



# NXC-ME260

## NetLinx Master-Ethernet Card/Module



# AMX Limited Warranty and Disclaimer

AMX Corporation warrants its products to be free of defects in material and workmanship under normal use for three (3) years from the date of purchase from AMX Corporation, with the following exceptions:

- Electroluminescent and LCD Control Panels are warranted for three (3) years, except for the display and touch overlay components that are warranted for a period of one (1) year.
- Disk drive mechanisms, pan/tilt heads, power supplies, MX Series products, and KC Series products are warranted for a period of one (1) year.
- Unless otherwise specified, OEM and custom products are warranted for a period of one (1) year.
- Software is warranted for a period of ninety (90) days.
- Batteries and incandescent lamps are not covered under the warranty.

This warranty extends only to products purchased directly from AMX Corporation or an Authorized AMX Dealer.

AMX Corporation is not liable for any damages caused by its products or for the failure of its products to perform. This includes any lost profits, lost savings, incidental damages, or consequential damages. AMX Corporation is not liable for any claim made by a third party or by an AMX Dealer for a third party.

This limitation of liability applies whether damages are sought, or a claim is made, under this warranty or as a tort claim (including negligence and strict product liability), a contract claim, or any other claim. This limitation of liability cannot be waived or amended by any person. This limitation of liability will be effective even if AMX Corporation or an authorized representative of AMX Corporation has been advised of the possibility of any such damages. This limitation of liability, however, will not apply to claims for personal injury.

Some states do not allow a limitation of how long an implied warranty last. Some states do not allow the limitation or exclusion of incidental or consequential damages for consumer products. In such states, the limitation or exclusion of the Limited Warranty may not apply. This Limited Warranty gives the owner specific legal rights. The owner may also have other rights that vary from state to state. The owner is advised to consult applicable state laws for full determination of rights.

**EXCEPT AS EXPRESSLY SET FORTH IN THIS WARRANTY, AMX CORPORATION MAKES NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. AMX CORPORATION EXPRESSLY DISCLAIMS ALL WARRANTIES NOT STATED IN THIS LIMITED WARRANTY. ANY IMPLIED WARRANTIES THAT MAY BE IMPOSED BY LAW ARE LIMITED TO THE TERMS OF THIS LIMITED WARRANTY.**

# Table of Contents

<b>Product Information .....</b>	<b>1</b>
Front and rear panel components .....	1
Specifications .....	2
Ethernet ports used by the ME260.....	3
Modes and front panel LED blink patterns .....	4
Rear panel LEDs: ICSNet/ICSHub.....	4
Rear panel LEDs: Ethernet .....	5
<b>Installation and Wiring .....</b>	<b>7</b>
Setting the Program Port DIP Switch .....	7
Baud rate settings .....	7
Program Run Disable (PRD) mode.....	7
Setting the Program Port DIP switch.....	8
Program Port Connections/Wiring.....	8
Preparing/connecting captive wires .....	8
DB-9 Program port (front panel).....	8
5-Pin Program port (rear panel) .....	9
ICSNet RJ-45 Connections/Wiring .....	9
ICSHub RJ-45 Connections/Wiring .....	9
ICSHub IN port.....	10
ICSHub OUT port.....	10
Ethernet 10/100 Base-T RJ-45 Connections/Wiring .....	10
SPE Port Connection/Wiring .....	11
SPE cable pinout information.....	12
Mounting the Modules Into an Equipment Rack.....	13
Mounting the NXC-ME260 in an NXF CardFrame or NXI .....	13
Replacing the Lithium Batteries.....	14
<b>Programming .....</b>	<b>15</b>
Program Port Commands.....	15
ESC Pass Codes.....	23
Notes on Specific Telnet/Terminal Clients .....	24
Windows client programs .....	24
Linux Telnet client .....	24
<b>Firmware Transfers .....</b>	<b>25</b>
Sending Firmware to a NetLinx Device (KIT file) .....	25
<b>NetLinx Security .....</b>	<b>27</b>

NetLinx Security Features ..... 27

Security Terms Used in This Document..... 27

    User..... 27

    Group ..... 27

    User Name ..... 28

    Group Name..... 28

    Password ..... 28

    Access Rights ..... 28

    Directory Associations..... 28

Initial Setup (via Telnet or Terminal Connection) ..... 29

    Getting connected ..... 29

    Accessing the Security configuration options..... 29

        1) Set system security options for NetLinx Master (Security Options Menu) ..... 30

        2) Display system security options for NetLinx Master ..... 31

        3) Add user..... 32

        4) Edit User ..... 32

        Edit User Menu ..... 32

        Access Rights Menu ..... 33

        5) Delete user..... 34

        6) Show the list of authorized users ..... 34

        7) Add Group..... 34

        Edit Group Menu ..... 35

        Edit Group Menu: Add directory association ..... 35

        Edit Group menu: Delete directory association..... 36

        Edit Group menu: List directory associations..... 36

        Edit Group menu: Change Access Rights..... 36

        Edit Group menu: Display Access Rights ..... 37

        8) Edit Group..... 37

        9) Delete Group..... 37

        10) Show List of Authorized Groups ..... 38

        11) Set Telnet Timeout in seconds ..... 38

        12) Display Telnet Timeout in seconds ..... 38

        13) Make changes permanent by saving to flash..... 38

    Main Security Menu ..... 39

    Default Security Configuration ..... 40

        Help menu..... 41

    Logging Into a Session..... 42

    Logout ..... 43

        Help Security..... 43

        Setup Security..... 43

# Product Information

The NXC-ME260 Master-Ethernet Card is a Master Card for NetLinx systems with a 10/100BaseT TCP/IP Ethernet connection, and an RJ-11 SPE (Server Port Expander) connector for use with an AXB-SPE (Server Port Expander). The NXC-ME260 is the only Master Card you need, as it incorporates the functionality of all previous NetLinx Master Cards (NXC-M, NXC-ME, and NXC-MPE).

Beyond replacing the previous set of NetLinx Master Cards, the NXC-ME260 represents a high-performance NetLinx Master Controller. With double the Flash memory (16 MB) and a more powerful processor (Coldfire 5407), the ME260 is faster than previous NetLinx Masters.

The NXC-MPE260 can be loaded in the Master Card slot of an NXF NetLinx Cardframe, in an NXI Integrated Controller, or in an NXM-MHS Module, as shown in FIG. 1.

## Front and rear panel components

FIG. 1 shows the front and rear panel components of the NXC-ME260.

