-1 RS-232 Pinout

Pin	Function	Notes
1	+5VDC	From Compact Power Supply
2	DSR	Not used
3	TX	Transmit
4	RX	Receive
5	SG	Signal Ground
6	RTS	Push to Talk Request To Send
7	CTS	CTS must be high to transmit
8	Frame Ground	

RS-422/485 ports on CNOE-800 (RJ45 socket)

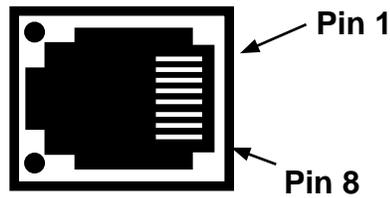


Figure 27-2 Ports 1 and 2 RJ45

Table 27-2 RS-485 Pinout

Pin	Function	Notes
1	Rx-	Input to CNOE-800
2	Rx+	Input to CNOE-800
3	Tx+	Output from CNOE-800
4	N/C	
5	SG	Signal Ground
6	Tx-	Output from CNOE-800
7	N/C	
8	Frame Ground	

The NR&D BB-85 may be used to bring the RS-485 signal lines out to a removable Screw Terminal block. The BB-85 is a small DIN-rail mounted block which connects to the CNOE-800 serial port with an included straight-through RJ-45 to RJ-45 cable (the NR&D MM0, or a Twisted Pair Ethernet patch cable may be used).

For 2-wire RS-485 applications, Rx+ and Tx+ must be tied together outside the CNOE-800, and Rx- and Tx- must also be tied together outside the CNOE-800.

10BaseT (Twisted Pair) Ethernet port on CNOE-800 (RJ45 socket)

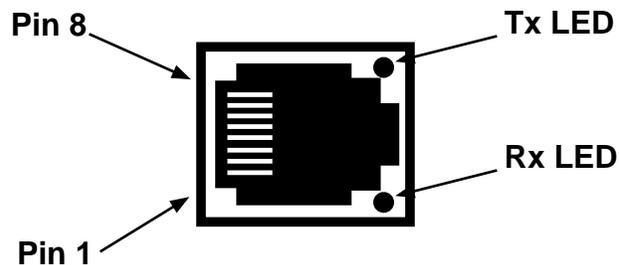


Figure 27-3 Ethernet Port RJ45

Table 27-3 10BaseT Pinout

Pin	Function
1	TX-
2	TX+
3	RX+
6	RX-

Recommended Cabling

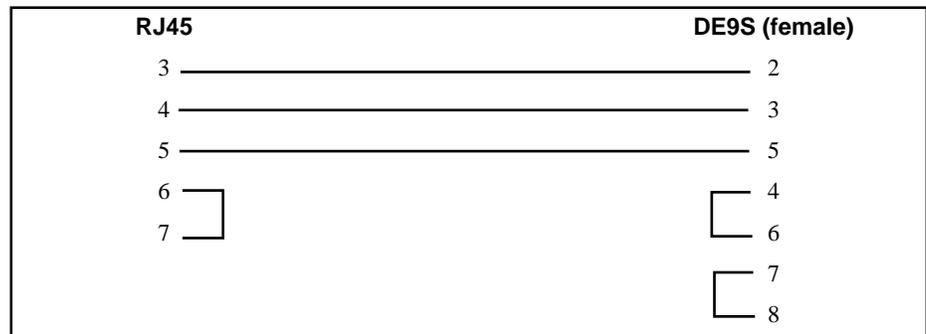
Cabling required to configure a CNOE-800

Configuration is accomplished from an MS-DOS personal computer connected to the CNOE-800. The factory default configuration for the first serial port is Dual Slave, 9600 baud, 8 data bits, EVEN parity, 1 stop bit which may be used for viewing and modifying CNOE-800 registers. The correct cabling needs to be installed to connect the personal computer to a CNOE-800 port.

CNOE-800 RS-232 to personal computer cabling

A connection to the RS-232 port of the PC may be made to either of the RS-232 ports of the module.

