

Installation and Configuration Guide



Trademark Notices

Comtrol, NS-Link, and DeviceMaster Industrial Gateway are trademarks of Comtrol Corporation.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

HyperTerminal is a registered trademark of Hilgraeve, Inc.

Portions of SocketServer are copyrighted by GoAhead Software, Inc. Copyright © 2001. GoAhead Software, Inc. All Rights Reserved.

Other product names mentioned herein may be trademarks and/or registered trademarks of their respective owners.

Sixth Edition, November 14, 2018 Copyright © 2001 - 2018. Comtrol Corporation. All Rights Reserved.

Comtrol Corporation makes no representations or warranties with regard to the contents of this document or to the suitability of the Comtrol product for any particular purpose. Specifications subject to change without notice. Some software or features may not be available at the time of publication. Contact your reseller for current product information.

Table of Contents

Introduction	9
Supported DeviceMaster Models	9
DeviceMaster Port Usage	9
Installation Overview	
NS-Link COM Port Driver Installation Overview	
NS-Link tty Port Installation Overview	
TCP/IP Socket Port Installation Overview	
Locating Software and Documentation	
Connectivity Requirements	12
Hardware Installation	
Installation Overview	
Product Name Change Notification	
1-Port - Panel Mount (DB9) Installation	
DM-2201: 1-Port DIN Rail (Terminal Block) Installation	
DM-2101: 1-Port DIN Rail (DB9) Installation	
DM-2202 and DM-2402: 2-Port DIN Rail (Terminal Block) Installation	
DM-2102 and DM-2302: 2-Port DIN Rail (DB9) Installation	
DM-2304: 4-Port DIN Rail (DB9) Installation	22
4-Port and 8-Port Installation	23
16-Port (DeviceMaster RTS - External Power Supply) Installation	25
16-Port (DeviceMaster PRO) Installation	
16/32-Port Rack Mount Models (Internal Power Supply) Installation	
Adding a Unit to an Existing Installation	
Replacing Hardware	
Initial Configuration	
PortVision DX Overview	
PortVision DX Requirements	
Configuring Security Settings and PortVision DX	
Installing PortVision DX	
Configuring the Network Settings	
Checking the SocketServer Version	
Uploading SocketServer with PortVision DX	
Customizing PortVision DX	
Accessing DeviceMaster Documentation from PortVision DX	
How to Download Documentation	
How to Open Previously Downloaded Documents	

	4
Overview	
Before Installing the NS-Link Driver	
Linux Installations	
Windows Installations	
Supported Operating Systems	
Installation Overview for Windows	
NS-Link for Windows Installation	
Configuring the NS-Link Driver for Windows	
Configuring COM Port Properties for Windows	
Enabling Secure Data Mode	5
ocket Port Configuration	6
SocketServer Overview	6
Web Page Help System	
SocketServer Architecture	
Accessing Socket Configuration	
Web Browser	
PortVision DX	
SocketServer Versions	
eviceMaster Security Understanding Security Methods and Terminology	6
Understanding Security Methods and Terminology TCP and UDP Socket Ports Used by the DeviceMaster	
Understanding Security Methods and Terminology TCP and UDP Socket Ports Used by the DeviceMaster DeviceMaster Security Features	
Understanding Security Methods and Terminology TCP and UDP Socket Ports Used by the DeviceMaster DeviceMaster Security Features Security Modes	
Understanding Security Methods and Terminology TCP and UDP Socket Ports Used by the DeviceMaster DeviceMaster Security Features Security Modes Secure Data Mode and Secure Config Mode Comparison	
Understanding Security Methods and Terminology TCP and UDP Socket Ports Used by the DeviceMaster DeviceMaster Security Features Security Modes Secure Data Mode and Secure Config Mode Comparison Security Comparison	
Understanding Security Methods and Terminology TCP and UDP Socket Ports Used by the DeviceMaster DeviceMaster Security Features Security Modes Secure Data Mode and Secure Config Mode Comparison Security Comparison SSH Server	
Understanding Security Methods and Terminology TCP and UDP Socket Ports Used by the DeviceMaster DeviceMaster Security Features Security Modes Secure Data Mode and Secure Config Mode Comparison Security Comparison SSH Server SSL Overview	
Understanding Security Methods and Terminology TCP and UDP Socket Ports Used by the DeviceMaster DeviceMaster Security Features Security Modes Secure Data Mode and Secure Config Mode Comparison Security Comparison SSH Server SSL Overview SSL Authentication	
Understanding Security Methods and Terminology TCP and UDP Socket Ports Used by the DeviceMaster DeviceMaster Security Features Security Modes Secure Data Mode and Secure Config Mode Comparison Security Comparison SSH Server SSL Overview SSL Authentication Server Authentication	
Understanding Security Methods and Terminology TCP and UDP Socket Ports Used by the DeviceMaster DeviceMaster Security Features Security Modes Secure Data Mode and Secure Config Mode Comparison Security Comparison SSH Server SSL Overview SSL Authentication Server Authentication <i>Client Authentication</i>	
Understanding Security Methods and Terminology TCP and UDP Socket Ports Used by the DeviceMaster DeviceMaster Security Features Security Modes Secure Data Mode and Secure Config Mode Comparison Security Comparison SSH Server SSL Overview SSL Authentication Server Authentication Client Authentication Certificates and Keys	
Understanding Security Methods and Terminology	
Understanding Security Methods and Terminology	
Understanding Security Methods and Terminology	6 7 <td< td=""></td<>
Understanding Security Methods and Terminology	6
Understanding Security Methods and Terminology	6 7 7 7 7 7 7 7 7 7 7 7 7 7
Understanding Security Methods and Terminology	6 7 7 7 7 7 7 7 7 7 7 7 7 7
Understanding Security Methods and Terminology	6 7 7 7 7 7 7 7 7 7 7 7 7 7
Understanding Security Methods and Terminology	6
Understanding Security Methods and Terminology TCP and UDP Socket Ports Used by the DeviceMaster DeviceMaster Security Features Security Modes Secure Data Mode and Secure Config Mode Comparison Security Comparison SSH Server SSL Overview SSL Overview SSL Authentication <i>Client Authentication</i> <i>Client Authentication</i> <i>Certificates and Keys</i> . SSL Performance SSL Cipher Suites DeviceMaster Supported Cipher Suites SSL Resources Configure/Enable Security Features Overview Example 1 Example 3	6
Understanding Security Methods and Terminology TCP and UDP Socket Ports Used by the DeviceMaster DeviceMaster Security Features Security Modes Secure Data Mode and Secure Config Mode Comparison Security Comparison SSH Server SSL Overview SSL Authentication <i>Client Authentication</i> <i>Client Authentication</i> <i>Certificates and Keys</i> . SSL Performance SSL Cipher Suites DeviceMaster Supported Cipher Suites SSL Resources Configure/Enable Security Features Overview Example 1. Example 2. Example 3. Key and Certificate Management	6 7 7 7 7 7 7 7 7 7 7 7 7 7

Connecting Serial Devices	
DB9 Connectors	
DB9 Null-Modem Cables (RS-232)	
DB9 Null-Modem Cables (RS-422)	
DB9 Straight-Through Cables (RS-232/485)	
DB9 Loopback Plugs	
Connecting DB9 Serial Devices	
RJ45 Connectors	
RJ45 Null-Modem Cables (RS-232)	
RJ45 Null-Modem Cables (RS-422)	
RJ45 Straight-Through Cables (RS-232/485)	
RJ45 Loopback Plugs	
RJ45 RS-485 Test Cable	
Connecting RJ45 Devices	
Four Screw Terminals (DM-2202)	
Serial Terminal (4) Connectors	
Serial Terminal (4) Null-Modem Cables (RS-232)	
Serial Terminal (4) Null-Modem Cables (RS-422)	
Serial Terminal (4) Straight-Through Cables (RS-232/485)	
Serial Terminal (4) Loopback Signals	
Connecting Serial Devices	
Eight Screw Terminals (DM-2402)	
Screw Terminal (8) Connectors	
Screw Terminal (8) Null-Modem Cables (RS-232)	
Screw Terminal (8) Null-Modem Cables (RS-422)	
Screw Terminal (8) Straight-Through Cables (RS-232/485)	
Screw Terminal (8) Loopback Signals	
Connecting Serial Devices	
Nine Screw Terminals (DM-2201)	
Screw Terminal Connectors (9)	
Screw Terminal (9) Null-Modem RS-232 Cables	
Screw Terminal (9) Null-Modem RS-422 Cables	
Screw Terminal (9) RS-232/485 Straight-Through Cables	
Screw Terminal (9) Loopback Signals	
Connecting Serial Devices	
Managing the DeviceMaster	
Rebooting the DeviceMaster	
Uploading SocketServer to Multiple DeviceMasters	
Configuring Multiple DeviceMasters Network Addresses	
Adding a New Device in PortVision DX	
Remote Using the IP Address	
Local Using the IP Address or MAC Address	
Using the SocketServer Configuration Files	
PortVision DX - Saving a SocketServer Configuration File	
PortVision DX - Loading a SocketServer Configuration File	
SocketServer - Saving Configuration Files	
SocketServer - Loading Configuration Files	

Using Driver Configuration Files	
Saving Driver Configuration Files	110
Saving Device-Level Configuration	
Saving Port-Level Configuration	
Loading Driver Configuration Files	
Loading Device Configuration	
Loading Port Configuration Changing the Bootloader Timeout	
PortVision DX - Changing Bootloader Timeout	
SocketServer - Changing Bootloader Timeout	
Managing Bootloader	
Checking the Bootloader Version	116
Uploading Bootloader	
Checking the NS-Link Version	
Restoring Factory Defaults (Specific Models)	
Restoring Serial Port Settings	
NS-Link COM Port	
Socket Port	
Accessing SocketServer Commands in Telnet/SSH Sessions (PortVision DX)	
Telnet Session	
SSH Session	
Accessing RedBoot Commands in Telnet/SSH Sessions (PortVision DX)	
RedBoot Procedures Accessing RedBoot Overview	
Establishing a Serial Connection	
Establishing a Telnet Connection	
Determining the Network Settings	
Configuring the Network Settings	
Changing the Bootloader Timeout	
Determining the Bootloader Version	
Resetting the DeviceMaster	
Configuring Passwords	
RedBoot Command Overview	
External Power Supply Specifications	139
1-Port 5VDC Panel Mount Power Supply	
1-Port Panel Mount 5-30VDC Power Supply	
DM-2101 and DM-2201: 1-Port DIN Rail Power Supply	
DM-2101 and DM-2201. 1-1 of t DH (Ran 1 ower Supply DM-2202 and DM-2402: 2-Port (Serial Terminals) Power Supply	
DM-2202 and DM-2402. 2-1 oft (Serial Terminals) Tower Suppry DM-2102 and DM-2302: 2-Port DB9 Power Supply (Bottom)	
DM-2102 and DM-2302: 2-Port DB9 Power Supply (Bottom) DM-2102 and DM-2302: 2-Port DB9 Power Supply (Top)	
DM-2102 and DM-2502. 2-1 of t DB5 1 ower Supply (10p) DM-2304: 4-Port DIN Rail Models Power Supply	
4-Port Panel Mount Power Supply	
8-Port Power Supply	
16-Port Power Supplies	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	

Troubleshooting and Technical Support	
Troubleshooting Checklist	
General Troubleshooting	
Testing Ports Using Port Monitor (PMon2)	
Overview	
Testing Comtrol COM Ports	
Testing Ports Using Test Terminal	
Overview	
Opening Ports	
Sending and Receiving Test Data (RS-232/422/485: 4-Wire)	
Loopback Test (RS-232)	
Sending and Receiving Data (RS-485: 2-Wire)	
Socket Mode Serial Port Testing	
Daisy-Chaining DeviceMaster 4/8/16-Port Units	
DeviceMaster LEDs	
TX/RX LEDs	
Network and Device LEDs	
Removing DeviceMaster Security Features	
Serial Connection Method	
Returning the DeviceMaster to Factory Defaults	
Clearing the Flash	
Clearing EEPROM	
Telnet Access	
Serial Port Access	
Web Server Access Technical Support	
	•••••••••• L / T

Introduction

This section discusses the following topics:

- <u>Supported DeviceMaster Models</u> on Page 9
- <u>DeviceMaster Port Usage</u> (below)
- *Installation Overview* on Page 10
 - <u>NS-Link COM Port Driver Installation Overview</u> on Page 10
 - <u>NS-Link tty Port Installation Overview</u> on Page 11
 - <u>TCP/IP Socket Port Installation Overview</u> on Page 11
- <u>Locating Software and Documentation</u> on Page 11
- <u>Connectivity Requirements</u> on Page 12

Supported DeviceMaster Models

This *Installation and Configuration Guide* supports the DeviceMaster platform, which includes the following models:

- DM-2000 series
- DeviceMaster PRO
- DeviceMaster RTS
- DeviceMaster Serial Hub

The *Guide* refers to DeviceMaster unless there is model-specific information. Download links in this *Guide* typically point to an **RTS** subdirectory, where the file resides that supports all DeviceMaster models.

Note: The DeviceMaster LT provides different RJ45 pin outs and is not discussed in this guide. Refer to the <u>DeviceMaster LT User Guide</u> for product-specific information.

DeviceMaster Port Usage

DeviceMaster serial ports can be configured for many environments, which include the following:

- *COM port* (or secure COM ports) when the NS-Link driver for Windows is installed
- *tty ports* when the NS-Link driver for Linux is installed
- Socket ports when SocketServer or the NS-Link web page is configured accordingly

Installation Overview

DeviceMaster installation and configuration follows these steps:

1. Hardware installation.

Power up the DeviceMaster. Technical Support suggests installing one DeviceMaster at a time to avoid configuration problems using <u>Hardware Installation</u> on Page 13.