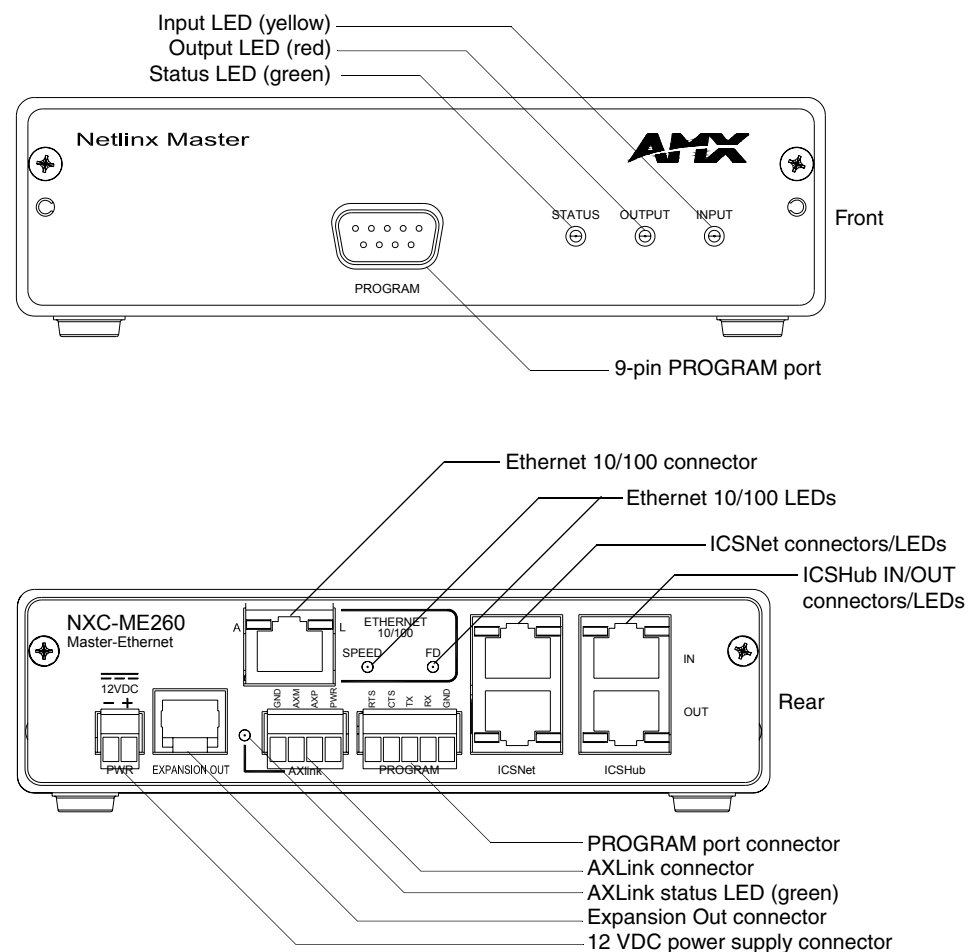


FIG. 1 Front and rear panel components

## Specifications

NXM-ME260 Specifications	
Power consumption	750 mA @ 12 VDC
Memory	<ul style="list-style-type: none"> <li>• Compact Flash: 16 MB standard (upgradeable)</li> <li>• Volatile: 16 MB</li> <li>• Non-volatile: 1 MB</li> </ul>
Microprocessor	Coldfire 5407 (32-bit )
<b>Front Panel Components:</b>	
Program port	<p>DB-9 (male) connector that supports RS-232 communications to your PC for system programming and diagnostics. You set the port's communication speed with the Baud Rate DIP switch. See the <i>Setting the Program Port DIP Switch</i> section on page 7 for details.</p> <p>There are Program ports located on the front and rear panels of the Master Card for easy access. Because these ports share the same circuitry, you should never use both at the same time; doing so will result in communication and/or programming errors.</p>
Status LED	Green LED blinks to indicate that the system is programmed and communicating properly.
Output LED	Red LED blinks when the Master Card transmits data, sets channels on and off, sends data strings, etc.
Input LED	Yellow LED blinks when the Master Card receives data from button pushes, strings, commands, channel levels, etc.
Front Panel LEDs - blink patterns	These LEDs also display special blink patterns when a mode is activated. See the <i>Modes and front panel LED blink patterns</i> section on page 4 for details.
Program Port DIP Switch	8-position DIP switch located behind the front panel for setting the baud rate for the Program port. The baud rate settings are 9600, 38,400 (default), 57,600 and 115,200 (bps). See the <i>Setting the Program Port DIP Switch</i> section on page 7 for details.
<b>Rear Panel Components:</b>	
PWR connector	2-pin (male) green captive-wire connector for 12 VDC power supply.
EXPANSION OUT port	RJ11 connector connects to an AXB-SPE Server Port Expander.
Ethernet 10/100 port	RJ-45 Ethernet 10/100 connector. The Ethernet Port automatically negotiates the connection speed (10 Mbps or 100 Mbps) and whether to use half duplex or full duplex mode.
Ethernet 10/100 LEDs	<p>LEDs that show communication activity, connections, speeds, and mode information:</p> <ul style="list-style-type: none"> <li>• A-activity - Yellow LED blinks when receiving Ethernet data packets.</li> <li>• L-link - Green LED lights when the Ethernet cables are connected and terminated correctly.</li> <li>• SPEED - Green LED lights when transmitting data at 100 Mbps, and is off when transmitting at 10 Mbps.</li> <li>• FD-full duplex - Green LED lights when running in full duplex mode, and is off when running half duplex mode.</li> </ul>
AXlink connector	<p>Black 4-pin (male) captive-wire connector that provides data and power to external control devices.</p> <ul style="list-style-type: none"> <li>• Power rating = 6 A max; actual load depends on connected power supply.</li> </ul>
Axlink Status LED	Green LED blinks to show AXlink and expansion port data activity.
PROGRAM port	5-pin (male) gray connector for system programming and diagnostics. There is a Program port located on the front and rear of the Master Cards for easy access. Because these ports share the same circuitry, you should never use both ports at the same time. Doing so will result in communication and/or programming errors.

<b>NXM-ME260 Specifications (Cont.)</b>	
<b>Rear Panel Components (Cont):</b>	
ICSNet connectors	Two RJ-45 connectors that provide power (500 mA) and data to external ICSNet devices.
ICSNet LEDs	Green LEDs that light when receiving data on that port.
ICSHub In/Out connectors	Two RJ-45 connectors that provide data to other Hubs connected to the Master Card.
ICSHub IN/OUT LEDs	Yellow LEDs that light when receiving data on that port.
Enclosure	Metal with black matte finish.
Front Faceplate	Plastic gray with translucent viewing window.
Dimensions (HWD):	
Card(s)	1.5" x 5.0" x 8.8" (45 mm x 127 mm x 224 mm)
Module	5.0" x 4.8" x 8.5" (127 mm x 121.9 mm x 215.9 mm)
Weight	Card only: 11.5 oz. (32.6 kg) Card with module: 13 oz. (36.8 kg)
Optional Accessories	<ul style="list-style-type: none"> <li>• 12 VDC power supply (PSN 6.5, PSN 2.8)</li> <li>• AC-RK Accessory Rack Kit (Module)</li> </ul>

### **Ethernet ports used by the ME260**

<b>Ethernet Ports Used by the ME260</b>		
<b>Port type</b>	<b>Description</b>	<b>Standard Port #</b>
ICSP	Peer-to-peer protocol used for both master-to-master and master-to-device communications.  For maximum flexibility, the NetLinx Master can be configured to utilize a different port than 1319, or disable ICSP over Ethernet completely from either Telnet or the Program Port located on the NetLinx Master itself.	1319 (UDP/TCP)
ICMP	You must be able to PING an NXC-ME260 to be able to connect to it over a network.	ICMP
Telnet	The NetLinx telnet server provides a mechanism to configure and diagnose a NetLinx system.  For maximum flexibility, the NetLinx Master can be configured to utilize a different port than 23, or disable Telnet completely from either Telnet or the Program Port located on the NetLinx Master itself. Once disabled, the only way to enable Telnet again is from the NetLinx Master's program port.	23 (TCP)
HTTP	The Master has a built-in web server that complies with the HTTP 1.0 specification and supports all of the required features of HTTP v1.1.	80 (TCP)
FTP	The NXC-ME260 has a built-in FTP server that conforms to RFC959.	21/20 (TCP)
Internet Inside	The Internet Inside feature of the NetLinx Master uses, by default, port 10500 for the XML based communication protocol. This port is connected to by the client web browser's JVM when Internet Inside control pages are retrieved from the NetLinx Master's web server.  For maximum flexibility, the NetLinx Master can be configured to utilize a different port than 10500 or to disable Internet Inside completely.	10500 (TCP)

**Modes and front panel LED blink patterns**

The following table lists the modes for the Master Cards/Modules and blink patterns for the front panel LEDs for each mode.

Modes and LED Blink Patterns				
Mode	Description	LEDs and Blink Patterns		
		STATUS (green)	OUTPUT (red)	INPUT (yellow)
OS Start	Starting the operating system (OS).	On	On	On
Boot	Master is booting.	On	Off	On
Contacting DHCP server	Master is contacting a DHCP server for IP configuration information.	On	Off	Fast Blink
Unknown DHCP server	Master could not find the DHCP server.	Fast Blink	Off	Off
Downloading Boot firmware	Downloading Boot firmware to the Master Card's on-board flash memory. <i>Do not cycle power during this process!</i>	Fast Blink	Fast Blink	Fast Blink
No program running	There is no program loaded, or the program is disabled.	On	Normal	Normal
Normal	Master is functioning normally.	1 blink per second	Indicates activity	Indicates activity



NOTE

A static IP must be used for both the Master and computer if there is no DHCP server.

**Rear panel LEDs: ICSNet/ICSHub**

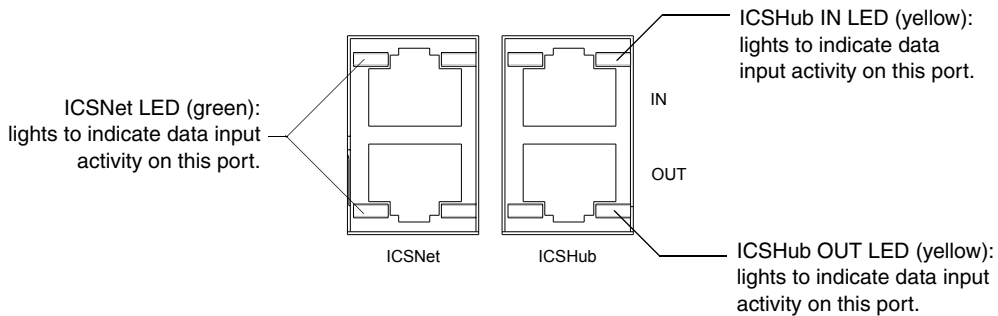
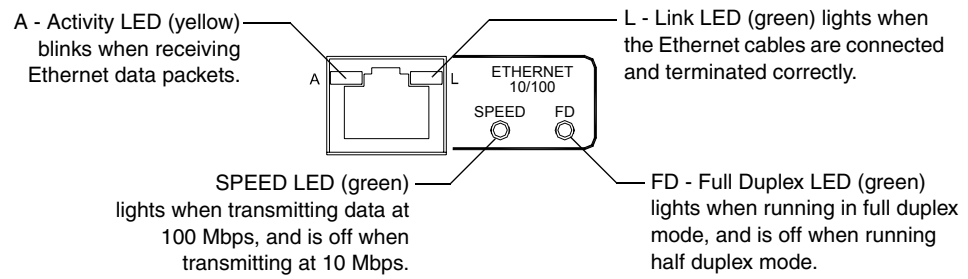


FIG. 2 Layouts of the ICSNet and ICShub LEDs



**Rear panel LEDs: Ethernet****FIG. 3** Layout of Ethernet LEDs



# Installation and Wiring

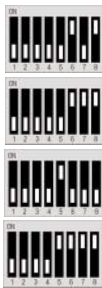
This section contains information about configuring the PROGRAM port, installing NetLinx Modules and the ME260, wiring diagrams, and pinouts for assembling cables.

## Setting the Program Port DIP Switch

### *Baud rate settings*

The Program Port DIP switch is located on the front of the Master Cards. For Modules, you must remove the front panel to access the DIP switch.

Use this DIP switch to set the baud rate for the Program Port, according to the settings shown in the following table. Make sure the baud rate you set matches the baud rate on your PC's COM port before programming the Master Card. By default, the baud rate is set to 38,400 (bps). Note the orientation of the DIP Switch and the ON position label.



Baud Rate Settings				
Baud Rate	Position 5	Position 6	Position 7	Position 8
9600 bps	OFF	ON	OFF	ON
38,400 bps (default)	OFF	ON	ON	ON
57,600 bps	ON	OFF	OFF	OFF
115,200 bps	ON	ON	ON	ON

### *Program Run Disable (PRD) mode*

You can also use the Program Port DIP switch to set the Master Card to Program Run Disable (PRD) mode according to the settings listed in the table below.



PRD Mode Settings	
PRD Mode	Position 1
Normal mode (default)	OFF
PRD Mode	ON

PRD mode prevents the NetLinx program stored in the Master Card from running when you power up the Master Card. PRD mode should only be used when you suspect the resident NetLinx program is causing inadvertent communication and/or control problems. If necessary, place the Master Card in PRD mode and use the NetLinx Studio program to resolve the communication and/or control problems with the resident NetLinx program. Then, download the new NetLinx program and try again.



DIP Switch positions 2,3 and 4 must remain in the OFF position at all times.

**Setting the Program Port DIP switch**

1. Disconnect the power supply from the 2-pin PWR (green) connector on the Master Card.
2. Remove the front faceplate and four mounting screws from the Master Card's front panel. Then, locate the Program Port DIP switch (to the left of the Program port).
3. Set DIP switch positions according to the information listed in the *Baud Rate Settings* and *PRD Mode Settings* tables above.
4. Replace the front panel and faceplate back onto the Master Card and reconnect the 12 VDC power supply to the 2-pin PWR connector.

**Program Port Connections/Wiring**

Master Cards are equipped with two Program ports. One is located on the front panel and the other is on the rear for easy access. The port on the front panel is a DB-9 (male) connector, and the rear port is a 5-pin (male) connector. Use a Programming cable to connect the Program port to your PC's COM port to communicate with the Master Card. Then, you can download NetLinx programs to the Master Card with the NetLinx Studio software program. Refer to the *NetLinx Studio* instruction manual for programming instructions.

**Preparing/connecting captive wires**

1. Strip 0.25 inch of wire insulation off all wires.
2. Insert each wire into the appropriate opening on the connector according to the wiring diagrams and connector types described in this section. Do not tighten the screws excessively; doing so may strip the threads and damage the connector.

**DB-9 Program port (front panel)**

The following table shows the front panel DB-9 Program port connector, pinouts, and signals.