CNOE-800 RS-232 to RS-232 PC DCE Port (9-pin) (MM1 Cable)

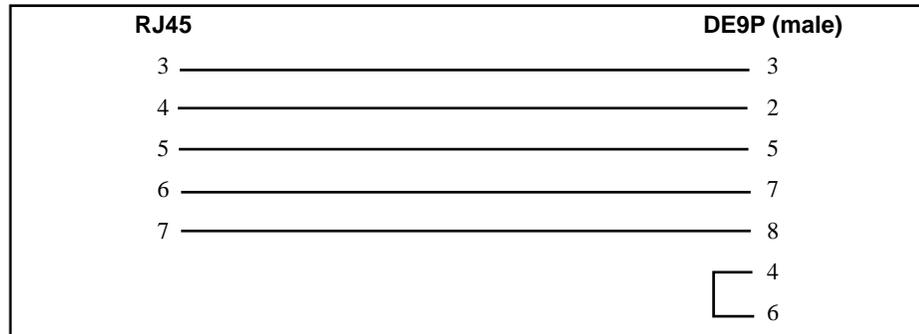


The Niobrara MM1 cable may be used for connecting the CNOE-800 to a personal computer.

CNOE-800 RS-232 to 9-pin DTE

The Niobrara MM3 cable may be used to connect the CNOE-800 RS-232 port to a 9-pin DCE device. This cable gives the CNOE-800 a standard PC type 9-pin male connector. The MM3 may be used in conjunction with the MM1 to connect two Modicon type RJ45 serial ports together. The MM3 may be used with a Niobrara SC902 cable to connect a Modicon type RJ45 RS-232 serial port to a SY/MAX type RS-422 port.

CNOE-800 RS-232 to RS-232 DTE Port (9-pin) (MM3 Cable)

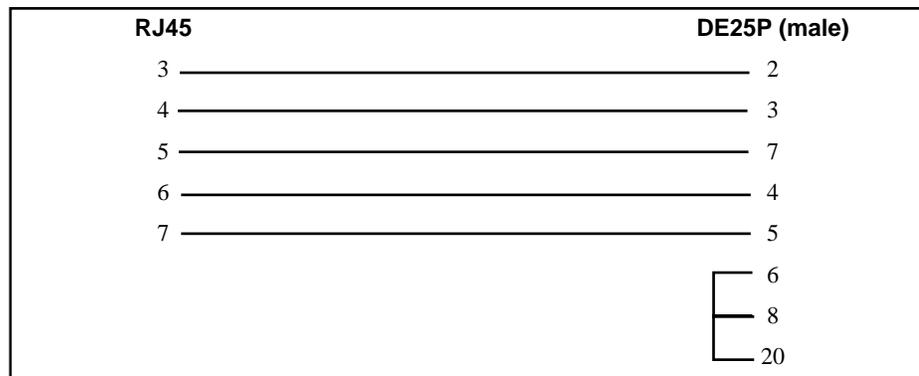


The Niobrara MM3 cable may be used for providing the CNOE-800 with a 9-pin port that acts like a personal computer's serial port.

CNOE-800 RS-232 to 25-pin DTE

The Niobrara MM4 cable may be used to connect the CNOE-800 RS-232 port to a 25-pin DCE device such as a modem or a Cutler-Hammer MINT II.

CNOE-800 RS-232 to RS-232 DTE Port (25-pin) (MM4 Cable)

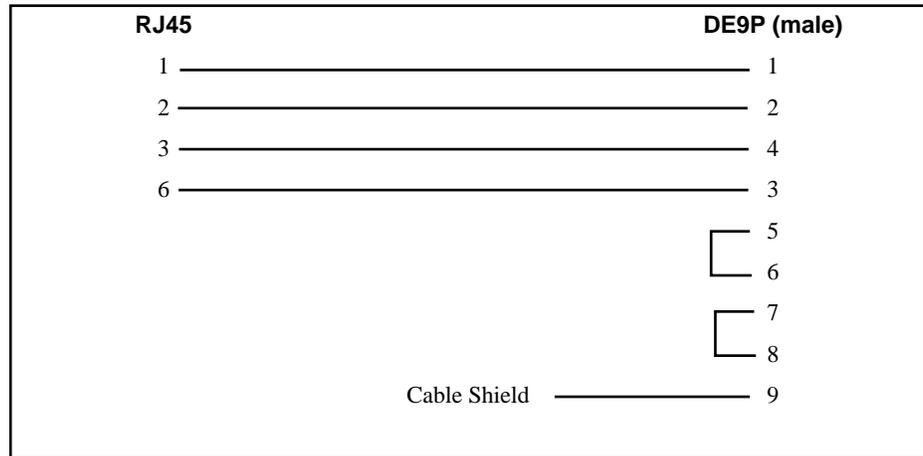


The Niobrara MM4 cable may be used to connect the CNOE-800 to a modem.