2. Install PortVision DX.

Note: PortVision DX replaces PortVision Plus. PortVision Plus does not support operating systems above Windows 7 and SocketServer versions above 9.00.

Comtrol recommends connecting the DeviceMaster to a PC or laptop running Windows and that you install PortVision DX for easy IP address configuration and firmware updates. See <u>PortVision DX</u> <u>Requirements</u> on Page 34 and refer to <u>Installing PortVision DX</u> on Page 35 to install PortVision DX.

3. Program the IP address.

See <u>Configuring the Network Settings</u> on Page 38 for detailed configuration procedures.

4. If necessary, update SocketServer.

Note: Technical Supports recommends that you update to the latest version of SocketServer before installing any NS-Link device driver or configuring socket ports.

- a. Check the SocketServer version using <u>Checking the SocketServer Version</u> on Page 41 to determine the version on the DeviceMaster.
- b. If necessary, update SocketServer. See <u>Uploading SocketServer with PortVision DX</u> on Page 42.

Note: In rare cases, you may need to update Bootloader to support a new feature. A notice will posted with SocketServer or the NS-Link device driver if this is the case.

- 5. Go to the appropriate overview or overviews for your installation:
 - NS-Link COM ports (or secure COM ports) <u>NS-Link COM Port Driver Installation Overview</u> on Page 10
 - NS-Link tty ports <u>NS-Link tty Port Installation Overview</u> on Page 11
 - TCP/IP socket ports <u>TCP/IP Socket Port Installation Overview</u> on Page 11

NS-Link COM Port Driver Installation Overview

Use the following overview, which are discussed in detail in the subsequent sections, to install and configure the DeviceMaster to run the NS-Link device driver for <u>Windows</u> operating systems..

- 1. After connecting the DeviceMaster, programming the IP address with PortVision DX, and uploading the latest version of SocketServer, you are ready to install the driver.
- 2. Install the NS-Link device driver.

See <u>Windows Installations</u> on Page 49 for an installation overview of the NS-Link driver for Windows operating systems.

For detailed installation and configuration information, download the *DeviceMaster NS-Link Device Driver User Guide* from the download site at: <u>http://downloads.comtrol.com/dev_mstr/rts/drivers/win7/</u><u>sw_doc/</u>.

Note: Although the download link displays win7 in the path, the driver supports multiple <u>Windows</u> operating systems (Page 34).

- 3. Configure the COM ports using the *DeviceMaster Drivers Management Console*. See <u>Configuring the NS-</u> <u>Link Driver for Windows</u> on Page 54, which provides an overview of COM port configuration.
- 4. Configure device properties, you can refer to <u>Configuring COM Port Properties for Windows</u> on Page 58.
- 5. Optionally, you may need to configure one or more ports for socket mode. See <u>Socket Port Configuration</u> on Page 61 for information about configuring socket ports using the *Server Configuration* web page.
- 6. Connect the serial devices to the DeviceMaster. Refer to <u>Connecting Serial Devices</u> on Page 87 for cabling and connector information.

NS-Link tty Port Installation Overview

Use the following steps, which are discussed in detail in the subsequent sections, to install and configure the DeviceMaster to run the NS-Link device driver for Linux operating systems.

- 1. After connecting the DeviceMaster, programming the IP address, and uploading the latest version of SocketServer, you are ready to install the driver.
- Locate and unpackage the driver assembly: <u>http://downloads.comtrol.com/dev_mstr/rts/drivers/linux/</u>. Refer to the **readme** file packaged with the Linux driver assembly for driver installation and configuration procedures for the tty port.
- 3. Optionally, you may need to configure one or more ports for socket mode. See <u>Socket Port Configuration</u> on Page 61 for information about configuring socket ports using the web interface (SocketServer/NS-Link).
- 4. Connect the serial devices to the DeviceMaster. Refer to <u>Connecting Serial Devices</u> on Page 87 for cabling and connector information.

TCP/IP Socket Port Installation Overview

Use the following steps, which are discussed in detail in the subsequent sections, to configure DeviceMaster socket ports.

- 1. After connecting the DeviceMaster, programming the IP address, and uploading the latest version of SocketServer, you are ready to configure socket port or serial tunneling.
- 2. Configure the serial socket ports using the PortVision DX property pages or enter the IP address in a web browser and use the SocketServer web pages.

You can refer to the SocketServer help system or <u>Socket Port Configuration</u> on Page 61 for information for configuration procedures.

3. Connect the serial devices to the DeviceMaster. Refer to <u>Connecting Serial Devices</u> on Page 87 for cabling and connector information.

Locating Software and Documentation

You can access the appropriate software assembly, PortVision DX, and DeviceMaster documentation from the Comtrol download site using any of these methods:

- PortVision DX features a **Documentation** option that you can use to download and later, access documentation from within PortVision DX. See <u>Accessing DeviceMaster Documentation from PortVision</u> <u>DX</u> on Page 44 for more information.
- Check for and download the latest files using the links in the following table.

If you are not sure what files are required for your installation, each <u>Installation Overview</u> subsection also provides links to the required files in this *Guide*.

Software		Description/Documentation	File
Configuration Application	PortVision DX	Install on a <u>Windows</u> host to configure the IP address and upload SocketServer on the DeviceMaster.	
SocketServer	SocketServer	This is the firmware that comes pre-installed on your DeviceMaster platform. You may need to upload the latest version of SocketServer before installing and configuring drivers or configuring sockets.	

Software		Description/Documentation	File
Device Driver	Linux	Install if you want tty ports. Refer to the Readme file compressed in the Linux driver assembly for driver configuration procedures.	
evice	Windows Server 2008 R2 through Windows 10	Install if you want COM ports. Refer to the <u>DeviceMaster Device Driver (NS-Link)</u>	
ď	10	<u>User Guide</u> . for detailed information.	
ader		The operating system that runs on the DeviceMaster hardware during the power on phase, which then loads SocketServer.	-
Bootloader	Bootloader	Only update the Bootloader on your DeviceMaster if advised by Technical Support or the download site when checking for the latest SocketServer or device driver version.	
This Guide	Any	You can check for the latest version of this <i>Installation</i> and <i>Configuration Guide</i> .	

Connectivity Requirements

An Ethernet connection: either to an Ethernet hub, switch, or router; or to a Network Interface Card (NIC) in the host system using a standard Ethernet cable.

Product Type	Connected to	Connector Name	
DeviceMaster RTS 1-port panel mount	Hub, switch, router, or NIC	10/100 ETHERNET	
DM-2101 and DM-2201 (1-port DIN Rail)	Hub, switch, router, or NIC	10/100	
DM-2201 and DM-2302	NIC	10/100	
(Formerly named the DeviceMaster RTS 2-port 1E models)	Hub, switch, or router	- 10/100	
DM-2202 and DM-2402	NIC	10/100 1E/2E	
(Formerly named the DeviceMaster RTS 2-port 2E models)	Hub, switch, or router	- 10/100 1E/2E	
DeviceMaster RTS 4-port 2E panel mount	NIC	10/100 1E/2E	
Devicemaster KTS 4-port ZE panel mount	Hub, switch, or router	10/100 IE/2E	
DM-2304 (4-port DIN Rail)	Hub, switch, router, or NIC	E1/E2	
DeviceMaster RTS 4/8/16-port (<i>external</i> power supply)	NIC	DOWN	
Devicemaster 1(15 4/0/10-poir (externat power suppry)	Hub, switch, or router	UP	
DeviceMaster RTS 16/32RM (internal power supply)	Hub, switch, router, or NIC	10/100 NETWORK	
DeviceMaster PRO 8/16-port	NIC	DOWN	
Devicemaster 1 no 6/10-port	Hub, switch, or router	UP	
DeviceMaster Serial Hub 8-port	NIC	DOWN	
Devicestaster bertai frub o-port	Hub, switch, or router	UP	
DeviceMaster Serial Hub 16-port	Hub, switch, router, or NIC	10/100 NETWORK	

Hardware Installation

Installation Overview

Use the links below to locate installation procedures for the following models:

DeviceMaster RTS			
1-Port	DB9 serial port - panel mount	<u>1-Port - Panel Mount (DB9) Installation</u> on Page 14	
1-Port	DM-2201 Screw terminal serial port - DIN rail	DM-2201: 1-Port DIN Rail (Terminal Block) Installation on Page 16	
1-Port	DM-2101 DB9 serial port - DIN rail	DM-2101: 1-Port DIN Rail (DB9) Installation on Page 17	
2-Ports	DM-2202 and DM-2402 Screw terminal serial ports - DIN rail	<u>DM-2202 and DM-2402: 2-Port DIN Rail</u> (<u>Terminal Block) Installation</u> on Page 18	
2-Ports	DM-2102 and DM-2302 DB9 serial ports - DIN rail	<u>DM-2102 and DM-2302: 2-Port DIN Rail</u> (<u>DB9) Installation</u> on Page 20	
4-Ports	DM-2304 DB9 serial ports - DIN rail	DM-2304: 4-Port DIN Rail (DB9) Installation on Page 22	
4† or 8†-Ports	DB9 serial ports with dual Ethernet ports	<u>4-Port and 8-Port Installation</u> on Page 23	
16-Ports	RJ45 serial ports with dual Ethernet ports	<u>16-Port (DeviceMaster RTS - External Power</u> <u>Supply) Installation</u> on Page 25	
16 or 32-Ports	RJ45 serial ports with a single Ethernet port	<u>16/32-Port Rack Mount Models (Internal</u> <u>Power Supply) Installation</u> on Page 29	
	DeviceMaster H	PRO	
8†-Ports	DB9 serial ports with dual Ethernet ports	<u>4-Port and 8-Port Installation</u> on Page 23	
16-Ports	RJ45 serial ports with dual Ethernet ports	<u>16-Port (DeviceMaster PRO) Installation</u> on Page 27	
	DeviceMaster Serial Hub		
8-Ports	DB9 serial ports with dual Ethernet ports	<u>4-Port and 8-Port Installation</u> on Page 23	
16-Ports	DB9 serial ports with a single Ethernet port	<u>16/32-Port Rack Mount Models (Internal</u> <u>Power Supply) Installation</u> on Page 29	

† The DeviceMaster RTS 4 and 8-port models may also include DB9 to RJ45 adapters.

Note: The DeviceMaster LT provides different RJ45 pin outs and is not discussed in this guide, refer to the <u>DeviceMaster LT User Guide</u>.

Product Name Change Notification

Comtrol has implemented a product name change for our DeviceMaster 2-port DIN rail models to align with our new 1-port and 4-port DIN rail model names.

Old Name/Description	New Model Name	Part Number
DeviceMaster RTS 2-Port 1E	DeviceMaster DM-2202	99480-0
DeviceMaster RTS 2-Port 1E DB9	DeviceMaster DM-2102	99550-0
DeviceMaster RTS 2-Port 2E	DeviceMaster DM-2402	99481-7
DeviceMaster RTS 2-Port 2E DB9	DeviceMaster DM- 2302	99560-9

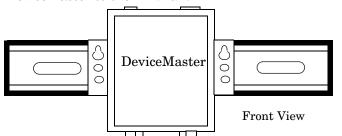
1-Port - Panel Mount (DB9) Installation

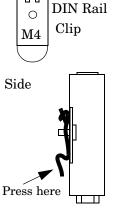
Use the following procedure to install the DeviceMaster 1-Port (panel mount).

- 1. Place the DeviceMaster 1-Port on a stable surface and skip to <u>Step 2</u> or optionally mount the DeviceMaster using the mounting flanges or DIN rail adapters.
 - a. Pick up the DeviceMaster so that the front of the device is facing you.
 - b. Pick up a DIN rail clip. (The three tines should be on top and the M4 label should face you.)
 - c. Slide the DIN rail clip behind the DeviceMaster and line it up with one of the screw holes on the DeviceMaster.
 - d. Insert the M4 screw into the hole and tighten with a Phillips screwdriver.
 - e. Repeat <u>Steps b</u> through d with the second DIN rail clip. Make sure the screws on both DIN rail clips line up.

Note: If you need to remove the DeviceMaster from the DIN rail, exert pressure on the backside of the tabs at the bottom of both DIN rail clips.

f. Attach the DeviceMaster to the DIN rail.





Note: Do not connect multiple units until you have changed the default IP address, see <u>Initial Configuration</u> on Page 33.

2. Connect the DeviceMaster port labeled 10/100 ETHERNET to the same Ethernet network segment as the host PC using a standard network cable.

3. Apply power to the DeviceMaster using the appropriate procedure for your power supply. *Note:* The supported input voltage (5VDC or 5-30VDC) is printed on the DeviceMaster.

5VDC Power Supply (Barrel Connector)

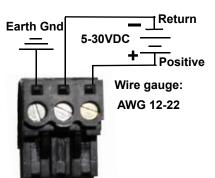
- Connect the 5VDC power supply to the DeviceMaster and to a power outlet.
- Go to <u>Step 4</u> to verify that the DeviceMaster is functioning properly.

5-30VDC with Screw Terminal Power Connector

Use the following procedure power on this model.

Observe proper ESD techniques when connecting and disconnecting the DeviceMaster.

- Insert the earth ground wire into the earth ground screw terminal.
- Insert the DC positive wire into the positive screw terminal and the DC return wire into the return screw terminal.
 Refer to <u>1-Port Panel Mount 5-30VDC Power Supply</u> on Page 140 for detailed power requirements.
- Use a small flat head screw to lock the wires into place.
- Verify that each wire has been tightened securely.