DB-9 Program Port, Pinouts, and Signals		
DB-9 Program Port Connector	Pin	Signal
	2	RX
	3	TX
	5	GND
	7	RTS
	8	CTS

### 5-Pin Program port (rear panel)

The table below lists the pinouts and signals for the rear panel Program port connector.

5-Pin Program Port Pinouts and Signals	
Pin	Signal
1	GND
2	RX
3	TX
4	CTS
5	RTS

### ICSNet RJ-45 Connections/Wiring

The following table shows the pinouts, signals, and pairing information to use for ICSNet RJ-45 connections. The ICSNet connections provide power and data to ICSNet devices. Each port provides up to 500 mA of current.

ICSNet RJ-45 Pinouts/Signals				
Pin	Signal	Connections	Pairing	Color
1	TX +	1 ----- 1	1 ----- 2	orange-white
2	TX -	2 ----- 2		orange
3	Mic -	3 ----- 3	3 ----- 6	green-white
4	GND	4 ----- 4		blue
5	12 VDC	5 ----- 5	4 ----- 5	blue-white
6	Mic +	6 ----- 6		green
7	RX +	7 ----- 7	7 ----- 8	brown-white
8	RX -	8 ----- 8		brown

### ICSHub RJ-45 Connections/Wiring

The two ICSHub RJ-45 connectors on the rear of the Master Card provide data to other Hubs connected to a downstream system. Hubs allow you to connect multiple NetLinx Hubs together in a daisy-chain configuration. Connect the OUT port to the IN port on the second or downstream NetLinx hub.

- Use CAT5 cables for all ICSHub connections.
- **Do not** connect the last hub in a daisy-chain configuration into the first hub.

### ICSHub IN port

The following table describes the pinout/signal information for the ICSHub IN port.

ICS Hub IN Pinouts and Signals		
Pin	Signal	Color
1	TX -	orange-white
2	TX +	orange
3	-----	-----
4	-----	-----
5	-----	-----
6	-----	-----
7	RX -	brown-white
8	RX +	brown

### ICSHub OUT port

The following table describes the pinout/signal information for the ICSHub OUT port.

ICSHub OUT Pinouts and Signals		
Pin	Signal	Color
1	RX +	orange-white
2	RX -	orange
3	-----	-----
4	-----	-----
5	-----	-----
6	-----	-----
7	TX +	brown-white
8	TX -	brown

## Ethernet 10/100 Base-T RJ-45 Connections/Wiring

The following table describes the RJ-45 pinouts, signals and pairing for the Ethernet 10/100 Base-T RJ-45 connector and cable.

Ethernet RJ-45 Pinouts and Signals				
Pin	Signals	Connections	Pairing	Color
1	TX +	1 ----- 1	1 ----- 2	orange-white
2	TX -	2 ----- 2		orange
3	RX +	3 ----- 3	3 ----- 6	green-white
4	no connection	4 ----- 4		blue
5	no connection	5 ----- 5		blue-white
6	RX -	6 ----- 6		green
7	no connection	7 ----- 7		brown-white
8	no connection	8 ----- 8		brown

FIG. 4 diagrams the RJ-45 cable and connectors.

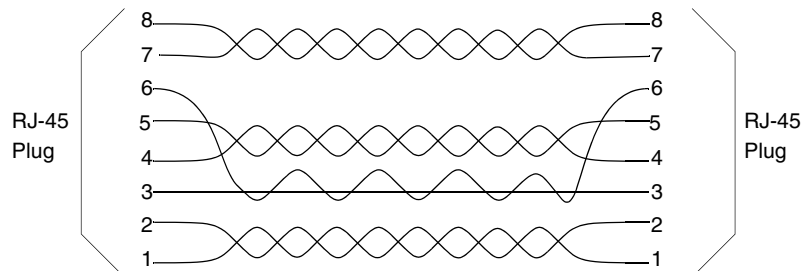


FIG. 4 RJ-45 wiring diagram

## SPE Port Connection/Wiring

Use an RJ-11 cable to connect the NXC-ME260 to an AXB-SPE Slave Port Expander.

The EXPANSION OUT port on the rear panel of the NXC-ME260 connects to the EXPANSION IN port on the rear panel of the AXB-SPE (FIG. 5).

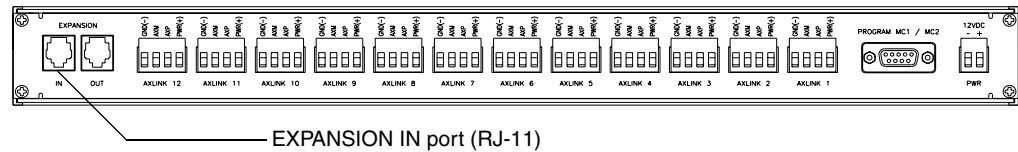


FIG. 5 AXB-SPE (rear panel)

You can daisy chain multiple AXB-SPE's by connecting the EXPANSION OUT on the primary AXB-SPE to the EXPANSION IN port on the secondary, as shown in FIG. 6. The connecting RJ-11 cable should not exceed 6" in length. Repeat this process to connect up to nine AXB-SPE's.

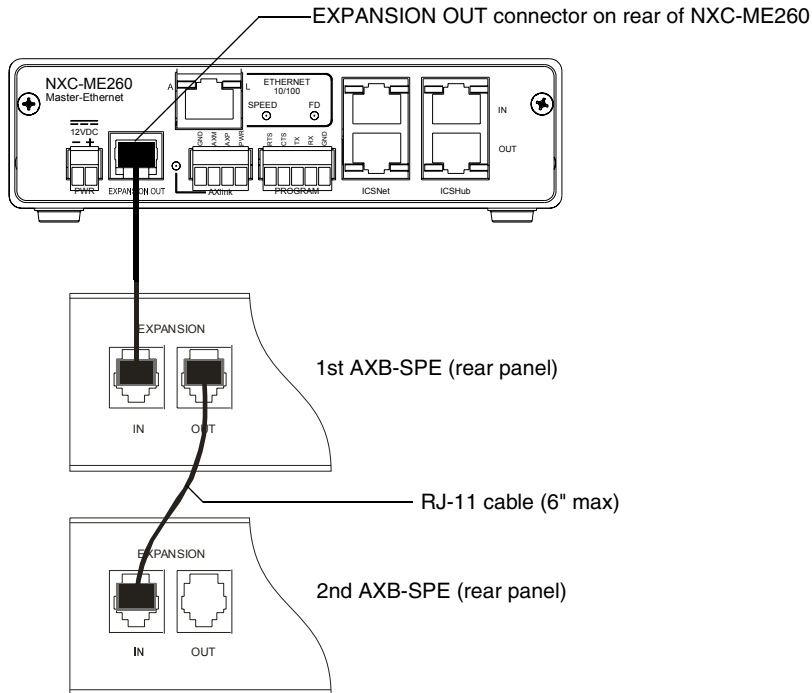


FIG. 6 Daisy chaining two or more AXB-SPE's off of an NXC-ME260

**SPE cable pinout information**

The following table gives pinout information for the RJ-11 SPE connector. AMX supplies a 6" RJ-11 cable with the AXB-SPE.

The EXPANSION connectors (on the AXB-SPE) use pins 2, 3, 4 and 5. Pin 2 is Ground; the others are all pin-to-pin connections.

SPE Connector Pinouts and Signals	
Pin	Signal
1	no connect
2	GND
3	TX
4	TX enable
5	RX
6	no connect



*Do not use a standard phone extension cable; it will not work with the AXB-SPE.*



FIG. 7 diagrams the RJ-11 cable and connectors.

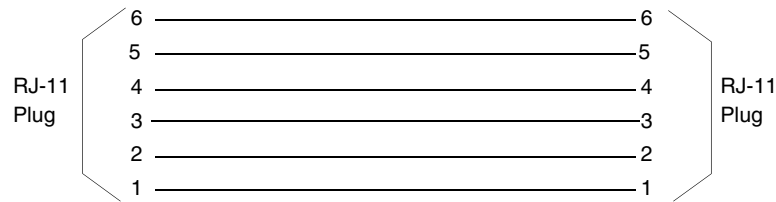


FIG. 7 RJ-11 wiring diagram

## Mounting the Modules Into an Equipment Rack

To install the Modules into an equipment rack, you'll need an optional AC-RK Kit.

1. Remove the front panel from the Module to expose the mounting holes.
2. Mount the module on the AC-RK bracket.
3. Place the AC-RK bracket (with the module) in the equipment rack and secure the bracket to the rack.
4. Replace the front panel to the Module, and reattach the plastic faceplate (if necessary).

## Mounting the NXC-ME260 in an NXF CardFrame or NXI

The NXC-ME260 can be installed in a NetLinx CardFrame (NXF), or NetLinx Integrated Controller (NXI). In both cases, the card mounts in a horizontal position, through the Master Card slot on the rear panel of the enclosure.

FIG. 8 shows the Master Card slot on the NXF CardFrame.

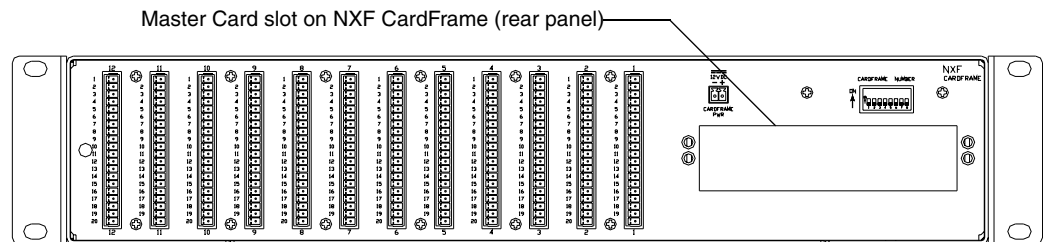


FIG. 8 Master Card slot on rear panel of the NXF CardFrame

FIG. 9 shows the Master Card slot on the NXI Integrated Controller.

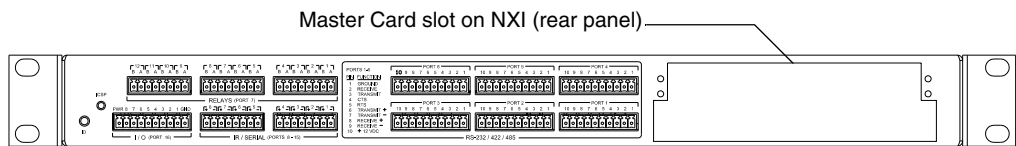


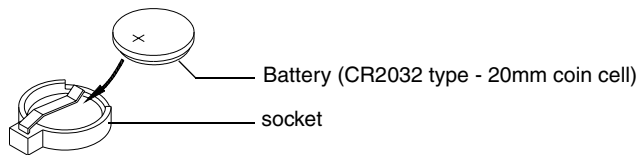
FIG. 9 Master Card slot on rear panel of the NXI Integrated Controller

To install a Master Card in either an NXF CardFrame or NXI Integrated Controller:

1. Discharge the static electricity from your body by touching a grounded object.
2. Unplug all the connectors from the Controller or Module.
3. Remove the two screws that hold the front plate on the Master Card, and remove the front plate.
4. Align the edges of the card with the guide slots inside the Master Card slot on the NXF or NXI.
5. Slide the card about halfway into the slot.
6. Inside the Master Card slot on the NXF or NXI, find the 6-pin control cable connector.
7. Plug the connector from the NXF or NXI into the 6-pin terminal on the Master Card. This connector is keyed to ensure correct orientation.
8. Once the control cable is connected, gently slide the card all the way in until you feel the rear edge of the card lightly snap into place.
9. Re-apply power and other connections as necessary.