CNOE-800 RS-485/422 to SY/MAX 9-pin Port

When a non-isolated connection can be made between the CNOE-800 and a SY/MAX pinout port, the following cable may be used.

CNOE-800 RS-422/485 to SY/MAX pinout 9-pin port (MM7 Cable)



Isolated Cabling to SY/MAX Port

The Niobrara DDC2I Isolated RS-232<>RS-422/485 converter provides an optically isolated connection from the CNOE-800 to a SY/MAX pinout device. A Niobrara MM0 cable is used to connect the RS-232 port on the CNOE-800 to the RJ45 port on the DDC2I. A Niobrara DC1 cable is used to connect the 9-pin RS-422 port on the DDC2I to the SY/MAX device. The DIP switches on the DDC2I should be set for 4-Wire, Bias, and Termination. The CNOE-800 will provide the power for the DDC2I.

The Niobrara MM3 and SC902 cables may also be used together to provide a non-isolated connection between the CNOE-800 and a SY/MAX port.

Appendix A

Modbus/TCP Protocol Specifications

The Modbus/TCP protocol may be obtained at <http://www.modbus.org/> on the Internet.

Appendix B

NR&D Internet Access

Niobrara is on the World Wide Web! Our Internet home page is at:

<http://www.niobrara.com>

where you will find product information, file downloads, and links to our distributors.

You may E-mail technical support at the following:

techsupport@niobrara.com

A

Auto-Scan, 164, 187
Auto-Transfer, 20

B

Backplane Mode, 152
BID, 108
BID Address, 152
BID Response, 151
Broadcast, 111
Buffers, 162

C

Channel Delay, 162
Chevron, 121
Clear Function Register, 198
Command Line Parameters, 175
Control Character, 148
CTS Delay, 21
CTS Timer, 151

D

Default Gate, 147
Default Gateway, 32
Destination Register, 151
Downstream Timeout, 147
Driver Mode, 19, 146
Drop Number, 145

E

Echo, 149
Ethernet Addresses, 185
Ethernet I/O Entries per Socket, 65, 153
Ethernet I/O Scanner, 63, 153
E-Net Search, 187
E-PEER, 137, 148
E-Peer, 187

F

FOUR WIRE, 20

G

Gateway Mode, 99

H

HALF DUPLEX, 20
Highlight, 149

I

IDEC Mode, 95
Identification Registers, 198
IP Address, 146
IP Addresses of Connected Devices, 186
IP Framing, 147

M

MAC Address, 147
Mailbox, 20, 178
MBAP Port, 147
Message Count, 152
Micro-1, 95
Modbus Slave Table, 188
Modbus TCP Routing, 164
Modbus/TCP, 32
Model 50, 95
MSTR, 43
MSTR timeout, 153
Multidrop Mode, 103

N

Network ID, 151
Net-to-Net Mode, 79
Node Priority, 149
Number of Nodes, 149

O

OFFLINE Functions, 167
On Ethernet, 19, 145
Options Bits List, 196, 200

P

Packet Response, 151
Packet Size Limit, 148
Packet Time Limit, 148
PAD, 162
PanelMate, 20, 148
Pause Time, 152
Peripheral Mode, 83
PLOGIC Mode, 89
PNIM Mode, 91
Port Number, 32, 185
Programming Channel Timeout, 153
Protocol Mode, 19
PT to PT, 20

Q

Quiet Timeout, 147

R

READ Command, 149
READ Count, 150
READ From, 150
READ To, 150
Register Bias, 149
Register Count, 151
Retries, 151
Retry Timeout, 149
RNIM, 107
RNIM Master, 112
RNIM Slave, 113
Route Appendix, 20, 148
Route Replacement, 20, 148
RTS/CTS, 115

S

Setup and Configuration Registers, 190
Share Mode, 85
Start Register, 151
Statistics, 178
Subnet Mask, 32, 147
SY/MAX Mode, 77
SY/MAX Setup, 171

T

Target Route, 148
TCP Backoff, 147
Terminal Emulator, 170

This Node's Number, 150
Time Slice, 149
Total E-Peer Nodes, 150
Transfer Interval, 149
Transfer Route, 150, 152
Transparent Mode, 85
TWO WIRE, 20

U

Update Interval, 151

V

View Registers, 169

W

WRITE Command, 149
WRITE Count, 150
WRITE From, 150
WRITE To, 150