- Plug the screw terminal power connector into the DeviceMaster.
 Note: Align the plug properly. The scalloped side of the screw terminal power connector should be aligned with the scalloped side of the power jack on the unit.
- Connect the power supply to a power source.
- Go to <u>Step 4</u> to verify that the DeviceMaster is functioning properly.
- 4. Verify that the **Status** LED has completed the boot cycle and network connection for the DeviceMaster is functioning properly using the table below.

1-Port Panel Mount LED Descriptions	
Status	The amber Status LED on the device is lit, indicating you have power and it has completed the boot cycle.
	Note: The Status LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.
Link/Act	If the red Link/Act LED is lit, it indicates a working Ethernet connection.
Duplex	If the red Duplex LED is lit, it indicates full-duplex activity.
100	If the red 100 LED is lit, it indicates a working 100 MB Ethernet connection (100 MB network, only). If the LED is not lit, it indicates a 10 MB Ethernet connection.
Note: For	r additional LED information, go to the <u>Status LED table</u> on Page 148.



Do not connect RS-422/485 devices until the IP address is configured and an appropriate port interface type has been configured. The default port setting is RS-232.

requirements.

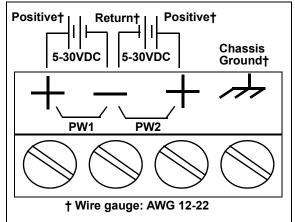
DM-2201: 1-Port DIN Rail (Terminal Block) Installation

Use the following procedure to install DM-2201. See <u>DM-2101: 1-Port DIN Rail (DB9) Installation</u> on Page 17 if the DeviceMaster has DB9 serial connectors.

- 1. Attach the DM-2201 1-Port to the DIN rail adapter.
- 2. Connect the power supply and apply power to the DM-2201 using the power supply specifications on the product label and the following information.

Observe proper ESD techniques when connecting and disconnecting the DeviceMaster. Caution

- a. If the DIN rail is not connected to earth ground, insert the earth ground wire into the chassis ground screw terminal.
- *Note:* The chassis ground connection is made only if the DIN rail is NOT connected to earth ground.
- b. Insert the DC positive wire into the + screw terminal and the DC return wire into the screw terminal.
 Refer to <u>DM-2101 and DM-2201: 1-Port DIN Rail</u> <u>Power Supply</u> on Page 140 for detailed power
- c. Use a small flat head screw driver to lock the wires into place.
- d. Verify that each wire has been tightened securely.
- e. Connect a UL Listed power supply and UL Listed power cord to a power source to apply power.
- **Note:** Do not connect multiple units until you have changed the default IP address, see <u>Initial Configuration</u> on Page 33.



- 3. Connect the **10/100 port** to the same Ethernet network segment as the host PC using a standard network cable.
- 4. Verify that the **Status** LED has completed the boot cycle and network connection for the DM-2201 is functioning using the following table.

	DM-2201 LED Descriptions	
	The STATUS LED on the device is lit, indicating you have power and it has completed the boot cycle.	
STATUS	Note: The Status LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.	
LINK	If the LINK (green) LED is lit, it indicates a working Ethernet connection.	
ACT	ACT If the ACT (yellow) LED flashes, it indicates network activity.	
Note: For	Note: For additional LED information, go to the <u>Status LED table</u> on Page 148.	



Do not connect RS-422/485 devices until the IP address is configured and an appropriate port interface type has been configured. The default port setting is RS-232.

5. Go to *Initial Configuration* on Page 33 to configure the DeviceMaster for use.

DM-2101: 1-Port DIN Rail (DB9) Installation

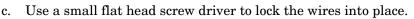
Use the following procedure to install a DM-2101.

- 1. Attach the DM-2101 to the DIN rail adapter.
- 2. Connect the power supply and apply power to the DM-2101 using the power supply specifications on the product label and the following information.

Observe proper ESD techniques when connecting and disconnecting the DeviceMaster.

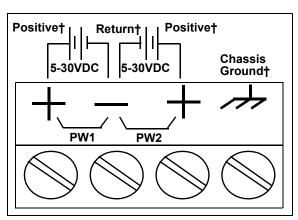
- a. If the DIN rail is not connected to earth ground, insert the earth ground wire into the chassis ground screw terminal.
- **Note:** The chassis ground connection is made only if the DIN rail is NOT connected to earth ground.
- b. Insert the DC positive wire into one of the + screw terminals and the DC return wire into the screw terminal.
 - A second redundant power supply can be connected to the unit by inserting the DC positive wire into the other + screw terminal and the DC return wire into the - screw terminal.
 - The DM-2101 continues to operate if one of the two connected power supplies should fail.

Refer to <u>DM-2101 and DM-2201: 1-Port DIN Rail</u> <u>Power Supply</u> on Page 140 for detailed power requirements.



- d. Verify that each wire has been tightened securely.
- e. Connect a UL Listed power supply and UL Listed power cord to a power source to apply power.
- **Note:** Do not connect multiple units until you have changed the default IP address, see <u>Initial Configuration</u> on Page 33.
- 3. Connect the **10/100** port to the same Ethernet network segment as the host PC using a standard Ethernet cable.
- 4. Verify that the **Status** LED has completed the boot cycle and network connection for the DM-2101 is functioning properly using the following table.

DM-2101 LED Descriptions			
STATUS	The STATUS LED on the device is lit, indicating you have power and it has completed the boot cycle.		
	Note: The Status LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.		
LINK	K If the LINK (green) LED is lit, it indicates a working Ethernet connection.		
ACT	ACT If the ACT (yellow) LED flashes, it indicates network activity.		
Note: For additional LED information, go to the <u>Status LED table</u> on Page 148.			



† Wire gauge: AWG 12-22

Do not connect RS-422/485 devices until the IP address is configured and an appropriate port interface type has been configured. The default port setting is RS-232.

5. Go to *Initial Configuration* on Page 33 to configure the DM-2101 for use.

DM-2202 and DM-2402: 2-Port DIN Rail (Terminal Block) Installation

Use the following procedure to install the DM-2202 and DM-2402. See <u>DM-2102 and DM-2302: 2-Port DIN</u> <u>Rail (DB9) Installation</u> on Page 20 if the DeviceMaster has DB9 serial connectors.

- 1. Attach the DeviceMaster to the DIN rail adapter.
- 2. Connect the power supply and apply power to the DeviceMaster using the power supply specifications on the product label and the following information.



Observe proper ESD techniques when connecting and disconnecting the DeviceMaster.

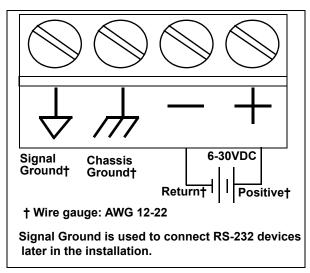
a. If the DIN rail is not connected to earth ground, insert the earth ground wire into the chassis ground screw terminal.

Note: The chassis ground connection is made only if the DIN rail is NOT connected to earth ground.

b. Insert the DC positive wire into the + screw terminal and the DC return wire into the - screw terminal.

Refer to <u>DM-2202 and DM-2402: 2-Port (Serial</u> <u>Terminals) Power Supply</u> on Page 141 for power requirements.

- c. Use a small flat head screw driver to lock the wires into place.
- d. Verify that each wire has been tightened securely.
- e. Connect a UL Listed power supply and UL Listed power cord to a power source to apply power.
- **Note:** Do not connect multiple units until you have changed the default IP address, see <u>Initial</u> <u>Configuration</u> on Page 33.
- 3. Use the appropriate method for network attachment of the DeviceMaster.



- **DM-2202:** Connect the 10/100 port to the same Ethernet network segment as the host PC using a standard network cable.
- **DM-2402:** Connect the DeviceMaster using either Ethernet port to the same Ethernet network segment as the host PC using a standard Ethernet cable. You can daisy-chain another DeviceMaster or Ethernet device to the other Ethernet port.

4. Verify that the **Status** LED has completed the boot cycle and network connection for the DeviceMaster is functioning properly using the following table.

DM-2202 and DM-2402 (2-Port with Serial Terminal Connectors) LED Descriptions			
STATUS	The STATUS LED on the device is lit, indicating you have power and it has completed the boot cycle.		
	Note: The Status LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.		
LINK	If the LINK (green) LED is lit, it indicates a working Ethernet connection.		
ACT	ACT If the ACT (yellow) LED flashes, it indicates network activity.		
Note: For additional LED information, go to the <u>Status LED tabl</u> e on Page 148.			



Do not connect RS-422/485 devices until the IP address is configured and an appropriate port interface type has been configured. The default port setting is RS-232.

DM-2102 and DM-2302: 2-Port DIN Rail (DB9) Installation

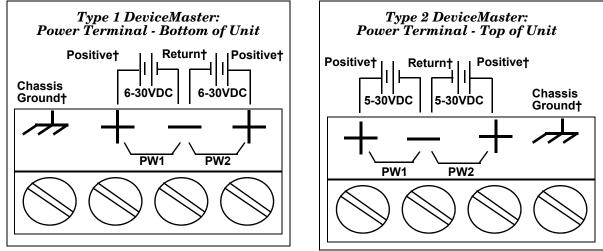
Use the following procedure to install DM-2102 and DM-2302.

- 1. Attach the DeviceMaster to the DIN rail adapter.
- 2. Connect the power supply and apply power to the DeviceMaster using the power supply specifications on the product label and the following information.

```
Observe proper ESD techniques when connecting and disconnecting the DeviceMaster.
```

a. If the DIN rail is not connected to earth ground, insert the earth ground wire into the chassis ground screw terminal.

Note: The chassis ground connection is made only if the DIN rail is NOT connected to earth ground.



† Wire gauge: AWG 12-22

b. Insert the DC positive wire into one of the + screw terminals and the DC return wire into the - screw terminal.

Type 1: 6-30VDC - serial number less than xxxx-030000.

Type 2: 5-30VDC - serial number greater than xxxx-030000.

A second redundant power supply can be connected to the unit by inserting the DC positive wire into the other + screw terminal and the DC return wire into the - screw terminal. The DeviceMaster continues to operate if one of the two connected power supplies should fail.

Refer to the appropriate subsection for detailed power requirements.

- DM-2102 and DM-2302: 2-Port DB9 Power Supply (Bottom) on Page 142
- DM-2102 and DM-2302: 2-Port DB9 Power Supply (Top) on Page 143
- Use a small flat head screw driver to lock the wires into place.
- d. Verify that each wire has been tightened securely.
- e. Connect a UL Listed power supply and UL Listed power cord to a power source to apply power.
- **Note:** Do not connect multiple units until you have changed the default IP address, see <u>Initial Configuration</u> on Page 33.

c.

- 3. Use the appropriate method for network attachment of your DeviceMaster 2-port:
 - **DM-2102**: Connect the **10/100 port** to the same Ethernet network segment as the host PC using a standard network cable.
 - **DM-2302**: Connect either 10/100 port to the same Ethernet network segment as the host PC using a standard network cable. You can daisy-chain another DeviceMaster or Ethernet device to the other Ethernet port.
- 4. Verify that the **Status** LED has completed the boot cycle and network connection for the DeviceMaster is functioning using the following table.

DM-2102 and DM-2302 (2-Port with DB9 Connectors) LED Descriptions			
	The STATUS LED on the device is lit, indicating you have power and it has completed the boot cycle.		
STATUS	Note: The Status LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.		
LINK	If the LINK (green) LED is lit, it indicates a working Ethernet connection.		
ACT If the ACT (yellow) LED flashes, it indicates network activity.			
Note: For additional LED information, go to the <u>Status LED table</u> on Page 148.			



Do not connect RS-422/485 devices until the IP address is configured and an appropriate ntion port interface type has been configured. The default port setting is RS-232.

DM-2304: 4-Port DIN Rail (DB9) Installation

Use the following procedure to install DM-2304.

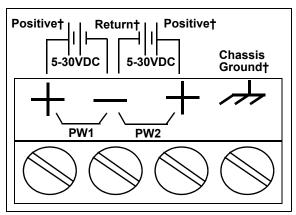
- 1. Attach the DeviceMaster to the DIN rail adapter.
- 2. Connect the power supply and apply power to the DeviceMaster using the power supply specifications on the product label and the following information.



Observe proper ESD techniques when connecting and disconnecting the DeviceMaster.

- a. If the DIN rail is not connected to earth ground, insert the earth ground wire into the chassis ground screw terminal.
- Note: The chassis ground connection is made only if the DIN rail is NOT connected to earth ground.
- b. Insert the DC positive wire into one of the + screw terminals and the DC return wire into the screw terminal.
 - A second redundant power supply can be connected to the unit by inserting the DC positive wire into the other + screw terminal and the DC return wire into the - screw terminal.
 - The DeviceMaster continues to operate if one of the two connected power supplies should fail.

Refer to <u>DM-2304: 4-Port DIN Rail Models Power</u> <u>Supply</u> on Page 144 for detailed power requirements.



† Wire gauge: AWG 12-22

- c. Use a small flat head screw driver to lock the wires into place.
- d. Verify that each wire has been tightened securely.
- e. Connect a UL Listed power supply and UL Listed power cord to a power source to apply power.
- **Note:** Do not connect multiple units until you have changed the default IP address, see <u>Initial Configuration</u> on Page 33.
- 3. Connect one of the **10/100** ports to the same Ethernet network segment as the host PC using a standard Ethernet cable. You can daisy-chain another DeviceMaster or Ethernet device to the other port using a standard Ethernet cable.
- 4. Verify that the **Status** LED has completed the boot cycle and network connection for the DeviceMaster is functioning properly using the following table.

DM-2304 LED Descriptions			
STATUS	The STATUS LED on the device is lit, indicating you have power and it has completed the boot cycle.		
	Note: The Status LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.		
LINK	If the LINK (green) LED is lit, it indicates a working Ethernet connection.		
ACT If the ACT (yellow) LED flashes, it indicates network activity.			
Note: For additional LED information, go to the <u>Status LED table</u> on Page 148.			