## Replacing the Lithium Batteries

The NXC-ME260 is equipped with two lithium batteries (FG# 57-0013) that have a life of approximately 5 years to protect their memory. When DC power is on, the batteries are not used. When replacing the batteries, remove one at a time to avoid losing the program in memory.



**FIG. 10** Lithium battery and socket

1. Discharge the static electricity from your body by touching a grounded metal object.
2. Unplug all the connectors from the Controller or Module.
  - NetLinx Integrated Controller (NXI): Remove the rear panel from the NXI. Then, disconnect the NXI control cable and remove the Master Card.
  - NetLinx Module (NXM-xxx): Remove the rear panel from the Module, and remove the Master Card.
3. Carefully slide one battery out of its socket, and insert the new battery.
4. Plug the 2-pin PWR (green) connector to reapply power. Wait approximately 1 minute. Then, remove the PWR connector again.
5. Carefully slide the other battery out of its socket and insert the new battery.
6. Replace the Master Card (re-connect the NXI control cable to the Master Card if replacing in an NXI).
7. Replace the rear panel and secure with the mounting screws; reconnect all control, communication, and power cables.

# Programming

The NetLinX programming language allows numbers in the range 0-32,767. Device 0 refers to the Master Card; numbers greater than 32,767 are reserved for internal use only.

The NetLinX programming language requires a Device:Port:System (D:P:S) syntax where Access expects only a device number. The NetLinX D:P:S triplet variable is expressed as:

```
DEVICE:PORT:SYSTEM
```

where:

- Device: 16-bit integer representing the device number (0-32,767).  
0 = the local Master.
- Port: 16-bit integer representing the port number (in the range 1 through the number of ports on the NetLinX Master or device).
- System: 16-bit integer representing the system number (0 = this system).

## Program Port Commands

The Program port commands listed in the Program Port Commands table below can be sent directly to the Master Card using a terminal program (i.e. Telnet). In order for Telnet to be effective, you must initiate a session with the master. Be sure that your PC's COM port and terminal program's communication settings match those in the following table.

PC COM Port Communication Settings	
Baud	38400 (default)
Parity	none
Data Bits	8
Stop Bits	1
Flow Control	none

In your terminal program, type "help" or a "?" <Enter> to display the Program port commands listed below.

Program Port Commands	
Command	Description
ECHO OFF	Disables terminal character's echo (display) function.
ECHO ON	Enables terminal character's echo (display) function.
DATE	Displays the current date and day of the week. Example: >DATE 10/31/2001 Wed

Program Port Commands (Cont.)	
Command	Description
SET DATE	<p>Prompts you to enter the new date for the Master Card.</p> <p>When the date is set on the Master Card, the new date will be reflected on all devices in the system that have clocks (i.e. touch panels). By the same token, if you set the date on any system device, the new date will be reflected on the system's Master, and on all connected devices.</p> <p>This will not update clocks on devices connected to another Master (in Master-to-Master systems).</p> <p>Example:</p> <pre>&gt;SET DATE Enter Date: (mm/dd/yyyy) -&gt;</pre>
TIME	<p>Displays the current time on the Master Card.</p> <p>Example:</p> <pre>&gt;TIME 13:42:04</pre>
SET TIME	<p>Prompts you to enter the new time for the Master Card.</p> <p>When the time is set on the Master Card, the new time will be reflected on all devices in the system that have clocks (i.e. touch panels). By the same token, if you set the time on any system device, the new time will be reflected on the system's Master, and on all connected devices.</p> <p>This will not update clocks on devices connected to another Master (in Master-to-Master systems).</p> <p>Example:</p> <pre>&gt;SET TIME Enter Date: (hh:mm:ss) -&gt;</pre>
DEVICE STATUS <D:P:S>	<p>Displays a list of all active (on) channels for the specified D:P:S. Enter DEVICE STATUS without the D:P:S variable, the Master Card displays ports, channels, and version information.</p> <p>Displays status of the specified Master.</p> <p>Example (on a local Master):</p> <pre>&gt;DEVICE STATUS [0:1:0] Device 0 AMX Corp.,Master,v2.10.75 contains 1 Ports. Port 1 - Channels:256 Levels:8 MaxStringLen=64 Types=8 bit MaxCommandLen=64 Types=8 bit The following input channels are on:None The following output channels are on:None The following feedback channels are on:None Level 1=0 Supported data types=UByte,UInt Level 2=0 Supported data types=UByte,UInt Level 3=0 Supported data types=UByte,UInt Level 4=0 Supported data types=UByte,UInt Level 5=0 Supported data types=UByte,UInt Level 6=0 Supported data types=UByte,UInt Level 7=0 Supported data types=UByte,UInt Level 8=0 Supported data types=UByte,UInt</pre>
DNS LIST <D:P:S>	<p>Displays:</p> <ul style="list-style-type: none"> <li>• Domain suffix</li> <li>• Configured DNS IP Information</li> </ul> <p>Example:</p> <pre>&gt;DNS LIST [0:1:0] Domain suffix:amx.com The following DNS IPs are configured Entry 1-192.168.20.5 Entry 2-12.18.110.8 Entry 3-12.18.110.7</pre>

Program Port Commands (Cont.)	
Command	Description
DISK FREE	<p>Displays the total bytes of free space available on the Master Card's compact Flash memory.</p> <p>Example:</p> <pre>&gt;DISK FREE The disk has 2441216 bytes of free space.</pre>
GET IP <D:P:S>	<p>Displays the Master Card's D:P:S, Host Name, Type (DHCP or Static), IP Address, Subnet Mask, Gateway IP, and MAC Address.</p> <p>Example:</p> <pre>&gt;GET IP [0:1:50] IP Settings for 0:1:50   HostName   MLK_INSTRUCTOR   Type       DHCP   IP Address 192.168.21.101   Subnet Mask 255.255.255.0   Gateway IP 192.168.21.2   MAC Address 00:60:9f:90:0d:39</pre>
MEM	<p>Displays the largest free block of Master Card memory.</p> <p>Example:</p> <pre>&gt;MEM The largest free block of memory is 11442776 bytes.</pre>
MSG ON or MSG OFF	<p>MSG On sets the terminal program to display all messages generated by the Master Card. MSG OFF disables the display.</p> <p>Example:</p> <pre>&gt; MSG ON Extended diagnostic information messages turned on. &gt; MSG OFF Extended diagnostic information messages turned off.</pre>
OFF <D:P:S, channel>	<p>Turns off a channel on a device. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system, or the name of the device that is defined in the DEFINE_DEVICE section of the program.</p> <p>Syntax:</p> <pre>OFF [name, channel] -or- OFF [D:P:S, channel]</pre> <p>Example:</p> <pre>&gt;OFF [5001:7:4] Sending Off [5001:7:4]</pre>
ON <D:P:S, channel>	<p>Turns on a channel on a device. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system; or the name of the device that is defined in the DEFINE_DEVICE section of the program.</p> <p>Syntax:</p> <pre>ON [name, channel] or ON [D:P:S, channel]</pre> <p>Example:</p> <pre>&gt;ON [5001:7:4] Sending On [5001:7:4]</pre>

Program Port Commands (Cont.)	
Command	Description
PASS <D:P:S>	<p>Sets up a pass through mode to a device. In pass through mode, any string received by the device is displayed on the screen, and anything typed is sent as a string to the device. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system, or the name of the device that is defined in the DEFINE_DEVICE section of the program.</p> <p>Example:</p> <pre>&gt;pass [5001:7:4] Entering pass mode. To exit pass mode, type + + esc esc.</pre>
PING <IP ADDRESS>	<p>Tests network connectivity to and confirms the presence of another networked device. The syntax is just like the PING application in Windows or Linux.</p> <p>Example:</p> <pre>&gt;ping 192.168.21.209 192.168.21.209 is alive.</pre>
PROGRAM INFO	<p>Displays the name of the NetLinx program residing in the Master Card.</p> <p>Example:</p> <pre>&gt;PROGRAM INFO -- Program Name Info -- Module Count = 1    1 Name is i!-PCLinkPowerPointTest  -- File Names = 2    1 = C:\Program Files\AMX Applications\i!-PCLinkPowerPoint    2 = C:\Program Files\Common Files\AMXShare\AXIs\NetLinx.axi    2 = Name is MDLPP  -- File Names = 2    1 C:\AppDev\i!-PCLink-PowerPoint\i!-PCLinkPowerPointMod.axs    2 C:\Program files\Common Files\AMXShare\AXIs\NetLinx.axi</pre>
PULSE <D:P:S, channel>	<p>Pulses a channel on a device on and off. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system; or the name of the device that is defined in the DEFINE_DEVICE section of the program.</p> <p>Example:</p> <pre>&gt;PULSE [50001:8:50,1] Sending Pulse [50001:8:50,1]</pre>
REBOOT <D:P:S>	<p>Reboots the Master Card or specified device.</p> <p>Example:</p> <pre>&gt;REBOOT [0:1:0] Rebooting...</pre>
RELEASE DHCP	<p>Releases the DHCP setting for the Master Card.</p> <p>Example:</p> <pre>&gt;RELEASE DHCP The Master must be rebooted to acquire a new DHCP lease.</pre>

Program Port Commands (Cont.)	
Command	Description
ROUTE MODE DIRECT   NORMAL	<p>Sets the Master-to-Master route mode:</p> <ul style="list-style-type: none"> <li>• Normal mode - allows a Master to communicate with any Master accessible via the routing tables (shown with the SHOW ROUTE command). This includes a directly-connected Master (route metric =1) and indirectly connected masters (route metric greater than 1, but less than 16).</li> <li>• Direct mode - allows communication only with masters that are directly connected (route metric = 1). Indirectly connected masters cannot be communicated within this mode.</li> </ul> <p>Examples:</p> <pre>&gt;ROUTE MODE DIRECT   Route Mode "Direct" Set &gt;ROUTE MODE NORMAL   Route Mode "Normal" Set</pre>
SEND_COMMAND <D:P:S>	Sends a command to a device. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system; or the name of the device that is defined in the DEFINE_DEVICE section of the NetLinx Program. The data of the string is entered with NetLinx string syntax.
SEND_STRING <D:P:S>	Sends a string to a device. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system; or the name of the device defined in the DEFINE_DEVICE section of the NetLinx Program. The data of the string is entered with NetLinx string syntax.
SET DNS <D:P:S>	<p>Prompts you to enter a Domain Name, DNS IP #1, DNS IP #2, and DNS IP #3. Then, enter Y (yes) to approve/store the information in the Master Card. Entering N (no) cancels the operation.</p> <p>Example:</p> <pre>&gt;SET DNS [0:1:0] -- Enter New Values or just hit Enter to keep current settings --  Enter Domain Suffix: amx.com Enter DNS Entry 1 : 192.168.20.5 Enter DNS Entry 2 : 12.18.110.8 Enter DNS Entry 3 : 12.18.110.7  You have entered: Domain Name: amx.com                   DNS Entry 1: 192.168.20.5                   DNS Entry 2: 12.18.110.8                   DNS Entry 3: 12.18.110.7  Is this correct? Type Y or N and Enter -&gt; Y Settings written. Device must be rebooted to enable new settings</pre>
SET IP <D:P:S>	<p>Prompts you to enter a Host Name, Type (DHCP or Fixed), IP address, Subnet Mask, and Gateway IP address. Enter Y (yes) to approve/store the information in the Master Card. Entering N (no) cancels the operation.</p> <p>Example:</p> <pre>&gt;SET IP [0:1:0] --- Enter New Values or just hit Enter to keep current settings ---  Enter Host Name:   MLK_INSTRUCTOR Enter IP type. Type D for DHCP or S for Static IP and then Enter: DHCP Enter Gateway IP: 192.168.21.2  You have entered: Host Name   MLK_INSTRUCTOR                   Type       DHCP                   Gateway IP 192.168.21.2  Is this correct? Type Y or N and Enter -&gt; y Settings written. Device must be rebooted to enable new settings.</pre>





Program Port Commands (Cont.)	
Command	Description
SHOW LOG	<p>Displays the log of messages stored in the Master's memory.</p> <p>The Master logs all internal messages and keeps the most recent messages. The log contains:-</p> <ul style="list-style-type: none"> <li>• Entries starting with first specified or most recent</li> <li>• Date, Day, and Time message was logged</li> <li>• Which object originated the message</li> <li>• The text of the message</li> </ul> <p>SHOW LOG [start] [end] SHOW LOG ALL</p> <p>If start is not entered, the most recent message will be first.</p> <p>If end is not entered, the last 20 messages will be shown.</p> <p>If ALL is entered, all stored messages will be shown, starting with the most recent.</p> <p>Example:</p> <pre>&gt;SHOW LOG Message Log for System 50 Version: v2.10.75 Entry      Date/Time      Object Text ----- 1: 11-01-2001 THU 14:14:49 ConnectionManager Memory Available = 11436804 &lt;26572&gt; 2: 11-01-2001 THU 14:12:14 ConnectionManager Memory Available = 11463376 &lt;65544&gt; 3: 11-01-2001 THU 14:10:21 ConnectionManager Memory Available = 11528920 &lt;11512&gt; 4: 11-01-2001 THU 14:10:21 TelnetSvr Accepted Telnet connection:socket=14 addr=192.168.16.110 port=2979 5: 11-01-2001 THU 14:05:51 Interpreter CIPEvent::OnLine 10002:1:50 6: 11-01-2001 THU 14:05:51 Interpreter CIPEvent::OnLine 128:1:50 7: 11-01-2001 THU 14:05:51 Interpreter CIPEvent::OffLine 128:1:50 8: 11-01-2001 THU 14:05:51 Interpreter CIPEvent::OnLine 96:1:50 9: 11-01-2001 THU 14:05:51 Interpreter CIPEvent::OffLine 96:1:50 10: 11-01-2001 THU 14:05:51 Interpreter CIPEvent::OnLine 128:1:50 11: 11-01-2001 THU 14:05:51 Interpreter CIPEvent::OnLine 96:1:50 12: 11-01-2001 THU 14:05:51 Interpreter CIPEvent::OnLine 5001:16:50 13: 11-01-2001 THU 14:05:51 Interpreter CIPEvent::OnLine 5001:15:50 14: 11-01-2001 THU 14:05:51 Interpreter CIPEvent::OnLine 5001:14:50 15: 11-01-2001 THU 14:05:51 Interpreter CIPEvent::OnLine 5001:13:50 16: 11-01-2001 THU 14:05:51 Interpreter CIPEvent::OnLine 5001:12:50 17: 11-01-2001 THU 14:05:51 Interpreter CIPEvent::OnLine 5001:11:50 18: 11-01-2001 THU 14:05:51 Interpreter CIPEvent::OnLine 5001:10:50 19: 11-01-2001 THU 14:05:51 Interpreter CIPEvent::OnLine 5001:9:50 20: 11-01-2001 THU 14:05:51 Interpreter CIPEvent::OnLine 5001:8:50</pre>
SHOW NOTIFY	<p>Displays a list of devices (up to 1000) that other systems have requested input from and the types of information needed.</p> <p>Example:</p> <pre>&gt;SHOW NOTIFY  Device Notification List of devices requested by other Systems  Device:Port   System  Needs ----- 00128:00001   00108  Channels Commands Strings Levels 33000:00001   00108  Channels Commands</pre>



Program Port Commands (Cont.)	
Command	Description
TCP LIST	Lists all active TCP/IP connections. Example: <pre>&gt;TCP LIST The following TCP connections exist(ed): 1: IP=192.168.21.56:1042 Socket=0 (Dead) 2: IP=192.168.21.56:1420 Socket=0 (Dead)</pre>
URL LIST <D:P:S>	Displays the list of URL addresses programmed in the Master Card (or another system). Example: <pre>&gt;URL LIST The following URLs exist in the URL connection list -&gt;Entry 0-192.168.13.65:1319 IP=192.168.13.65 State=Connected Entry 1-192.168.13.200:1319 IP=192.168.13.200 State=Issue Connect</pre>

## ESC Pass Codes

There are 'escape' codes in the pass mode. These codes can switch the display mode or exit the pass mode. The following 'escape' codes are defined.

ESC Pass Codes	
Command	Description
+ + ESC ESC Exit Pass Mode	Typing a plus (shift =) followed by another plus followed by an ESC (the escape key) followed by another escape exits the pass mode. The Telnet session returns to "normal".
+ + ESC A ASCII Display Mode	Typing a plus (shift =) followed by another plus followed by an ESC (the escape key) followed by an 'A' sets the display to ASCII mode. Any ASCII characters received by the device will be displayed by their ASCII symbol. Any non-ASCII characters will be displayed with a \ followed by two hex characters to indicate the character's hex value.
+ + ESC D Decimal Display Mode	Typing a plus (shift =) followed by another plus followed by an ESC (the escape key) followed by an 'D' sets the display to decimal mode. Any characters received by the device will be displayed with a \ followed by numeric characters to indicate the character's decimal value.
+ + ESC H Hex Display Mode	Typing a plus (shift =) followed by another plus followed by an ESC (the escape key) followed by an 'H' sets the display to hexadecimal mode. Any characters received by the device will be displayed with a \ followed by two hex characters to indicate the character's hex value.

## Notes on Specific Telnet/Terminal Clients

Telnet and terminal clients will have different behaviors in some situations. This section states some of the known anomalies.

### *Windows client programs*

Anomalies occur when using a windows client if you are not typing standard ASCII characters (i.e. using the keypad and the ALT key to enter decimal codes). Most programs will allow you to enter specific decimal codes by holding ALT and using keypad numbers.

For example, hold ALT, hit keypad 1, then hit keypad 0, then release ALT. The standard line feed code is entered (decimal 10). Windows will perform an AnsiToOem conversion on some codes entered this way because of the way Windows handles languages and code pages. The following codes are known to be altered, but others may be affected depending on the computer's setup.

- Characters 15, 21, and 22
- Any characters above 127

This affects both Windows Telnet and Terminal programs.

### *Linux Telnet client*

The Linux Telnet client has three anomalies that are known at this time:

- A null (\00) character is sent after a carriage return.
- If an ALT 255 is entered, two 255 characters are sent (per the telnet RFC).
- If the code to go back to command mode is entered (ALT 29 which is ^J), the character is not sent, but telnet command mode is entered.

# Firmware Transfers

NetLinx Studio 2.0 provides the ability to download KIT firmware files to the NetLinx NXC-ME260 Master.

To send firmware files, select **Tools > Firmware Transfers**, then select Send to NetLinx Device from the sub-menu.



NOTE

*When using the NXC-ME260 with G4 products, use firmware build 85 or higher. Earlier firmware versions do not support G4 products.*

## Sending Firmware to a NetLinx Device (KIT file)

Use the Firmware Transfers options in the Tools menu to update the firmware in NetLinx Master Controllers or System devices. NXI Master Controllers use Kit files for firmware upgrades. A Kit file (.KIT) is a package of several files, all of which are required to upgrade the firmware, and are available online via [www.amx.com/firmware-files.asp](http://www.amx.com/firmware-files.asp).

- The Online Device Tree (Online Tree tab of the Workspace Window) displays information about each online device, including the current firmware version.
- Before attempting to upgrade the firmware, you must have the appropriate Kit file for your NetLinx Master.



NOTE

*If for any reason your Kit file transfer should fail, continue to retry the transfer until you are successful. DO NOT reboot the Master, or change connections until the transfer is complete. Failure to complete this operation successfully may result in a factory repair of the Master.*

To update NetLinx firmware:

1. Choose **Tools > Firmware Transfers > Send to NetLinx Device** to open the Send To NetLinx Device dialog.
2. Click the Browse button to navigate to the target directory (in the Browse For Folder dialog). The selected directory path is displayed in the Location text box. Assuming that the specified target directory contains one or more Kit files, the Kit files in the selected directory are displayed in the Files list box (with the file's last modified date and time).
3. Enter the Device and System ID numbers for the target NetLinx Device in the Device and System text boxes.

If the Kit file is determined to be specifically for the target Master, the Device number is forced to zero. If the Kit file is for an unspecified device, you must enter the correct Device ID number. You can use the Online Device Tree to determine the device's assigned ID.

4. Review the File, Connection, Address, and Target Device information before you send.
  - Check the Reboot option.
  - Click the Send button to send the selected KIT file to the specified device. You can watch the progress of the transfer in the Send to NetLinx Device dialog.
  - When the transfer is finished, and the reboot is complete, press the Close button.



*Allow 20-30 seconds for NetLinx Masters to reboot. When the Master has rebooted, the Status LED on the front panel blinks once a second to indicate that it is functioning properly. Once it has rebooted, click OK.*

# NetLinx Security

NetLinx Masters (version 2.10.80 or later) have built-in security capabilities. It will require a valid user name and password to access the NetLinx System's Telnet, HTTP and FTP servers.