Do not connect RS-422/485 devices until the IP address is configured and an appropriate port interface type has been configured. The default port setting is RS-232.

5. Go to *Initial Configuration* on Page 33 to configure the DeviceMaster for use.

4-Port and 8-Port Installation

Use the following procedure to install the DeviceMaster 4-port or 8-port.

1. Optionally, attach the mounting brackets using the screws provided in the kit (6-32 1/4" flathead machine) or place the DeviceMaster on a stable surface.





DeviceMaster PRO and DeviceMaster Serial Hub

Failure to use the correct screws can damage the PCB and void the warranty. Do NOT use screws that exceed the length of the screws provided with the mounting bracket kit.

Note: If you ordered the DeviceMaster Rackmount Shelf Kit accessory, use the document that accompanied that kit or <u>download the document</u> to mount the DeviceMaster on the shelf.

- **Note:** Do not connect multiple units until you have changed the default IP address, see <u>Initial Configuration</u> on Page 33.
- 2. Connect the DeviceMaster to the same Ethernet network segment as the host PC. If the DeviceMaster serial number is below xxxx-030000 use one of the following methods to connect the cable. Serial numbers above xxxx-030000, the Ethernet port are interchangeable.
 - Ethernet hub or switch (10/100Base-T): Connect to the port labeled UP on the DeviceMaster using a standard Ethernet cable.
 - **Server NIC** (10/100Base-T): Connect to the port labeled DOWN on the DeviceMaster using a standard Ethernet cable.
 - **Daisy-chaining DeviceMaster units**: Connect the port labeled **DOWN** on the first DeviceMaster to the port labeled **UP** on the second DeviceMaster or other device using a standard Ethernet cable. Refer to <u>Daisy-Chaining DeviceMaster 4/8/16-Port Units</u> on Page 166.
- **Note:** Do not connect multiple units until you have changed the default IP address, see <u>Initial Configuration</u> on Page 33.
- 3. Apply power to the DeviceMaster by connecting the AC power adapter to the DeviceMaster, the appropriate power cord for your location to the power adapter, and plugging the power cord into a power source. If you want to provide a power supply, see <u>4-Port Panel Mount Power Supply</u> on Page 144.

4. Verify that the **PWR** LED has completed the boot cycle and the network connection for the DeviceMaster is functioning properly.

4-Port and 8-Port LED Descriptions					
	LED on the front panel of the DeviceMaster is lit, indicating you have power and it has completed the boot cycle.				
PWR	Note: The PWR LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.				
LNK ACT	The red LNK ACT LED is lit, indicating that you have a working Ethernet connection.				
COL	If the red COL LED is lit, there is a network collision.				
100	If the red 100 LED is lit, it indicates a working 100 MB Ethernet connection (100 MB network, only). If the LED is not lit, it indicates a 10 MB Ethernet connection.	UP DOWN			
Note: For additional LED information, go to the <u>Status LED table</u> on Page 148.					



Do not connect RS-422/485 devices until the IP address is configured and an appropriate port interface type has been configured. The default port setting is RS-232.

16-Port (DeviceMaster RTS - External Power Supply) Installation

Use the following procedure to install the DeviceMaster RTS 16-port with an external power supply.

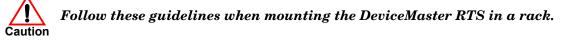
1. Place the DeviceMaster RTS on a stable surface, or *optionally* mount the DeviceMaster in a rack.

Rack Installation:

- Attach the L brackets to the interface using the screws supplied with the unit. ิล
- b. You can mount the unit facing in either direction.



Attach the L bracket into your rack. c.



- If the DeviceMaster is installed in a closed or multi-rack assembly, the operating • temperature of the rack environment may be greater than the ambient temperature. Be sure to install the DeviceMaster in an environment that is compatible with the maximum rated ambient temperature.
- Make sure that the mechanical loading is level to avoid a hazardous condition; such as, loading heavy equipment in the rack unevenly. The rack should safely support the combined weight of all equipment in the rack.
- Slots and openings in the cabinet are provided for ventilation. To ensure reliable operation of the DeviceMaster and to protect it from overheating, maintain a minimum of 1 inch of clearance on all sides of the unit.
- AC power inputs are intended to be used with a three-wire grounding type plug, which has a grounding pin. Equipment grounding ensures safe operation. Do not defeat the grounding means and verify that the DeviceMaster is reliably grounded when mounting within the rack.
- **Note:** Do not connect multiple units until you have changed the default IP address, see <u>Initial Configuration</u> on Page 33.
- Connect the DeviceMaster RTS to the same Ethernet network segment as the host PC. If the $\mathbf{2}$. DeviceMaster serial number is below xxxx-030000 use one of the following methods to connect the cable. Serial numbers above xxxx-030000, the Ethernet port are interchangeable.
 - Ethernet hub or switch (10/100Base-T): Connect to the port labeled UP on the DeviceMaster RTS using a standard Ethernet cable.
 - Server NIC (10/100Base-T): Connect to the port labeled DOWN on the DeviceMaster RTS using a standard Ethernet cable.
 - Daisy-chaining DeviceMaster units: Connect the port labeled DOWN on the first DeviceMaster RTS to the port labeled UP on the second DeviceMaster or other device using a standard Ethernet cable.



Do not connect RS-422/485 devices until the IP address is configured and an appropriate Caution port interface type has been configured (Step 5). The default port setting is RS-232.

- 3. Apply power to the DeviceMaster RTS by connecting the AC power adapter to the DeviceMaster, the power cord to the power adapter, and plugging the power cord into a power source. See <u>External Power</u> <u>Supply Specifications</u> on Page 139 if you want to provide your own power supply.
- 4. Verify that the **PWR** LED has completed the boot cycle and network connection for the DeviceMaster RTS is functioning properly using the table below.

DeviceMaster RTS 16-Port (External Power Supply) LED Descriptions					
Dad	Red LED on the front panel of the DeviceMaster is lit, indicating you have power and it has completed the boot cycle.				
Red LEDNote: The LED flashes while booting and it takes approximately 15 seconds f Bootloader to complete the cycle. When the Bootloader completes the cy LED has a solid, steady light that blinks approximately every 10 second					
LNK ACT	The red LNK ACT LED is lit, indicating that you have a working Ethernet connection.				
COL	If the red COL LED is lit, there is a network collision.				
100	If the red 100 LED is lit, it indicates a working 100 MB Ethernet connection (100 MB network, only). If the LED is not lit, it indicates a 10 MB Ethernet connection.	UP DOWN			
Note: For additional LED information, go to the <u>Status LED table</u> on Page 148.					

16-Port (DeviceMaster PRO) Installation

Use the following procedure to install the DeviceMaster PRO 16-port with an external power supply.

1. Place the DeviceMaster PRO on a stable surface, or *optionally* mount the DeviceMaster PRO in a rack. *Rack Installation:*

- a. Attach the L brackets to the DeviceMaster PRO using the screws supplied with the unit.
- b. You can mount the unit facing in either direction.

DEVICEMASTER PRO	1 7 7 7 7	9 15	
			o t
UP DOWN	2	10 16 16 24 VDC	POWER

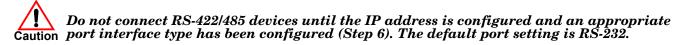
c. Attach the L bracket into your rack.



Follow these guidelines when mounting the DeviceMaster in a rack.

- If the DeviceMaster PRO is installed in a closed or multi-rack assembly, the operating temperature of the rack environment may be greater than the ambient temperature. Be sure to install the DeviceMaster in an environment that is compatible with the maximum rated ambient temperature.
- Make sure that the mechanical loading is level to avoid a hazardous condition; such as, loading heavy equipment in the rack unevenly. The rack should safely support the combined weight of all equipment in the rack.
- Slots and openings in the cabinet are provided for ventilation. To ensure reliable operation of the DeviceMaster and to protect it from overheating, maintain a minimum of 1 inch of clearance on all sides of the unit.
- AC power inputs are intended to be used with a three-wire grounding type plug, which has a grounding pin. Equipment grounding ensures safe operation. Do not defeat the grounding means and verify that the DeviceMaster is reliably grounded when mounting within the rack.
- *Note:* Do not connect multiple units until you have changed the default IP address, see <u>Initial Configuration</u> on Page 33.
- 2. Connect the DeviceMaster PRO to the same Ethernet network segment as the host PC using one of the following methods.
 - **Ethernet hub or switch (10/100Base-T)**: Connect to the port labeled **UP** on the DeviceMaster PRO using a standard Ethernet cable.
 - **Server NIC** (10/100Base-T): Connect to the port labeled DOWN on the DeviceMaster PRO using a standard Ethernet cable.
 - **Daisy-chaining DeviceMaster units**: Connect the port labeled **DOWN** on the first DeviceMaster PRO to the port labeled **UP** on the second DeviceMaster PRO or other device using a standard Ethernet cable.

Note: Do not connect multiple units until you have changed the default IP address, see <u>Initial</u> <u>Configuration</u> on Page 33.



- 3. Connect the power cord into a power source.
- 4. Apply power to the DeviceMaster PRO by turning on the power switch.

5. Verify that the **PWR** LED has completed the boot cycle and network connection for the DeviceMaster is functioning properly using the table below.

DeviceMaster PRO 16-Port LED Description				
Red LED (Front panel)	 Red LED on the front panel of the DeviceMaster PRO is lit, indicating you have power and it has completed the boot cycle. Note: The LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds. 			
LNK/ACT	The red LNK/ACT LED is lit, indicating that you have a working Ethernet connection.			
COL	If the red COL LED is lit, there is a network collision.	10/100 NETWORK		
100	If the red 100 LED is lit, it indicates a working 100 MB Ethernet connection (100 MB network, only). If the LED is not lit, it indicates a 10 MB Ethernet connection.	$ \begin{array}{c c} & & & \\ & & & &$		
Note: For additional LED information, go to the <u>Status LED table</u> on Page 148.				

16/32-Port Rack Mount Models (Internal Power Supply) Installation

Use the following procedure to install the DeviceMaster 16-port or 32-port with an internal power supply.

1. Place the DeviceMaster on a stable surface, or *optionally* mount the DeviceMaster in a rack.

Rack Installation:

a. Attach the L brackets to the interface using the screws supplied with the unit.



- b. You can mount the unit facing in either direction.
- c. Attach the L bracket into your rack.



Follow these guidelines when mounting the DeviceMaster in a rack.

- If the DeviceMaster is installed in a closed or multi-rack assembly, the operating temperature of the rack environment may be greater than the ambient temperature. Be sure to install the DeviceMaster in an environment that is compatible with the maximum rated ambient temperature.
- Make sure that the mechanical loading is level to avoid a hazardous condition; such as, loading heavy equipment in the rack unevenly. The rack should safely support the combined weight of all equipment in the rack.
- Slots and openings in the cabinet are provided for ventilation. To ensure reliable operation of the DeviceMaster and to protect it from overheating, maintain a minimum of 1 inch of clearance on all sides of the unit.
- AC power inputs are intended to be used with a three-wire grounding type plug, which has a grounding pin. Equipment grounding ensures safe operation. Do not defeat the grounding means and verify that the DeviceMaster is reliably grounded when mounting within the rack.
- **Note:** Do not connect multiple units until you have changed the default IP address, see <u>Initial Configuration</u> on Page 33.
- 2. Connect the DeviceMaster port labeled 10/100 NETWORK to the same Ethernet network segment as the host PC using a standard network cable.

DeviceMaster RTS

DEVICEMANTER RTS RM



Do not connect RS-422/485 devices until the IP address is configured and an appropriate Caution port interface type has been configured (Step 5). The default port setting is RS-232.

- 3. Apply power to the DeviceMaster by connecting the appropriate power cord into the power socket on the DeviceMaster, plugging the power cord into a power source, and turning on the power switch.
- 4. Verify that the **Status** LED has completed the boot cycle and network connection for the DeviceMaster is functioning properly using the table below.

16/32-Port (Internal Power Supply) LED Descriptions						
	The amber Status LED on the device is lit, indicating you have power and it has completed the boot cycle.					
Status	Note: The Status LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds. For additional LED information, go to the <u>Status LED table</u> on Page 148.					
LNK/ACT	The red LNK/ACT LED is lit, indicating that you have a working Ethernet connection.	INV/				
Duplex	If the red Duplex LED is lit, it indicates full-duplex activity.	ACT Duplex				
100	If the red 100 LED is lit, it indicates a working 100 MB Ethernet connection (100 MB network, only). If the LED is not lit, it indicates a 10 MB Ethernet connection.	● 100 10/100 ETHERNET				
Note: The port LED activity may be inconsistent until the port has been opened. After a port is opened, LED activity works as documented.						

5. Go to *Initial Configuration* on Page 33 to configure the DeviceMaster for use.

Adding a Unit to an Existing Installation

Use this procedure to add another DeviceMaster to an existing configuration.

- 1. Install the DeviceMaster to an Ethernet hub or server NIC using the appropriate subsection found in *Installation Overview* on Page 13.
 - **Note:** Technical support recommends installing one unit at a time and testing that unit when installing multiple units. In the event troubleshooting must be done, a single unit is easier to resolve than several at once.
- 2. Power-up the new DeviceMaster and verify that the PWR or Status LED lights.
- 3. Program an IP address into the new DeviceMaster using PortVision DX.
- 4. If necessary, upload the latest firmware.
- 5. Configure serial ports to support the serial devices or upload configuration files from PortVision DX.
- 6. Connect the serial devices.

Replacing Hardware

Use this procedure to replace hardware.