The security capabilities are configured and applied via a Telnet connection or the NetLinx Master's RS-232 terminal interface (the DB9 PROGRAM port on the rear of the Controller).



NOTE

*Always use the Program port when entering potentially sensitive security information. The Telnet server interface exposes this security information to the network in clear text format, which would be rather easy to intercept by an unauthorized client. By using the Program port, there is some level of security during the configuration of the database, due to the physical proximity of the user to the system.*

## NetLinx Security Features

NetLinx security allows you to define access rights for users or groups.



NOTE

*A "User" represents a single potential client of the NetLinx Master, while a "Group" represents a logical collection of users. Any properties possessed by groups (i.e., access rights, directory associations, etc.) are inherited by all the members of the group.*

The following table lists the NetLinx features that the administrator (or other 'qualified' user) may grant or deny access to.

NetLinx Security Features	
NetLinx Master Security Configuration	The user has access to the security configuration commands of the Master. Only those users with security configuration access rights granted will have access to the security configuration commands.
Telnet Security	The user has access to the Telnet server functionality. All basic commands are available to the user.
Terminal (PROGRAM port) Security	The user has access to the Terminal (RS232 PROGRAM port) server functionality. All basic commands are available to the user.
HTTP (web server) Security	The user has access to the HTTP server functionality. Directory associations assign specific directories/files to a particular user.
FTP Security	The user has access to the FTP server functionality. Only the administrator account has access to the root directory; all other 'qualified' clients are restricted to the /user/ directory and its 'tree'.

## Security Terms Used in This Document

### **User**

A user is a single potential client of the NetLinx Master.

### **Group**

A group is a logical collection of users. Note that any properties possessed by groups (i.e., access rights, directory associations, etc.) are inherited by all of the members of the group.

### User Name

A user name is a valid character string (4 - 20 alpha-numeric characters) defining the user. This string is *case sensitive*. Each user name must be unique.

### Group Name

A group name is a valid character string (4 - 20 alpha-numeric characters) defining the group. This string is *case sensitive*. Each group name must be unique.

### Password

A password is a valid character string (4 - 20 alpha-numeric characters) to supplement the user name in defining the potential client. This string is also *case sensitive*.

### Access Rights

Each of the features of the NetLinx Master has security procedures defined for them. The access right for a particular feature determines if the user / group is to have access to the feature (make use of the feature).

### Directory Associations

A Directory Association is a path that defines the directories and/or files that a particular user or group can access via the HTTP (Web) Server on the NetLinx Master. This character string can range from 1 to 128 alpha-numeric characters. This string is *case sensitive*. This is the path to the file or directory you want to grant access. Access is limited to the user (i.e. doc:user) directory of the master. All subdirectories of the user directory can be granted access.

A single '/' is sufficient to grant access to all files and directories in the user directory and it's sub-directory. The '\*' wildcard can also be added to enable access to all files. All entries should start with a '/'. Here are some examples of valid entries:

Path	Notes
/	Enables access to the user directory and all files and subdirectories in the user directory.
/*	Enables access to the user directory and all files and subdirectories in the user directory.
/user1	If user1 is a file in the user directory, only the file is granted access. If user1 is a subdirectory of the user directory, all files in the user1 and its sub-directories are granted access.
/user1/	user1 is a subdirectory of the user directory. All files in the user1 and its sub-directories are granted access.
/Room1/iWebControlPages/*	/Room1/iWebControlPages is a subdirectory and all files and its subdirectories are granted access.
/results.txt	results.txt is a file in the user directory and access is granted to that file.

By default, all accounts that enable HTTP Access are given a '/' Directory Association if no other Directory Association has been assigned to the account.

When you are prompted to enter the path for a Directory Association, the NetLinx Master will attempt to validate the path. If the directory or file is not valid (i.e. it does not exist at the time you entered the path), the NetLinx Master will ask you whether you were intending to grant access to a file or directory. From the answer, it will enter the appropriate Directory Association. The NetLinx



Master will not create the path if it is not valid. That must be done via another means, most commonly by using an FTP client and connecting to the FTP server on the NetLinx Master.

## Initial Setup (via Telnet or Terminal Connection)

Security administration and configuration is done via either Telnet (the Ethernet Port on the NetLinx Master), or Terminal (the PROGRAM Port on the NetLinx Master).

If you have NetLinx Studio installed, use the **Tools > Windows Telnet** option to launch a Telnet session (or alternatively the **Tools > Terminal** option to open a Terminal session). If you do not have NetLinx Studio on your machine, you can use another terminal program (i.e. HyperTerminal).

### Getting connected

1. Apply power to the NetLinx Master and allow it to boot up.
2. Connect your PC or laptop to the NetLinx Master:
  - a. If connecting via Telnet, connect the PC or laptop Ethernet (RJ-45) port through a Router/Hub to the Ethernet port on the NetLinx Master.
  - b. If connecting via Terminal; connect the PC COM (RS232) port to the PROGRAM port on the front of the NetLinx Master. Verify that the baud rate for the COM port matches the Master COM Port setting on the NetLinx Master (default = 38,400).
3. Launch NetLinx Studio, and select **Tools > Windows Telnet** to open a Telnet session window. Select **Tools > Terminal** to open a Terminal session.
4. Type **echo on** to view the characters while entering commands.

### Accessing the Security configuration options

1. In the Telnet (or Terminal) session, type **help security** to view the available security commands. Here is a listing of the security help:

```

---- These commands apply to the Security Manager and Database ----
logout                               Logout and close secure session
setup security                        Access the security setup menus

```

2. Type **setup security** to access the Main Security Menu, shown below:

```
>setup security
```

```

--- These commands apply to the Security Manager and Database ---
1) Set system security options for NetLinx Master
2) Display system security options for NetLinx Master
3) Add user
4) Edit user
5) Delete user
6) Show the list of authorized users
7) Add group
8) Edit group
9) Delete group
10) Show list of authorized groups
11) Set Telnet Timeout in seconds
12) Display Telnet Timeout in seconds
13) Make changes permanent by saving to flash

```

↓ (Cont.)

Or <ENTER> to return to previous menu

Security Setup ->

3. The Main Security Menu shows a list of choices and a prompt. To select one of the listed choices, simply enter the number of the choice (1-13) at the prompt and press <ENTER>.
4. Each option in the Main Security Menu displays a sub-menu specific to that option.

The following sub-section describe using each of the Main Security Menu options.

For a detailed description of each option in the Main Security Menu, refer to *Main Security Menu on page 39*.

### 1) Set system security options for NetLinx Master (Security Options Menu)

Type **1** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to display the **Security Options Menu**.

The Security Options Menu sets the "global" options for the NetLinx Master. It is accessed by the Set Security system options of the Main Security Menu. This first thing that will happen is you will be asked one of two questions. If NetLinx Master security is enabled, you will see the following:

```
NetLinx Master security is Enabled
Do you want to keep NetLinx Master security enabled? (y or n):
```

- If you answer **y** for yes, security will remain enabled and you will be taken to the Security Options Menu.
- If you answer **n** for no, all security settings (except FTP security) will be disabled and you will be taken back to the Main Security Menu.

If NetLinx Master security is not enabled, you will see the following:

```
NetLinx Master security is Disabled
Do you want to enable security for the NetLinx Master? (y or n):
```

- If you answer **y** for yes, security will be enabled and you will be taken to the Security Options Menu.
- If you answer **n** for no, all security settings (except FTP security) will remain disabled and you will be taken back to the Main Security Menu.

The Security Options Menu is displayed as follows:

```
Select to change current security option
 1) Terminal (RS232) Security..... Enabled
 2) HTTP Security..... Enabled
 3) Telnet Security..... Enabled
 4) Security Configuration Security..... Enabled
Or <ENTER> to return to previous menu
```

Security Options ->

The selection listed will display what the current settings. To change an option, select the number listed next to the option.



*The Master must be rebooted after changing the HTTP setting.*

For example, if selection 2) is selected, HTTP Security will be disabled. The menu will then be displayed again as follows:

```
Select to change current security option
 1) Terminal (RS232) Security..... Enabled
 2) HTTP Security..... Disabled
 3) Telnet Security..... Enabled
 4) Security Configuration Security..... Enabled
Or <ENTER> to return to previous menu
```

Security Options ->

Each selection simply toggles the security setting selected. Press <ENTER> to exit the menu and return to the Main Security Menu.



*The Master must be rebooted after changing the HTTP setting.*

The items in the Security Options Menu are described below:

Security Options Menu	
Command	Description
1) Terminal (RS232) Security (Enabled/Disabled)	This selection enables/disables Terminal (RS232 Program port) Security. If Terminal Security is enabled, a user must have sufficient access rights to login to a Terminal session.
2) HTTP Security (Enabled/Disabled)	This selection enables/disables HTTP (Web Server) Security. If HTTP Security is enabled, a user must have sufficient access rights to browse to the NetLinx Master with a Web Browser.
3) Telnet Security (Enabled/Disabled)	This selection enables/disables Telnet Security. If Telnet Security is enabled, a user must have sufficient access rights to login to a Telnet session.
4) Security Configuration Security (Enabled/Disabled)	This selection enables/disables Security Configuration Security. If Security Configuration Security is enabled, a user must have sufficient access rights to access the Main Security Menu.

### **2) Display system security options for NetLinx Master**

Type 2 and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to display the current security options, and their current state (Enabled/Disabled). For example:

```
Master Security.....Disabled
Terminal.....Disabled
HTTP.....Disabled
Telnet.....Disabled
Security/Configuration.....Disabled
```

Press <ENTER> key to continue

### 3) Add user

1. Type **3** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to create a new user account. A sample session response is:

```
The following users are currently enrolled:
administrator
Fred
Betty
```

```
Enter user name:
```

2. At the **Enter user name** prompt, enter a new user name (for example "Bilbo"). A user name is a valid character string (4 - 20 alpha-numeric characters) defining the user. This string is *case sensitive*. Each user name must be unique.
3. Press <ENTER> to enter the new user name. The session then prompts you for a password for the new user.
4. Enter a password for the new user. A password is a valid character string (4 - 20 alpha-numeric characters) to supplement the user name in defining the potential client. This string is also *case sensitive*.
5. The session then prompts you to verify the new password. Enter the password again, and press <ENTER>.
6. Assuming the password was verified, the session then displays the Edit User menu (*see below*).

### 4) Edit User

1. Type **4** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to edit an existing user account. A sample session response is:

```
Select from the following list of enrolled users:
```

```
1) administrator
2) Fred
3) Betty
4) Bilbo
```

```
Select User:
```

2. Select the user account (1-x) that you want to edit, and press <ENTER> to display the Edit User Menu (described below).