- 1. Remove the old unit and attach a new or spare DeviceMaster.
- 2. Connect the new DeviceMaster to the network hub or server NIC.
- 3. Apply power to the new DeviceMaster and verify that it passes the power on self-test.
- 4. Program the IP address of the new DeviceMaster.
- 5. If necessary, upload the latest protocol firmware.
- 6. Configure any ports as necessary to match the previous unit or upload configuration files from PortVision DX.
- 7. Transfer *all* cabling from the old DeviceMaster to the new DeviceMaster.
- 8. It is not necessary to shut down and restart the host PC.

Initial Configuration

There are several ways to configure network information. Comtrol Technical Support recommends connecting the DeviceMaster to a PC or laptop running Windows and installing *PortVision DX* for initial configuration.

Optionally, you can use RedBoot to configure the network address, see <u>RedBoot Procedures</u> on Page 131.

This section shows how to use PortVision DX for initial DeviceMaster configuration. It also defines requirements and how configuring DeviceMaster security affects PortVision DX and shows you how to:

- Install PortVision DX
- Configure the network address (<u>Page 38</u>)
- Check the SocketServer version on the DeviceMaster (Page 41)
- If necessary, download the latest version SocketServer and upload it into the DeviceMaster (Page 42)
- Organize how PortVision DX displays your Comtrol Ethernet attached products
- Access the latest documentation for your Comtrol Ethernet attached product

PortVision DX Overview

PortVision DX automatically detects Comtrol Ethernet attached products physically attached to the local network segment so that you can configure the network address, upload firmware, and manage the following products:

- DeviceMaster family
 - DM-2000 series
 - DeviceMaster EIP-2000 series
 - DeviceMaster MOD-2000 series
 - DeviceMaster PNIO-2000 series
 - DeviceMaster PRO
 - DeviceMaster RTS
 - DeviceMaster Serial Hub
- DeviceMaster UP
- DeviceMaster LT
- IO-Link Master
- RocketLinx switches

In addition to identifying Comtrol Ethernet attached products, you can use PortVision DX to display any third-party switch and hardware that may be connected directly to those devices. All non-Comtrol products and unmanaged RocketLinx switches are treated as non-intelligent devices and have limited feature support. For example, you cannot configure or update firmware on a third-party switch.

PortVision DX Requirements

Use PortVision DX to identify, configure, update, and manage the DeviceMaster on Windows Server 2008 R2 through Windows 10 operating systems.

PortVision DX requires that you connect the Comtrol Ethernet attached product to the same network segment as the Windows host system if you want to be able to scan and locate it automatically during the configuration process.

Note: You must install PortVision DX v3.02 or higher to load firmware with a .cmtl extension.

Configuring Security Settings and PortVision DX

The following list provides basic PortVision DX operations that are affected how the DeviceMaster interacts with PortVision DX when security is enabled using the web interface (SocketServer/NS-Link).

- PortVision DX must scan the DeviceMaster before configuring security.
- PortVision DX locates the DeviceMaster before setting either Secure Data Mode or Secure Config Mode.
 - If PortVision DX discovers the DeviceMaster after setting security, the following conditions occur:
 - A lock symbol displays before the Device Name.
 - The IP address of the DeviceMaster does not display.
 - The Software Settings and Web Interface tabs are not present in the Properties page.
 - The IP mode displays as DHCP without the ability to modify.
 - The **Upload** and **Reboot** icons on the *Launch Bar* are grayed out and the options are disabled in the popup menus.

Note: If the DeviceMaster was previously configured with security, PortVision DX features are reduced.

Installing PortVision DX

During initial configuration, PortVision DX automatically detects and identifies DeviceMaster units, if they are in the same network segment.

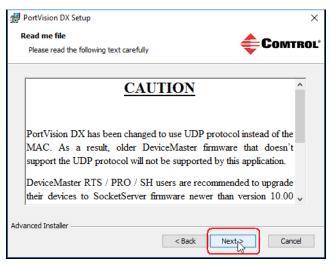
1. Download PortVision DX: <u>http://downloads.comtrol.com/dev_mstr/portvision_dx</u>.

Note: Depending on your operating system, you may need to respond to a Security Warning to permit access.

- 2. Execute the PortVision_DX[version].msi file.
- 3. Click Next on the Welcome screen.



4. Review the CAUTION - Read me file and then click Next.



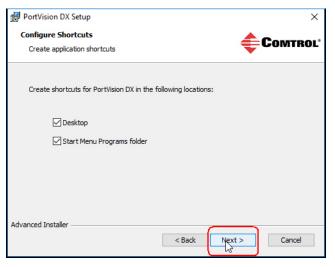
5. Click I accept the terms in the License Agreement and Next.

🛃 PortVision DX Setup			Х
End-User License Agreement		-	COMTROL
Please read the following license agreement	carefully	•	COMINCL
PortVisio	<u>n DX</u> ™		
END USER LICENS	SE AGREE	MENT	
COMTROL CORPORATION ("COMTRO ADMINISTRATION AND MANAG DEVICEMASTER, ROCKETLINX, AN	iement s	YSTEM FO	DR ITS
I accept the terms in the License Agreement	ent		
\bigcirc I do not accept the terms in the License A	greement		
Advanced Installer	< Back	Next >	Cancel

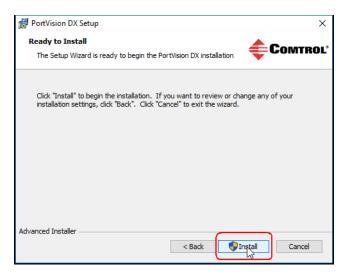
6. Click Next or optionally, browse to a different location and then click Next.

🛃 PortVision DX Setup	_		×
Select Installation Folder		Сомт	PO1*
This is the folder where PortVision DX will be installed.	V		NUL
To install in this folder, click "Next". To install to a different folder, ent "Browse".	er it bel	ow or click	
Eolder:			
C:\Program Files (x86)\Comtrol\PortVision DX\		Browse	
Advanced Installer	_	1	
< Back Next >		Cance	el

7. Click Next to configure the shortcuts.

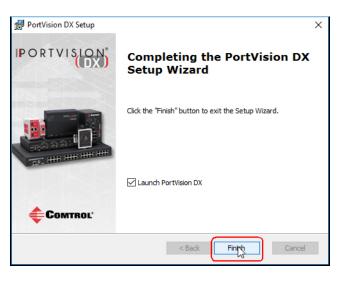


8. Click Install.



- 9. Depending on the operating system, you may need to click **Yes** to the *Do you want to allow the following program to install software on this computer*? query.
- 10. Click Launch PortVision DX and Finish in the last installation screen.
- 11. Depending on the operating system, you may need to click Yes to the *Do you want to allow the following program to make changes to this computer*? query.
- 12. Select the Comtrol Ethernet attached products that you want to locate and then click Scan.
 - Save time, only scan for DeviceMasters.

Scan Network	×
Select any number of device types from the list below and click Scan to start scanning the network.	
I DeviceMaster □ IO-Link Master □ RocketLinx (Managed Only)	
Note: If you want to abort the process, click Cancel.	



- **Note:** If the Comtrol Ethernet attached product is not on the local segment and it has been programmed with an IP address, it will be necessary to manually add the Comtrol Ethernet attached product to PortVision DX.
- 13. Go to <u>Step 6</u> in the next section, *Configuring the Network Settings*, to program the DeviceMaster network settings.

If you need additional information about PortVision DX, refer to the Help system.

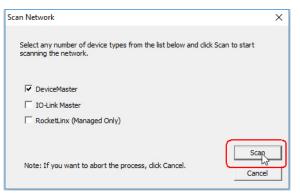
Configuring the Network Settings

Use the following procedure to change the default network settings on the DeviceMaster for your network. The default network settings are:

- IP address: 192.168.250.250
- Subnet mask: 255.255.0.0
- Gateway address: 192.168.250.1
- **Note:** Technical Support advises configuring one new DeviceMaster at a time to avoid device driver configuration problems. If you want to configure multiple DeviceMasters using the Assign IP to Multiple Devices option, see <u>Configuring Multiple DeviceMasters Network Addresses</u> on Page 105.

The following procedure shows how to configure a single DeviceMaster connected to the same network segment as the Windows system. If the DeviceMaster is not on the same physical segment, you can add it manually using <u>Adding a New Device in PortVision DX</u> on Page 105.

- 1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 35).
- 2. Start PortVision DX using the **PortVision DX** desktop shortcut or from the **Start** button, click **Comtrol** > **PortVision DX**.
- 3. Depending on your operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* query.
- 4. Click the Scan button in the Toolbar.
- 5. Click Scan to locate the Comtrol Ethernet attached products including the DeviceMaster on the network.



Note: If you do not have any RocketLinx managed switches or IO-Link Masters, it saves scanning time if you do not scan for them.

If PortVision DX does not locate your DeviceMaster on the network, make sure that you are using the <u>latest version of</u> <u>PortVision DX</u>.

- 6. Highlight the DeviceMaster for which you want to program network information and open the **Properties** screen using one of these methods.
 - Double-click the DeviceMaster in the *Device Tree* or *Device List* pane.
 - Highlight the DeviceMaster in the Device Tree or Device List pane and click the Properties button.
 - Right-click the DeviceMaster in the *Device Tree* or *Device List* pane and click **Properties** in the popup menu
 - Highlight the DeviceMaster, click the Manage menu and then Properties.