Any changes made via the Edit User menu will affect the selected user account.

### Edit User Menu

The Edit User Menu is accessed whenever you enter the Add user, or Edit user selections from the Main Security Menu. The Edit User Menu is displayed as follows:

```
Please select from the following options:
```

```
1) Change User Password
2) Change Inherits From Group
3) Add Directory Association
4) Delete Directory Association
5) List Directory Associations
6) Change Access Rights
7) Display User Record Contents
```

(Cont.)

Or <ENTER> to return to previous menu

Edit User ->

Each selection (1-7) accesses the named option. Press <ENTER> by itself to exit the menu and return to the Main Security Menu.

The Edit User Menu options are described in the following table:

Edit User Menu	
Command	Description
1) Change User Password	This selection prompts you to enter the new password (twice) for the user. Once the new password is entered, the user must use the new password from that point forward.
2) Change Inherits From Group	This selection will display the current group the user is assigned to (if any). It will then display a list of current groups and prompts you to select the new group.
3) Add Directory Association	This selection will display any current Directory Associations assigned to the user, and then will prompt you for a path for the new Directory Association. Refer to <i>Directory Associations on page 28</i> for details.
4) Delete Directory Association	This selection will display any current Directory Associations assigned to the user, and then will prompt you to select the Directory Association you want to delete.
5) List Directory Associations	This selection will display any current Directory Associations assigned to the user.
6) Change Access Rights	This selection will display access the Access Rights Menu for the user, which allows you to set the rights assigned to the user.
7) Display User Record Contents	This selection will display the group the user is assigned to and the current Access Rights assigned to the user.

### Access Rights Menu

The Access Rights Menu is accessed whenever you select Change Access Rights from the Edit User Menu, or Change Access Rights from the Edit Group Menu. The Access Rights Menu is displayed as follows:

```
Select to change current access right
 1) Terminal (RS232) Access..... Disabled
 2) Admin Change Password Access..... Disabled
 3) FTP Access..... Disabled
 4) HTTP Access..... Enabled
 5) Telnet Access..... Enabled
 6) Security Configuration Access..... Enabled
Or <ENTER> to return to previous menu
Set Rights ->
```

The selection listed will display the current access rights. Each selection simply toggles the access right selected. Press <ENTER> to exit the menu and return to the previous menu.

The Access Rights Menu is described in the following table:



*The Master must be rebooted after changing the HTTP setting.*

Access Rights Menu	
Command	Description
1) Terminal (RS232) Access (Enable/Disable)	Enables/disables Terminal (RS232 Program port) Access. The account has sufficient access rights to login to a Terminal session if this option is enabled.
2) Admin Change Password Access (Enable/Disable)	Enables/disables Administrator Change Password Access. The account has sufficient access rights to change the administrator password if this option is enabled.
3) FTP Access (Enable/Disable)	Enables/disables FTP Access. The account has sufficient access rights to access the NetLinx Master's FTP Server if this option is enabled.
4) HTTP Access (Enable/Disable)	This selection enables/disables HTTP (Web Server) Access. The account has sufficient access rights to browse to the NetLinx Master with a Web Browser if this option is enabled.
5) Telnet Access (Enable/Disable)	This selection enables/disables Telnet Access. The account has sufficient access rights to login to a Telnet session if this option is enabled.
6) Security Configuration Access (Enable/Disable)	This selection enables/disables Security Configuration Access. The account has sufficient access rights to access the Main Security Menu if this option is enabled.

### 5) Delete user

1. Type **5** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to delete an existing user account. A sample session response is:

```
Select from the following list of enrolled users:
1) Fred
2) Betty
3) Bilbo
Select User ->
```

2. Select the user to delete and press <ENTER> to delete the user account, and return to the Security Setup menu.

### 6) Show the list of authorized users

1. Type **6** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to view a list of currently enrolled users.
2. Press <ENTER> to return to the Security Setup menu.

### 7) Add Group

1. Type **7** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to add a group account. A sample session response is:

```
The following groups are currently enrolled:
administrator
```

```
Enter name of new group:
```

2. Enter a name for the group. A group name is a valid character string (4 - 20 alpha-numeric characters) defining the group. This string is *case sensitive*, and each group name must be unique.
3. Press <ENTER> to display the following Edit Group menu:

## Edit Group Menu

```
Please select from the following options:
1) Add directory association
2) Delete directory association
3) List directory associations
4) Change Access rights
5) Display Access Rights
Or <ENTER> to return to previous menu.
Edit Group ->
```

### Edit Group Menu: Add directory association

1. At the Edit Group prompt, type **1** to add a new directory association. A sample session response is:

```
There are currently no directories associated with this account
New directory:
```

A Directory Association is a path that defines the directories and/or files that a particular user or group can access via the HTTP (Web) Server on the NetLinx Master. This character string can range from 1 to 128 alpha-numeric characters. This string is *case sensitive*. This is the path to the file or directory you want to grant access. Access is limited to the user (i.e. doc:user) directory of the master. All subdirectories of the user directory can be granted access.

A single '/' is sufficient to grant access to all files and directories in the user directory and it's sub-directory. The '\*' wildcard can also be added to enable access to all files. All entries should start with a '/'. Here are some examples of valid entries:

Path	Notes
/	Enables access to the user directory and all files and subdirectories in the user directory.
/*	Enables access to the user directory and all files and subdirectories in the user directory.
/user1	If user1 is a file in the user directory, only the file is granted access. If user1 is a subdirectory of the user directory, all files in the user1 and its sub-directories are granted access.
/user1/	user1 is a subdirectory of the user directory. All files in the user1 and its sub-directories are granted access.
/Room1/iWebControlPages/*	/Room1/iWebControlPages is a subdirectory and all files and its subdirectories are granted access.
/results.txt	results.txt is a file in the user directory and access is granted to that file.

By default, all accounts that enable HTTP Access are given a '/' Directory Association if no other Directory Association has been assigned to the account.

When you are prompted to enter the path for a Directory Association, the NetLinx Master will attempt to validate the path. If the directory or file is not valid (i.e. it does not exist at the time you entered the path), the NetLinx Master will ask you whether you were intending to grant access to a file or directory. From the answer, it will enter the appropriate Directory Association. The NetLinx Master will not create the path if it is not valid. That must be done via another means, most commonly by using an FTP client and connecting to the FTP server on the NetLinx Master.

**Edit Group menu: Delete directory association**

1. At the Edit Group prompt, type **2** to delete an existing directory association. A sample session response is:

```
Select a directory association from the following:
1) /directory1/*
2) /directory2/*
Select Directory ->
```

2. Select the directory association to be deleted, and press <ENTER> to delete the directory association, and return to the Edit Group menu.

**Edit Group menu: List directory associations**

1. At the Edit Group prompt, type **3** to list all existing directory associations. A sample session response is:

```
The following directory associations are enrolled:
/directory1/*
/directory2/*

Press <ENTER> key to continue
```

2. Press <ENTER> to return to the Edit Group menu.

**Edit Group menu: Change Access Rights**

1. At the Edit Group prompt, type **4** to change the current access rights for the selected group account. A sample session response is:

```
Select to change current access right:
1) Terminal (RS232) Access.....Disabled
2) Admin Change Password Access.....Disabled
3) FTP Access.....Disabled
4) HTTP Access.....Disabled
5) Telnet Access.....Disabled
6) Security Configuration Access.....Disabled
or <ENTER> to return to previous menu

Set Rights ->
```



*The Master must be rebooted after changing the HTTP setting.*

2. Each selection simply toggles the security setting selected. <ENTER> is entered by itself to exit the menu and return to the Main Security Menu.



**Edit Group menu: Display Access Rights**

1. At the Edit Group prompt, type **5** to view the current access rights for the selected group account. A sample session response is:

```
Terminal (RS232).....Disabled
Admin Password Change.....Disabled
FTP.....Disabled
HTTP.....Disabled
Telnet.....Disabled
Security Configuration.....Disabled
```

Press <ENTER> key to continue



*The Master must be rebooted after changing the HTTP setting.*

2. Press <ENTER> to return to the Edit Group menu.

**8) Edit Group**

1. Type **8** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to edit an existing group account. A sample session response is:

```
Select from the following list:
1) administrator
2) Group 1
3) Group 2
Select group ->
```

2. Select a group from the list of currently enrolled groups and press <ENTER> to open the Edit Group Menu. This is the same Edit Group Menu that was access via the Add Group option:

```
1) Add directory association
2) Delete directory association
3) List directory associations
4) Change Access rights
5) Display Access Rights
```

This menu is described on the previous pages (see *Edit Group Menu on page 35*).

**9) Delete Group**

1. Type **9** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to delete an existing group account. A sample session response is:

```
Select from the following list:
1) Group 1
2) Group 2
Select group ->
```

2. Select the group account to be deleted, and press <ENTER> to delete the group and return to the Security Setup menu.

### 10) Show List of Authorized Groups

1. Type **10** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to display a list of all authorized group accounts. A sample session response is:

```
The following groups are currently enrolled:  
administrator  
Group 1
```

```
Press <ENTER> key to continue
```

2. Press <ENTER> to return to the Security Setup Menu.

### 11) Set Telnet Timeout in seconds

1. Type **11** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to set the Telnet Timeout value, in seconds. A sample session response is:

```
Specify Telnet Timeout in seconds:
```

2. Enter the number of seconds before you want The Telnet session to timeout, and press <ENTER> to return to the Security Setup Menu.

### 12) Display Telnet Timeout in seconds

1. Type **12** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to view the current Telnet Timeout value (in seconds). A sample session response is:

```
Telnet Timeout is 10 seconds.
```

2. Press <ENTER> to return to the Security Setup Menu.

### 13) Make changes permanent by saving to flash

When changes are made to the security settings of the master, they are initially only changed in RAM and are not automatically saved permanently into flash. This selection saved the current security settings into flash. Also, if you attempt to exit the Main Security Menu and the security settings have changed but not made permanent, you will be prompted to save the settings at that time.

Type **13** and <ENTER> at the Security Setup prompt to (permanently) save all changes to flash.