	ion DX	.								
e Man	nage View	Tools Help								
	\sim	12	sk	1 6	9 0	T 5	A 🚽	r		
.	\sim	Carmen	2			~	• -			
Scan	Refresh All	Properties	Save	Load Upload	Reboot Webpage I	Notes Help	About Exit			
IP (ORTVIS	LON [®]				The contents o in the <i>Device</i> I ew				
ame : Sca	an Results		<u>^</u>		, i					
			_			Dev	ice Tree	Pane		
se menu	or toolbar to ad	ld notes in	<u> </u>							
his area.										
				ra Nama	Model	D Addr	MAC Address	Coffuero Varian	Status	
				e Name	Model	IP Addr		Software Version	Status	
			B 🗸	Device 3C:00:02	ES8508F-MM	192.168.0.164	00:C0:4E:3C:00:02	v1.3c (b1.6.1.5)	ON-LINE	
			8 8	Device 3C:00:02 Device 2D:00:08	ES8508F-MM ES7506	192.168.0.164 192.168.11.100	00:C0:4E:3C:00:02 00:C0:4E:2D:00:08	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5)	ON-LINE ON-LINE	
				Device 3C:00:02 Device 2D:00:08 Device 32:00:00	ES8508F-MM ES7506 ES7528	192.168.0.164 192.168.11.100 192.168.11.101	00:C0:4E:3C:00:02 00:C0:4E:2D:00:08 00:C0:4E:32:00:00	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5) v1.4a (b0.3.0.10)	ON-LINE ON-LINE ON-LINE	
			間 ~ 間 ~ 間 ~ 間 ~	Device 3C:00:02 Device 2D:00:08 Device 32:00:00 Device 35:00:09	ES8508F-MM ES7506 ES7528 ES8509-XT	192.168.0.164 192.168.11.100 192.168.11.101	00:C0:4E:3C:00:02 00:C0:4E:2D:00:08 00:C0:4E:32:00:00	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5) v1.4a (b0.3.0.10)	ON-LINE ON-LINE ON-LINE ON-LINE	
			8 - 8 - 8 - 8 - 8 - 8 - 8 - 8 -	Device 3C:00:02 Device 2D:00:08 Device 32:00:00 Device 35:00:09 Device 2C:00:6C	ES8508F-MM ES7506 ES7528 ES8509-XT ES8510	192.168.0.164 192.168.11.100 192.168.11.101 192.1(192.1)	00:C0:4E:3C:00:02 00:C0:4E:2D:00:08 00:C0:4E:32:00:00 ice List F	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5) v1.4a (b0.3.0.10) Pane L.5 ? (b1.6.2.12)	ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE	
			調査の問題の	Device 3C:00:02 Device 2D:00:08 Device 32:00:00 Device 35:00:09 Device 2C:00:6C Device 34:00:08	ES8508F-MM ES7506 ES7528 ES8509-XT ES8510 ES7510	192.168.0.164 192.168.11.100 192.168.11.101 192.1¢ 192.1¢ 192.168.11.104	00:C0:4E:3C:00:02 00:C0:4E:2D:00:08 00:C0:4E:32:00:00 ice List F 00:C0:4E:34:00:08	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5) v1.4a (b0.3.0.10) 2ane v1.3c_beta4 (b1.2.1.6)	ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE	
			調査部務部務部務部務部務部務部務部務部務部務部務部務部務部務部務部務部務部務部務	Device 3C:00:02 Device 2D:00:08 Device 32:00:00 Device 35:00:09 Device 2C:00:6C Device 34:00:08 Device 36:00:02	ES8508F-MM ES7506 ES7528 ES8509-XT ES8510 ES7510 ES9528-XT	192.168.0.164 192.168.11.100 192.168.11.101 192.1(192.1(192.1(192.168.11.104 192.168.11.104	00:C0:4E:3C:00:02 00:C0:4E:2D:00:08 00:C0:4E:32:00:00 ice List F 00:C0:4E:34:00:08 00:C0:4E:36:00:02	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5) v1.4a (b0.3.0.10) 2 ane L.5 ? (b1.6.2.12) v1.3c_beta4 (b1.2.1.6) v1.4a (b11.0.4)	ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE	
			ななななななななななななななななななななななななななななななななななななな	Device 3C:00:02 Device 2D:00:08 Device 32:00:00 Device 35:00:09 Device 2C:00:6C Device 36:00:08 Device 36:00:02 Device 30:00:10	ES8508F-MM ES7506 ES7528 ES8509-XT ES8510 ES7510 ES9528-XT ES8510-XTE	192.168.0.164 192.168.11.100 192.168.11.101 192.11 Dev 192.168.11.104 192.168.11.104 192.168.11.105 192.168.11.105	00:C0:4E:3C:00:02 00:C0:4E:2D:00:08 00:C0:4E:32:00:00 ice List F 00:C0:4E:34:00:08 00:C0:4E:34:00:08 00:C0:4E:36:00:02 00:C0:4E:30:00:10	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5) v1.4a (b0.3.0.10) Dane v1.3c beta4 (b1.2.1.6) v1.4a (b1.1.0.4) v2.7b beta2 (b1.6.2.12)	ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE	
				Device 3C:00:02 Device 2D:00:08 Device 32:00:00 Device 35:00:09 Device 2C:00:6C Device 34:00:08 Device 36:00:02 Device 30:00:10 Device 38:00:02	ESS08F-MM ES7506 ES7528 ES8509-XT ES8510 ES7510 ES9528-XT ES8510-XTE ES8510-XTE	192.168.0.164 192.168.11.100 192.168.11.101 192.11 192.11 192.168.11.104 192.168.11.105 192.168.11.105 192.168.11.107	00:C0:4E:3C:00:02 00:C0:4E:3C:00:02 00:C0:4E:32:00:00 ice List F 00:C0:4E:36:00:02 00:C0:4E:36:00:02 00:C0:4E:38:00:02	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5) v1.4a (b0.3.0.10) 200 e (5) v1.4b (b1.2.1.6) v1.4a (b1.1.0.4) v1.4a (b1.1.0.4) v2.7b (b1.6.2.12) v1.3c (b1.6.2.12) v1.3c (b1.6.2.12)	ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE	
				Device 3C:00:02 Device 2D:00:08 Device 32:00:00 Device 35:00:09 Device 2C:00:6C Device 34:00:08 Device 36:00:02 Device 30:00:10 Device 38:00:02 Device 3A:00:0D	ES8508F-MM ES7506 ES7528 ES8509-XT ES8510 ES7510 ES9528-XT ES8510-XTE ES9528-XT ES8510-XT ES8508	192.168.0.164 192.168.11.100 192.168.11.101 192.14 192.14 192.168.11.104 192.168.11.104 192.168.11.106 192.168.11.106	00:C0:4E:3C:00:02 00:C0:4E:3C:00:08 00:C0:4E:32:00:00 ice List F 00:C0:4E:34:00:08 00:C0:4E:36:00:02 00:C0:4E:38:00:02 00:C0:4E:38:00:02 00:C0:4E:38:00:02	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5) v1.4a (b0.3.0.10) ene 1.5 v1.3c_beta4 (b1.2.1.6) v1.4a (b1.1.0.4) v2.7b_beta2 (b1.6.2.12) v1.3c_beta7 (b1.4.1.6) v1.3c (b1.5.1.5)	ON-LINE	
				Device 3C:00:02 Device 2D:00:08 Device 32:00:00 Device 35:00:09 Device 35:00:09 Device 36:00:02 Device 36:00:02 Device 30:00:10 Device 38:00:02 Device 30:00:00 Device 33:00:00 Device 33:00:00	ES8508F-MM ES7506 ES7528 ES8509-XT ES8510 ES9528-XT ES9528-XT ES8510-XT ES8508 ES8510-XT	192.168.0.164 192.168.11.100 192.168.11.101 192.14 Devi 192.168.11.104 192.168.11.105 192.168.11.106 192.168.11.106 192.168.11.108 192.168.11.101	00:C0:4E:3C:00:02 00:C0:4E:3C:00:08 00:C0:4E:32:00:00 ice List F 00:C0:4E:34:00:08 00:C0:4E:34:00:08 00:C0:4E:36:00:02 00:C0:4E:38:00:02 00:C0:4E:3A:00:0D 00:C0:4E:3A:00:0D 00:C0:4E:3A:00:01	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5) v1.4a (b0.3.0.10) v1.5c beta4 (b1.2.1.6) v1.4a (b1.1.0.4) v2.7b beta2 (b1.6.2.12) v1.3c beta7 (b1.4.1.6) v1.3c (b1.5.1.5) v2.7c beta2 (b1.6.2.12)	ON-LINE	
				Device 3C:00:02 Device 2D:00:08 Device 32:00:00 Device 32:00:00 Device 3C:00:00 Device 30:00:00 Device 30:00:00 Device 30:00:00 Device 30:00:00 Device 30:00:00 Device 30:00:00 Device 3D:00:00 Device 2F:03:10 Device 1C:FF:FD	ES8508F-MM ES7506 ES7528 ES8509-XT ES8510 ES7510 ES9528-XT ES8510-XT ES8510-XT ES8510-XT ES8508 ES8510-XT SH-8P (DB9)	192.168.0.164 192.168.11.00 192.168.11.01 192.14 Dev 192.168.11.04 192.168.11.04 192.168.11.06 192.168.11.07 192.168.11.08 192.168.11.10 192.168.11.11	00:C0:4E:3C:00:02 00:C0:4E:3C:00:08 00:C0:4E:32:00:00 ice List F 00:C0:4E:34:00:08 00:C0:4E:34:00:08 00:C0:4E:36:00:10 00:C0:4E:38:00:02 00:C0:4E:38:00:02 00:C0:4E:38:00:02 00:C0:4E:36:00:10 00:C0:4E:56:31D 00:C0:4E:1C:FF:FD	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5) v1.4a (b0.3.010) ane (b1.6.2.12) v1.3c beta4 (b1.2.1.6) v1.4a (b1.1.0.4) v2.7b beta2 (b1.6.2.12) v1.3c (b1.5.1.5) v2.7c beta2 (b1.6.2.12) v3.5tin(9.28)	ON-LINE	
				Device 3C:00:02 Device 2D:00:08 Device 32:00:00 Device 35:00:09 Device 35:00:09 Device 36:00:02 Device 36:00:02 Device 30:00:10 Device 30:00:02 Device 30:00:02 Device 30:00:02 Device 2F:03:10 Device 2F:03:10 Device 1C:FF:FD Device 9570-000036	ES8508F-MM ES7506 ES7528 ES8509-XT ES8510 ES7510 ES9528-XT ES8510-XT ES8510-XT ES8508 ES8510-XT SH-8P (DB9) 4-EIP	192.168.0.164 192.168.11.00 192.168.11.01 192.11 Dev 192.168.11.105 192.168.11.105 192.168.11.105 192.168.11.108 192.168.11.108 192.168.11.109	00:C0:4E:3C:00:02 00:C0:4E:2D:00:08 00:C0:4E:2D:00:08 ice List F 00:C0:4E:36:00:02 00:C0:4E:36:00:02 00:C0:4E:36:00:02 00:C0:4E:3A:00:0D 00:C0:4E:2F:03:1D 00:C0:4E:2F:FED 00:C0:4E:39:00:23	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5) v1.4a (b0.3.0.10) ene t.5) v1.3c beta4 (b1.2.1.6) v1.4a (b1.1.0.4) v2.7b beta2 (b1.6.2.12) v1.3c beta7 (b1.4.1.6) v1.3c (b1.5.1.5) v2.7c beta2 (b1.6.2.12) NS-Link 9.28 EtherNet/IP 1.2.0	ON-LINE	
				Device 3C:00:02 Device 2D:00:08 Device 32:00:00 Device 35:00:09 Device 35:00:09 Device 36:00:02 Device 36:00:02 Device 36:00:02 Device 36:00:02 Device 36:00:01 Device 36:00:00 Device 36:00:00 Device 36:00:00 Device 36:00 Device 36:00 Devi	ES8508F-MM ES7506 ES7528 ES8509-XT ES8510 ES7510 ES9528-XT ES8510-XTE ES8510-XT ES8508 ES8510-XT SH-8P (DB9) 4-EIP PRO-8P (DB9)	192.168.0.164 192.168.11.00 192.168.11.01 192.14 Dev 192.168.11.04 192.168.11.04 192.168.11.06 192.168.11.07 192.168.11.10 192.168.11.10 192.168.11.10 192.168.11.198 192.168.11.198	0:C04E32:00:02 0:C04E22:00:08 0:C04E22:00:08 0:C04E32:00:00 0:C04E34:00:08 0:C04E36:00:02 0:C04E36:00:02 0:C04E36:00:02 0:C04E36:00:02 0:C04E36:00:02 0:C04E36:00:02 0:C04E12:FFI5	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5) v1.4s (b0.3.0.10) ane (.5) v1.3c (b1.6.2.12) v1.4s (b1.2.1.6) v1.4s (b1.2.1.6) v1.4s (b1.2.1.6) v1.3c (b1.6.2.12) v1.3c (ON-LINE	
				Device 3C:00:02 Device 3C:00:00 Device 2D:00:08 Device 3C:00:00 Device 3C:00:00 Device 3C:00:00 Device 3C:00:02 Device 3C:00:02 Device 3C:00:02 Device 3C:00:02 Device 3C:00:01 Device 3C:00:02 Device 3C:00:02 Device 3C:00:02 Device 3C:00:02 Device 1C:FF:FD Device 17:FF:FF Device 17:FF:FF Device 17:FF:FF Device 17:FF:FF	ES8508F-MM ES7506 ES7528 ES8509-XT ES8510 ES7510 ES9528-XT ES8510-XT ES8510-XT ES8508 ES8510-XT ES8508 ES8510-XT SH-8P (DB9) A-EIP PRO-8P (DB9) RTS-4P (DB9)	192.168.0.164 192.168.11.00 192.168.11.01 192.14 Dev 192.168.11.04 192.168.11.05 192.168.11.105 192.168.11.105 192.168.11.107 192.168.11.101 192.168.11.110 192.168.11.111 192.168.11.121	00:C04E3C:00:02 00:C04E3C:00:08 00:C04E32:00:08 00:C04E32:00:08 00:C04E32:00:08 00:C04E32:00:08 00:C04E32:00:02 00:C04E32:00:02 00:C04E32:00:02 00:C04E32:00:02 00:C04E3:00:23 00:C04E3:00:23 00:C04E3:00:23 00:C04E3:00:23	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5) v1.4a (b0.3.0.10) ane (b1.5) v1.3c (b1.6.2.12) v1.3c (b1.6.2.12) v1	ON-LINE	
				Device 3C:00:02 Device 2D:00:08 Device 2D:00:09 Device 35:00:09 Device 35:00:09 Device 36:00:02 Device 36:00:02 Device 30:00:02 Device 30:00:02 Device 30:00:02 Device 2F:03:10 Device 2F:03:10 Device 17:FF:FD Device 07:FF:FC Device 07:FF:FC Device 07:FF:FC Device 07:FF:FC	ES8508F-MM ES7506 ES7528 ES8509-XT ES8510 ES7510 ES9528-XT ES8510-XT ES8510-XT ES8508 ES8510-XT SH-8P (DB9) 4-EIP PRO-8P (DB9) RT5-4P (DB9) RT5-4P (DB9)	192.168.0.164 192.168.11.00 192.168.11.01 192.11 Dev 192.168.11.05 192.168.11.105 192.168.11.105 192.168.11.108 192.168.11.108 192.168.11.108 192.168.11.198 192.168.11.20 192.168.11.20	00:C04E3C0042 00:C04E320008 00:C04E320008 00:C04E320000 00:C04E340048 00:C04E340048 00:C04E340048 00:C04E340048 00:C04E340048 00:C04E340048 00:C04E340048 00:C04E340048 00:C04E340028 00:C04E340028 00:C04E340028 00:C04E3420028 00:C04E3420028 00:C04E3420028 00:C04E3420028 00:C04E3420028 00:C04E3420028 00:C04E342FFF8	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5) v1.4a (b0.30.10) e1.5 v1.3c beta4 (b1.21.6) v1.4a (b1.21.6) v1.4a (b1.10.4) v2.7b beta2 (b1.6.212) v1.3c beta7 (b1.41.6) v1.3c (b1.51.5) v2.7c beta2 (b1.6.212) NS-Link 9.28 EtherNet/IP 1.2.0 NS-Link 9.18 SocketServer 9.30 SocketServer 9.35	ON-LINE ON-LINE	
				Device 3C:00:02 Device 3C:00:00 Device 2D:00:08 Device 3C:00:00 Device 3C:00:00 Device 3C:00:00 Device 3C:00:02 Device 3C:00:02 Device 3C:00:02 Device 3C:00:02 Device 3C:00:01 Device 3C:00:02 Device 3C:00:02 Device 3C:00:02 Device 3C:00:02 Device 1C:FF:FD Device 17:FF:FF Device 17:FF:FF Device 17:FF:FF Device 17:FF:FF	ES8508F-MM ES7506 ES7528 ES8509-XT ES8510 ES7510 ES9528-XT ES8510-XT ES8510-XT ES8508 ES8510-XT ES8508 ES8510-XT SH-8P (DB9) A-EIP PRO-8P (DB9) RTS-4P (DB9)	192.168.0.164 192.168.11.00 192.168.11.01 192.14 Dev 192.168.11.04 192.168.11.05 192.168.11.105 192.168.11.105 192.168.11.107 192.168.11.101 192.168.11.110 192.168.11.111 192.168.11.121	00:C04E3C:00:02 00:C04E3C:00:08 00:C04E32:00:08 00:C04E32:00:08 00:C04E32:00:08 00:C04E32:00:08 00:C04E32:00:02 00:C04E32:00:02 00:C04E32:00:02 00:C04E32:00:02 00:C04E3:00:23 00:C04E3:00:23 00:C04E3:00:23 00:C04E3:00:23	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5) v1.4a (b0.30.10) e1.5 v1.3c beta4 (b1.21.6) v1.4a (b1.21.6) v1.4a (b1.10.4) v2.7b beta2 (b1.6.212) v1.3c beta7 (b1.41.6) v1.3c (b1.51.5) v2.7c beta2 (b1.6.212) NS-Link 9.28 EtherNet/IP 1.2.0 NS-Link 9.18 SocketServer 9.30 SocketServer 9.35	ON-LINE	
				Device 3C:00:02 Device 2D:00:08 Device 2D:00:09 Device 35:00:09 Device 35:00:09 Device 36:00:02 Device 36:00:02 Device 30:00:02 Device 30:00:02 Device 30:00:02 Device 2F:03:10 Device 2F:03:10 Device 17:FF:FD Device 07:FF:FC Device 07:FF:FC Device 07:FF:FC Device 07:FF:FC	ES8508F-MM ES7506 ES7528 ES8509-XT ES8510 ES7510 ES9528-XT ES8510-XT ES8510-XT ES8508 ES8510-XT SH-8P (DB9) 4-EIP PRO-8P (DB9) RT5-4P (DB9) RT5-4P (DB9)	192.168.0.164 192.168.11.00 192.168.11.01 192.11 Dev 192.168.11.05 192.168.11.105 192.168.11.105 192.168.11.108 192.168.11.108 192.168.11.108 192.168.11.198 192.168.11.20 192.168.11.20	00:C04E3C0042 00:C04E320008 00:C04E320008 00:C04E320000 00:C04E340048 00:C04E340048 00:C04E340048 00:C04E340048 00:C04E340048 00:C04E340048 00:C04E340048 00:C04E340048 00:C04E340028 00:C04E340028 00:C04E340028 00:C04E3420028 00:C04E3420028 00:C04E3420028 00:C04E3420028 00:C04E3420028 00:C04E3420028 00:C04E342FFF8	v1.3c (b1.6.1.5) v2.3 (b1.6.4.5) v1.4a (b0.30.10) e1.5 v1.3c beta4 (b1.21.6) v1.4a (b1.21.6) v1.4a (b1.10.4) v2.7b beta2 (b1.6.212) v1.3c beta7 (b1.41.6) v1.3c (b1.51.5) v2.7c beta2 (b1.6.212) NS-Link 9.28 EtherNet/IP 1.2.0 NS-Link 9.18 SocketServer 9.30 SocketServer 9.35	ON-LINE ON-LINE	

ls Documentation	
General Software Settings Web Interface	
DeviceMaster RTS 2-F	Port (2E)
DEV CE-MASTER*	
Basic Information Device Name : Device 29:FF:F5 MAC Address : 00:C0:4E:29:FF:F5 Serial Number : Device Status : ON-LINE Device Status : ON-LINE Detection Type : LOCAL	
IP Address : 192 168 11 52 Subnet Mask : 255 255 0 0 Default Gateway : 192 168 0 2 Bootloader Timeout : 15 15 15 15	

7. Optionally, rename the DeviceMaster in the Device Name field.

Note: SocketServer versions previous to v9.00 did not support the Bootloader Timeout option in the PortVision DX **Properties** screen.

- **Note:** The MAC address and Device Status fields are automatically populated and you cannot change those values.
- 8. Optionally, enter the serial number, which is on a label on the DeviceMaster.
- 9. If necessary, you can change the **Detection Type**.
 - **REMOTE** means that the DeviceMaster is not connected to this segment of the network and it uses IP communications, not MAC communications.
 - LOCAL means that the DeviceMaster is on this local network segment and uses MAC communications. An IP address is not required but Technical support recommends using an IP address.
- 10. Change the DeviceMaster network properties as required for your site.
 - If you want to disable IP communications on the DeviceMaster, click Disable IP.
 - To use the DeviceMaster with DHCP, click **DHCP IP**, and make sure that you provide the MAC address of the device to the network administrator. Make sure that the administrator reserves the IP address, subnet mask and gateway address of the DeviceMaster in the DHCP server.
 - To program a static IP address, click Static IP and enter the appropriate values for your site.

Note: For additional information, open the PortVision DX Help system.

- 11. Typically, the **Bootloader Timeout** value should be left to it's default value. In some situations, you may need to temporarily adjust the **Bootloader Timeout** to a higher value during a firmware update.
- 12. Click Apply Changes to update the network information on the DeviceMaster.

Note: If you are deploying multiple DeviceMasters that share common values, you can save the configuration file and load that configuration onto other DeviceMasters. See <u>Using the SocketServer</u> <u>Configuration Files</u> on Page 107 for more information.

13. Click Close to exit the *Properties* window.

Go to <u>*Checking the SocketServer Version</u>* on Page 41 to check the SocketServer version. You should update SocketServer firmware before any further configuration.</u>

Checking the SocketServer Version

<u>SocketServer</u> refers to the web page that is integrated in the firmware that comes pre-installed on your DeviceMaster platform, which provides an interface to TCP/IP socket mode configuration and services. If you install an NS-Link device driver, an NS-Link version of SocketServer loads on the DeviceMaster.

Note: Technical Support recommends that you update to the latest version of SocketServer before installing an NS-Link device driver or configuring socket ports.

Use the following procedure to check the SocketServer version on the DeviceMaster and check the ftp site for the latest version.

- 1. If necessary, open PortVision DX (Comtrol > PortVision DX) or use the desktop shortcut and scan the network.
- 2. Check the SocketServer version number of the Software Version for the DeviceMaster.