NOTE

*Reboot the Master for the security configuration changes to take effect.*

## Main Security Menu

The Main Security menu is described below:

Main Security Menu	
Command	Description
1) Set system security options for NetLinx Master	This selection will bring up the Security Options Menu that allows you to change the security options for the NetLinx Master (refer to the <i>Security Options Menu</i> section on page 31 for details). These are "global" options that enable rights given to users and groups. For instance, if you want to disable Telnet security for all users, you would simply go to this menu and disable Telnet security for the entire master. This would allow any user, whether they have the rights to Telnet or not. These options can be thought of as options to turn on security for different features of the NetLinx Master.
2) Display system security options for NetLinx Master	This selection will display the current security options for the NetLinx Master.
3) Add user	This selection will prompt you for a user name and password for a user you would like to create. After the user is added, you will be taken to the Edit User Menu to setup the new users rights (see the <i>Edit User Menu</i> section on page 33 for details).
4) Edit user	This selection will prompt you select a user. Once you have selected the user you want to edit, it will take you to the Edit User Menu so you can edit the user's rights (see the <i>Edit User Menu</i> section on page 33 for details).
5) Delete user	This selection will prompt you select a user to delete.
6) Show the list of authorized users	This selection displays a list of users.
7) Add group	This selection will prompt you for a group name from a group you would like to create. After the group is added, you will be taken to the Edit Group Menu to setup the new users right (see the <i>Edit Group Menu</i> section on page 35 for details).
8) Edit group	This selection will prompt you select a group. Once you have selected the group you want to edit, it will take you to the Edit Group Menu so you can edit the group's rights (see the <i>Edit Group Menu</i> section on page 35 for details).
9) Delete group	This selection will prompt you select a group to delete. A group can only be deleted if there are no users assigned to that group.
10) Show list of authorized groups	This selection displays a list of groups.
11) Set Telnet Timeout in seconds	This selection allows you to set the time a telnet session waits for a user to login. When a Telnet client connects to the NetLinx Master, it is prompted for a user name. If the client does not enter a users name for the length of time set in this selection, the session will be closed by the NetLinx Master.
12) Display Telnet Timeout in seconds	This selection allows you to display the time a telnet session waits for a user to login.
13) Make changes permanent by saving to flash	When changes are made to the security settings of the master, they are initially only changed in RAM and are not automatically saved permanently into flash. This selection saved the current security settings into flash. Also, if you attempt to exit the Main Security Menu and the security settings have changed but not made permanent, you will be prompted to save the settings at that time.

Main Security Menu (Cont.)	
Command	Description
14) Reset Database	If a user has been given "administrator rights", this additional menu option is displayed. This selection will reset the security database to its Default Security Configuration settings, erasing all users and groups that were added. This is a permanent change and you will be asked to verify this before the database is reset.
15) Display Database	If a user has been given "administrator rights", this additional menu option is displayed. This selection will display the current security settings to the terminal (excluding user passwords).

## Default Security Configuration

By default, the NetLinx Master will create the following accounts, access rights, directory associations, and security options.

```
Account 1:          User Name: administrator
Password:          password
Group:             administrator
Rights:            All
Directory Association: /*
```

```
Account 2:          User Name: NetLinx
Password:          password
Group:             none
Rights:            FTP Access
Directory Association: none
```

```
Group 1:           Group: administrator
Rights:            All
Directory Association: /*
```

```
Security Options:  FTP Security Enabled
                  Admin Change Password Security Enabled
                  All other options disabled
```

- The "administrator" user account cannot be deleted or modified with the exception of its password. Only a user with "Change Admin Password Access" rights can change the administrator password.
- The "NetLinx " user account is created to be compatible with previous NetLinx Master firmware versions.
- The "administrator" group account cannot be deleted or modified.
- The FTP Security and Admin Change Password Security are always enabled and cannot be disabled.

## Help menu

Type **help** at the prompt in the Telnet session to display the following help topics:

Help Menu Options	
Command	Description
----- Help ----- <D:P:S>	(Extended diag messages are OFF) <D:P:S>: Device:Port:System. If omitted, assumes master.
? or Help	Displays this list.
DATE	Displays the current date.
DEVICE HOLDOFF ON OFF	Sets the master to holdoff devices (i.e. does not allow them to report ONLINE) until the NetLinx program has completed executing the DEFINE_START section.  If set to ON, any messages to devices in DEFINE_START will be lost, however, this prevents incoming messages being lost in the master upon startup. When DEVICE_HOLDOFF is ON, you must use ONLINE events to trigger device startup SEND_COMMANDS.  By default, DEVICE_HOLDOFF is OFF to maintain compatibility with Access systems where f devices are initialized in DEFINE_START.
DEVICE STATUS <D:P:S>	Provides information about the specified device.
DNS LIST <D:P:S>	Displays the DNS configuration of a device.
DISK FREE	Displays the amount of free space on the disk.
GET DEVICE HOLDOFF	Displays the state of the device holdoff setting in the master
GET IP <D:P:S>	Displays the IP configuration of a device.
HELP SECURITY	Displays security related commands.
IP STATUS	Provides information about NetLinx IP Connections.
MEM	Shows size of the largest block of available memory.
MSG ON OFF	Enables/Disables extended diagnostic messages.
OFF [D:P:S or NAME, CHAN]	Turns off the specified channel.
ON [D:P:S or NAME, CHAN]	Turns on the specified channel.
PASS [D:P:S or NAME]	Puts the Session in pass mode to the specified device. <ul style="list-style-type: none"> <li>• Mode is exited by ++ ESC ESC.</li> <li>• Display Format is set by ++ ESC n If n is A, format = ASCII If n is D, format = Decimal If n is H, format = Hex</li> </ul>
PING [ADDRESS]	Pings an address (IP or URL). Specify -a option for reverse lookup.
PROGRAM INFO	Displays a list of program modules loaded.
PULSE [D:P:S or NAME, CHAN]	Pulses the specified channel.
REBOOT <D:P:S>	Reboots the device.
RELEASE DHCP	Releases the current DHCP lease.
ROUTE MODE DIRECT NORMAL	Set the Master-Master route mode.
SEND_COMMAND D:P:S or NAME, COMMAND	Sends the specified command to the device. The Command uses NetLinx string syntax. <ul style="list-style-type: none"> <li>• Ex: send_command 1:1:1, "This is a test", 13, 10"</li> <li>• Ex: send_command RS232_1, "This is a test", 13, 10"</li> </ul>
SEND_STRING D:P:S or NAME, STRING	Sends the specified string to the device.
SET DATE	Set the current date.

Help Menu Options (Cont.)	
Command	Description
SET DNS <D:P:S>	Setup the DNS configuration of a device.
SET ICSP PORT	Sets the IP port listened to for ICSP connections.
SET ICSP TCP TIMEOUT	Sets the timeout period for ICSP and i!-WebControl TCP connections.
SET IP <D:P:S>	Setup the IP configuration of a device.
SET TELNET PORT	Sets the IP port listened to for telnet connections.
SET THRESHOLD	Sets the master's internal message thresholds.
SET TIME	Set the current time.
SET URL <D:P:S>	Setup the initiated connection list URLs of a device.
SHOW COMBINE	Displays a list of devices, levels, and channels that are currently combined.
SHOW DEVICE <D:P:S>	Displays a list of devices connected and attributes.
SHOW LOG <START>	Display the message log. <start> specifies message to begin the display. 'all' will display all messages.
SHOW NOTIFY	Display the Notify Device List (Master-Master).
SHOW REMOTE	Displays the Remote Device List (Master-Master).
SHOW ROUTE	Displays the Master's routing information.
SHOW SYSTEM <S>	Displays a list of devices in a system.
TCP LIST	Displays a list of active TCP connections.
TIME	Display the current time.
URL LIST <D:P:S>	Display the initiated connection list URLs of a device.

## Logging Into a Session

Until Telnet security is enabled, a session will begin with a welcome banner.

```
Welcome to NetLinx v2.10.80 Copyright AMX Corp. 1999-2002
>
```



NOTE

*The welcome banner is not displayed for Terminal sessions.*

When Telnet security is enabled (or Terminal security for a terminal session), the user will be prompted for a user name and password before they will be allowed to access any commands available from Telnet. No welcome banner will be displayed until a valid login is made. When the session is started, the user will see a login prompt as seen below:

```
Login:
```

The user (Login) name is case sensitive. The user name must be entered with the exact combination of upper and lower letters as was assigned to them by the security administrator. The user name must be at least 4 characters long and no more than 20 characters. Any combination of letters, numbers, or other characters may be used.

The user would enter their user name and then would be prompted for a password:

```
Login: User1
Password:
```

The password is case sensitive. The password must be entered with the exact combination of upper and lower letters as was assigned to them by the security administrator. The password must be at

least 4 characters long and no more than 20 characters. Any combination of letters, numbers, or other characters may be used.

After the password is entered, if the password is correct you will see a welcome banner as shown below:

```
Login: User1
Password: *****
Welcome to NetLinx v2.10.80 Copyright AMX Corp. 1999-2002
>
```

If the password is incorrect, the following will be displayed:

```
Login: User1
Password: *****
Login not authorized. Please try again.
```

After a delay, another login prompt will be displayed to allow the user to try again. If after 5 prompts, the login is not done correctly the following will be displayed and the connection closed:

```
Login not allowed. Goodbye!
```

If a user opens a connection but does not enter a user name or password (i.e. they just sit at a login prompt), the connection will be closed after 1 minute.

## Logout

The logout command will log the user out of the current secure telnet session. For a Telnet connection, the session will be closed and the connection between the Telnet client and the NetLinx Master will be dropped. For a Terminal session, the user will be logged out and to access Terminal commands again the user will first have to login.

### *Help Security*

The help security command will display the security menu as shown previously.

### *Setup Security*

The security command displays a series of menus that allow the security administrator to create and edit users, create and edit groups, and setup directory associations for the Web Server. A user must be given rights to access this command. Any user that does not have rights to Security Configuration will see the following message when trying to access the setup security command:

```
>setup security
You are not authorized to access security commands
```

If a user is authorized, or if Security Configuration security is not enabled, the Main Security Menu will be displayed.



**AMX reserves the right to alter specifications without notice at any time.**

ARGENTINA • AUSTRALIA • BELGIUM • BRAZIL • CANADA • CHINA • ENGLAND • FRANCE • GERMANY • GREECE • HONG KONG • INDIA • INDONESIA • ITALY • JAPAN  
LEBANON • MALAYSIA • MEXICO • NETHERLANDS • NEW ZEALAND • PHILIPPINES • PORTUGAL • RUSSIA • SINGAPORE • SPAIN • SWITZERLAND • THAILAND • TURKEY • USA  
ATLANTA • BOSTON • CHICAGO • CLEVELAND • DALLAS • DENVER • INDIANAPOLIS • LOS ANGELES • MINNEAPOLIS • PHILADELPHIA • PHOENIX • PORTLAND • SPOKANE • TAMPA  
3000 RESEARCH DRIVE, RICHARDSON, TX 75082 USA • 800.222.0913 • 469.624.8000 • 469-624-7153 fax • 800.932.6993 technical support • [www.amx.com](http://www.amx.com)

060-004-2564 6/03 ©2003 AMX Corporation. All rights reserved. AMX, the AMX logo, the building icon, the home icon, and the light bulb icon are all trademarks of AMX Corporation. AMX reserves the right to alter specifications without notice at any time. \*In Canada doing business as Panja Inc.



## Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>