PortVision DX							
ile Manage View Tools Help							
Scan Refresh All Properties Si			Notes Help	🚹 🚽			
PORTVISION	E E E E E E E E E E E E E E E E E E E						
Name : Scan Results							
*							
			Software	(main annlic	ation) version		
ise menu or toolbar to add notes in Anis area.			Software	(main applic	ation) version		
	Device Name	Model	Software	MAC Address	Software Version	Status	
	Device Name	Model ES8510		MAC Address	Software Version	Status ON-LINE	
			IP Addr	MAC Address 00:C0:4E:2C:00:6C	Software Version v2.7c_beta2 (b1.6.2.12)		
	Device 2C:00:6C	ES8510	▲ IP Addr 192.168.11.103 192.168.11.104	MAC Address 00:C0:4E:2C:00:6C 00:C0:4E:34:00:08	Software Version v2.7c_beta2 (b1.6.2.12) v1.3c_beta4 (b1.2.1.6)	ON-LINE	
	Device 2C:00:6C	ES8510 ES7510	▲ IP Addr 192.168.11.103 192.168.11.104 192.168.11.105	MAC Address 00:C0:4E:2C:00:6C 00:C0:4E:34:00:08 00:C0:4E:36:00:02	Software Version v2.7c_beta2 (b1.6.2.12) v1.3c_beta4 (b1.2.1.6) v1.4a (b1.1.0.4)	ON-LINE ON-LINE ON-LINE	
	Device 2C:00:6C Device 34:00:08 V Device 36:00:02	ES8510 ES7510 ES9528-XT	▲ IP Addr 192.168.11.103 192.168.11.104 192.168.11.105 192.168.11.105	MAC Address 00:C0:4E:2C:00:6C 00:C0:4E:34:00:08 00:C0:4E:36:00:02 00:C0:4E:30:00:10	Software Version v2.7c_beta2 (b1.6.2.12) v1.3c_beta4 (b1.2.1.6) v1.4a (b1.1.0.4) v2.7b_beta2 (b1.6.2.12)	ON-LINE ON-LINE	
		ES8510 ES7510 ES9528-XT ES8510-XTE	▲ IP Addr 192.168.11.103 192.168.11.104 192.168.11.105 192.168.11.105	MAC Address 00:C0:4E:2C:00:6C 00:C0:4E:34:00:08 00:C0:4E:36:00:02 00:C0:4E:36:00:10 00:C0:4E:38:00:02	Software Version v1.3c_beta2 (b1.6.2.12) v1.3c_beta4 (b1.2.1.6) v1.4a (b1.1.0.4) v2.7b_beta2 (b1.6.2.12) v1.3c (b1.4.1.6)	ON-LINE ON-LINE ON-LINE ON-LINE	
	✓ Device 2C:00:6C ✓ Device 34:00:08 ✓ Device 36:00:02 ✓ Device 30:00:10 Device 34:00:02 Device 34:00:02 ✓ Device 34:00:02	ES8510 ES7510 ES9528-XT ES8510-XTE ES7510-XT	▲ IP Addr 192.168.11.03 192.168.11.04 192.168.11.05 192.168.11.05 192.168.11.07 192.168.11.108	MAC Address 00:C0:4E:2C:00-6C 00:C0:4E:36:00:02 00:C0:4E:36:00:02 00:C0:4E:38:00:02 00:C0:4E:38:00:02 00:C0:4E:38:00:02	Software Version v2.7c_beta2 (b1.6.2.12) v1.3c_beta4 (b1.21.6) v1.4a (b1.10.4) v2.7b_beta2 (b1.6.2.12) v1.3c (b1.41.6) v1.3c (b1.51.5)	ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE	
is area.	✓ Device 2C:00:6C ✓ Device 34:00:08 ✓ Device 36:00:02 ✓ Device 38:00:02	ES8510 ES7510 ES9528-XT ES8510-XT ES8510-XT ES8508 ES8510-XT	P Addr 192.168.11.103 192.168.11.104 192.168.11.105 192.168.11.106 192.168.11.108 192.168.11.108	MAC Address 00:C0:4E:2C:00:6C 00:C0:4E:34:00:08 00:C0:4E:36:00:02 00:C0:4E:38:00:02 00:C0:4E:38:00:02 00:C0:4E:38:00:02 00:C0:4E:38:00:02	Software Version v2.7c_beta2 (b1.6.2.12) v1.3c_beta4 (b1.2.1.6) v1.4a (b1.1.0.4) v2.7b_beta2 (b1.6.2.12) v1.3c (b1.4.1.6) v1.3c (b1.5.1.5) v2.7c_beta2 (b1.5.2.12)	ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE	
er menu or toobar to add notes in	✓ Device 2C:00.6C ✓ Device 34:00:08 ✓ Device 34:00:02 ✓ Device 30:00:10 ✓ Device 30:00:10 ✓ Device 34:00:02 ✓ Device 34:00:02 ✓ Device 34:00:02 ✓ Device 34:00:01 ✓ Device 34:00:01 ✓ Device 10:01 ✓ Device 10:01	ES8510 ES7510 ES9528-XT ES8510-XT ES8508 ES8510-XT ES8508 ES8510-XT SH-8P (DB9)	▲ IP Addr 192.168.11.103 192.168.11.104 192.168.11.105 192.168.11.106 192.168.11.107 192.168.11.101 192.168.11.114	MAC Address 00:C0:4E:2C:00-6C 00:C0:4E:34:00:08 00:C0:4E:36:00:02 00:C0:4E:30:00:10 00:C0:4E:38:00:02 00:C0:4E:38:00:02 00:C0:4E:2F:63:1D 00:C0:4E:1C:FF:FD	Software Version v2.7c_beta2 (b1.6.2.1.2) v1.3c_beta4 (b1.2.1.6) v2.7b_beta2 (b1.6.2.1.2) v1.4c_b01.1.0A) v2.7b_beta2 (b1.6.2.1.2) v1.3c_b15.1.5) v2.7c_beta2 (b1.6.2.1.2) v2.7c_beta2 (b1.6.2.1.2)	ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE	
s area.	✓ Device 2C:00.6C ✓ Device 30:00:10 ✓ Device 20:00:10 ✓ Device 20:00:10 ✓ Device 20:00:10 ✓ Device 20:00:10	ES8510 ES7510 ES9528-XT ES8510-XT ES8508 ES8508-XT SH-8P (DB9) 4-EIP	P Addr 192166.11.103 192166.11.04 192168.11.05 192168.11.105 192168.11.106 192168.11.108 192168.11.10 192168.11.14 192168.11.198	MAC Address 00:C0-4E:2C-00-6C 00:C0-4E:34:00-08 00:C0-4E:36:00-12 00:C0-4E:38:00-02 00:C0-4E:38:00:00 00:C0-4E:2F:03:10 00:C0-4E:1C:FF:FD 00:C0-4E:39:00:23	Software Version v2.7c, beta2 (b1.6.2.12) v1.3c, beta4 (b1.0.2.16) v1.3c, bita4 (b1.0.10) v2.7b, beta2 (b1.6.2.12) v1.3c, (b1.1.6) v1.3c, (b1.6.1.2) NS-Link 8.04 EherNet/IP 1.2.0	ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE	
is area.	✓ Device 2C:00.6C ✓ Device 36:00.02 ✓ Device 36:00.02 ✓ Device 38:00.02 ✓ Device 12:FF:FD ✓ Device 12:FF:FD ✓ Device 17:FF:FB	ES8510 ES7510 ES9528-XT ES8510-XT ES8510-XT ES8508 ES8510-XT SH-8P (DB9) 4-EIP PRO-8P (DB9)	▲ IP Addr 192.168.11.103 192.168.11.003 192.168.11.005 192.168.11.005 192.168.11.005 192.168.11.107 192.168.11.101 192.168.11.14 192.168.11.20	MAC Address 00:C04E:2C:00.6C 00:C04E:23:00.03 00:C04E:36:00.02 00:C04E:36:00.02 00:C04E:36:00.02 00:C04E:2F:FE 00:C04E:2F:FE 00:C04E:2F:FE 00:C04E:27:FF:FE	Software Version v2.7c_beta2 (b1.6.2.12) v1.3c_beta2 (b1.6.2.12) v1.4a (b1.10.4) v2.7c_beta2 (b1.6.2.12) v1.3c (b1.41.6) v1.3c (b1.41.6) v1.3c (b1.41.6) v1.3c (b1.51.5) v2.7c_beta2 (b1.6.2.12) NS-Link 804 EtherNeVIP 12.0 NS-Link 918	ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE	
s area.		ES8510 ES7510 ES9528-XT ES8510-XTE ES7510-XT ES8508 ES8510-XT SH-8P (DB9) 4-EIP PRO-8P (DB9) RTS-4P (DB9)	▲ IP Addr 19216811103 19216811104 19216811105 19216811106 1921681110 19216811110 19216811110 19216811110 19216811110	MAC Address 00:C04E2C:006C 00:C04E340008 00:C04E340008 00:C04E3400010 00:C04E3400:00 00:C04E240310 00:C04E276310 00:C04E27FFID 00:C04E27FFID	Software Version v2.7c, beta2 (b1.6.2.12) v1.3c, beta4 (b1.6.2.16) v1.3c, bita4 (b1.10.4) v2.7c, beta2 (b1.6.2.12) v1.3c, (b1.4.1.6) v1.3c, (b1.4.1.6) v1.3c, (b1.4.1.6) v1.3c, (b1.5.1.5) v1.3c, (b1.5.1.5) v1.3c, (b1.4.1.6) v1.3c, (b1.6.1.2) NS-Link8.04 EherNet/IP 1.2.0 NS-Link9.18 SocketServer 9.18	ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE	
is area.	✓ Device 22:00:6C ✓ Device 34:00:08 ✓ Device 36:00:02 ✓ Device 36:00:02 ✓ Device 38:00:02 ✓ Device 38:00:02 ✓ Device 38:00:02 ✓ Device 38:00:02 ✓ Device 27:03:10 ✓ Device 21:7FF:FB ✓ Device 0570-000:05 ✓ Device 12:7FF:FB ✓ Device 12:7FF:FB ✓ Device 42:FF:FB	ES8510 ES7510 ES9528-XT ES8510-XTE ES8500 ES8510-XT ES8500 ES8510-XT SH-8P (DB9) 4-EIP PRO-8P (DB9) RT5-4P (DB9) RT5-4P (DB9) RT5-4P (C-30V)	▲ IP Addr 192168.11.03 192168.11.03 192168.11.05 192168.11.05 192168.11.07 192168.11.01 192168.11.01 192168.11.19 192168.11.20 192168.11.20 192166.11.20	MAC Address 00:C0:4E:2C:00-6C 00:C0:4E:36:00:02 00:C0:4E:36:00:02 00:C0:4E:38:00:02 00:C0:4E:38:00:02 00:C0:4E:38:00:02 00:C0:4E:2F0:31D 00:C0:4E:2F0:31D 00:C0:4E:2F0:320 00:C0:4E:2FFFF8 00:C0:4E:2FFFF8	Software Version v2.7c_beta2 (b16.2.12) v1.3c_beta4 (b1.2.16) v2.7b_beta2 (b16.2.12) v1.3c (b1.1.16) v1.3c (b1.1.1.6) v1.3c (b1.1.6) v1.3c (b1.2.12) NS-Link 8.04 EtherNet/P 1.2.0 NS-Link 9.18 SocketServer 9.35	ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE	
s area.	✓ Device 2C:00.6C ✓ Device 34:00:08 ✓ Device 36:00:02 ✓ Device 36:00:02 ✓ Device 38:00:02 ✓ Device 38:00:02 ✓ Device 34:00:00 ✓ Device 34:00:00 ✓ Device 10:FF:FD ✓ Device 10:FF:FD ✓ Device 07:FF:FB Ø Device 07:FF:FB Ø Device 07:FF:FB Ø Device 07:FF:FB Ø Device 10:FF:FB Ø Device 10:FF:F5	ES8510 ES9528-XT ES9528-XT ES9510-XT ES7510-XT ES8508 ES8510-XT ES8508 ES8510-XT SH-8P (DB9) RTS-4P (DB9) RTS-4P (DB9) RTS-4P (CB9) RTS-4P (2E)	▲ IP Addr 192166:11:03 192166:11:04 192166:11:04 192166:11:06 192166:11:06 192166:11:08 192166:11:08 192166:11:08 192166:11:09 192166:11:23 192166:11:23	MAC Address 00:C04E2C:00-6C 00:C04E360002 00:C04E360002 00:C04E360010 00:C04E380010 00:C04E384000D 00:C04E26310 00:C04E2767FF 00:C04E27FFF5 00:C04E27FFF5 00:C04E27FFF5	Software Version v2.7c, beta2 (b1.6.2.12) v1.3c, beta4 (b1.6.2.16) v1.3c, beta4 (b1.6.2.12) v1.3c, beta4 (b1.5.15) v1.3c, beta4 (b1.5.15) v1.3c, beta4 (b1.6.2.12) NS-Link8.04 DherNet/P1.2.0 NS-Link9.18 SocketServer 9.18 SocketServer 9.35	ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE	
er menu or toobar to add notes in	✓ Device 34:00:6C ✓ Device 34:00:08 ✓ Device 34:00:02 ✓ Device 36:00:02 ✓ Device 38:00:02 ✓ Device 38:00:02 ✓ Device 38:00:02 ✓ Device 37:00:02 ✓ Device 27:07:31:0 ✓ Device 97:00:00:36 ✓ Device 17:FF:FF	ES8510 ES9528-XT ES9528-XT ES9510-XT ES9510-XT ES9510-XT ES9510-XT SH-8P (D89) RTS-4P (D89) RTS-4P (D89) RTS-4P (D89) RTS-2P (2E) UP-1P (5V)	▲ IP Addr 192.168.11.103 192.168.11.003 192.168.11.005 192.168.11.005 192.168.11.007 192.168.11.007 192.168.11.01 192.168.11.20 192.168.11.20 192.168.11.20 192.168.11.20 192.168.11.20	MAC Address 00:C04E2C:006C 00:C04E340008 00:C04E3600:20 00:C04E3800:20 00:C04E3800:20 00:C04E3800:20 00:C04E3600:20 00:C04E26FFF0 00:C04E27FFF8 00:C04E27FFF8 00:C04E27FFF8 00:C04E27FF78	Software Version v2.7c_beta2 (b1.6.2.1.2) v1.3c_beta2 (b1.6.2.1.2) v1.3c_beta3 (b1.2.1.6) v1.3c (b1.4.1.6) v1.3c (b1.4.1.6) v1.3c (b1.4.1.6) v1.3c (b1.6.2.12) NS-Link 8.04 EhenNet/P1.2.0 NS-Link 9.18 SocketServer 9.35 SocketServer 9.35 BocketServer 9.35 BocketServer 9.35 SocketServer 9.35	ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE	
is area.	✓ Device 22:00.6C ✓ Device 34:00:03 ✓ Device 36:00:02 ✓ Device 36:00:02 ✓ Device 38:00:02 ✓ Device 38:00:02 ✓ Device 38:00:02 ✓ Device 38:00:02 ✓ Device 27:00:03 ✓ Device 1CFFFFD ✓ Device 1CFFFFE ✓ Device 07:FFFC ✓ Device 29:FF:F5 ✓ Device 15:FFFF ✓ Device 29:FF:F3 ✓ Device 15:FF:F5 ✓ Device 15:FF:F3 ✓ Device 15:FF:F3 ✓ Device 15:FF:F3 ✓ Device 15:FF:F3 ✓ Device 15:F3:F3	ES8510 ES9528-XT ES9528-XT ES9510-XT ES9510-XT ES8500 ES8510-XT SH-8P (DB9) A-EIP PRO-8P (DB9) RT5-4P (DB9) RT5-2P (2E) UP-1P (S90) UP-4P (DB9)	▲ IP Addr 192166:11.03 192166:11.04 192166:11.04 192166:11.06 192166:11.06 192166:11.08 192166:11.19 192166:11.23 192166:11.23 192166:11.23 192166:11.54	MAC Address 00:C04E240006 00:C04E240008 00:C04E340008 00:C04E340008 00:C04E360001 00:C04E360001 00:C04E36002 00:C04E2601 00:C04E2767E 00:C04E2767FE 00:C04E27FFF 00:C04E27FFF 00:C04E27FFF 00:C04E27FFF	Software Version v2.7c beta2 (b1.6.2.12) v1.3c beta4 (b1.6.2.16) v1.3c bita4 (b1.2.16) v1.3c bita5 (b1.6.2.12) v1.3c bita5 (b1.6.2.15) v2.7c beta2 (b1.6.2.12) NS-Link8.04 btenNet/P1.2.0 NS-Link9.18 SocketServer 9.18 SocketServer 9.35 EtherNet/P1 A.10 Modbus Server 4.04	ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE	
	✓ Device 34:00:6C ✓ Device 34:00:08 ✓ Device 34:00:02 ✓ Device 36:00:02 ✓ Device 38:00:02 ✓ Device 38:00:02 ✓ Device 38:00:02 ✓ Device 37:00:02 ✓ Device 27:07:31:0 ✓ Device 97:00:00:36 ✓ Device 17:FF:FF	ES8510 ES9528-XT ES9528-XT ES9510-XT ES9510-XT ES9510-XT ES9510-XT SH-8P (D89) RTS-4P (D89) RTS-4P (D89) RTS-4P (D89) RTS-2P (2E) UP-1P (5V)	▲ IP Addr 192.168.11.103 192.168.11.003 192.168.11.005 192.168.11.005 192.168.11.007 192.168.11.007 192.168.11.01 192.168.11.20 192.168.11.20 192.168.11.20 192.168.11.20 192.168.11.20	MAC Address 00-C04E2-C006C 00:C04E2400.60 00:C04E23600.10 00:C04E23600.10 00:C04E23600.10 00:C04E2603.10 00:C04E26703.10 00:C04E276750 00:C04E277FFE 00:C04E277FFE 00:C04E2747FFE 00:C04E217FFE 00:C04E215047A 00:C04E21305CD	Software Version v2.7c_beta2 (b1.6.2.1.2) v1.3c_beta2 (b1.6.2.1.2) v1.3c_beta3 (b1.2.1.6) v1.3c (b1.4.1.6) v1.3c (b1.4.1.6) v1.3c (b1.4.1.6) v1.3c (b1.6.2.12) NS-Link 8.04 EhenNet/P1.2.0 NS-Link 9.18 SocketServer 9.35 SocketServer 9.35 BocketServer 9.35 BocketServer 9.35 SocketServer 9.35	ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE ON-LINE	

- 3. Check the Comtrol ftp site to see if a later version is available by accessing the ftp subdirectory that contains the latest version of SocketServer.
 - View an ftp subdirectory that contains the latest version of SocketServer: <u>http://</u> <u>downloads.comtrol.com/dev_mstr/rts/software/socketserver</u>.

downloads.comtrol.com -/dev_mstr/rts/software/socketserver/ (To Parent Directory) 10/14/2015 10:54 AM 148450 1800456 SocketServer History.pdf 9/2/2014 9:50 AM 172465 DeviceMaster Binary Format.pdf 5/7/2015 12:44 PM 92973 DeviceMaster ProductNotice.pdf 5/7/2015 11:10 AM <dir> help 10/13/2015 5:27 PM 1188657 socketServer-10.06.cmt1

Note: The DeviceMaster PRO, DeviceMaster RTS, and DeviceMaster Serial Hub all use the same firmware, although the above paths point to the location of the DeviceMaster RTS file.

4. If the version on the web site is later than the version on the DeviceMaster, download the file, and then go to <u>Uploading SocketServer with PortVision DX</u> on Page 42.

If the SocketServer version on the DeviceMaster is current, you are ready to continue the installation and configuration process.

Uploading SocketServer with PortVision DX

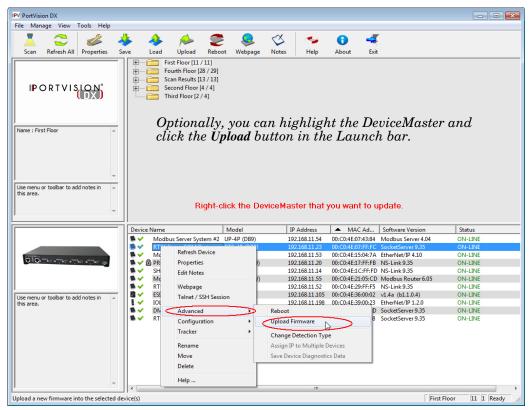
Use this section to upload a newer version of <u>SocketServer</u> on the DeviceMaster using PortVision DX. Technical Support recommends updating SocketServer before any further configuration to avoid configuration problems.

You can use this procedure if your DeviceMaster is connected to the host PC, laptop, or if the DeviceMaster resides on the local network segment.

1. Make sure that you have downloaded the latest SocketServer version from:

http://downloads.comtrol.com/dev_mstr/rts/software/socketserver.

- 2. If necessary, open PortVision DX: Comtrol > PortVision DX or use the desktop shortcut.
- 3. Right-click the DeviceMaster or DeviceMasters for which you want to update, click Advanced > Upload Firmware, browse to the SocketServer .cmtl file, and then click Open.



If the **Detection Type** is set to **REMOTE**, you may want to change it to **LOCAL**. The DeviceMaster *Status* on a DeviceMaster that is set to **REMOTE** displays in blue: **ON-LINE** (TCP).

- 4. Click **Yes** to the *Upload Firmware* message that warns you that this is a sensitive process. It may take a few moments for the firmware to upload onto the DeviceMaster. The DeviceMaster reboots itself during the upload process.
- 5. Click **Ok** to the advisory message about waiting to use the device until the status reads **ON-LINE**. In the next polling cycle, PortVision DX updates the *Device List* pane and displays the new SocketServer version or right-click the DeviceMaster and click **Refresh**.
- 6. If the upload fails, reset the Bootloader timeout to 60 seconds and then repeat <u>Steps 3</u> through 5. For procedures, see <u>Changing the Bootloader Timeout</u> on Page 114.

You are now ready to continue the installation and configuration process.

- Device Driver (NS-Link) Installation on Page 47
- <u>Socket Port Configuration</u> on Page 61

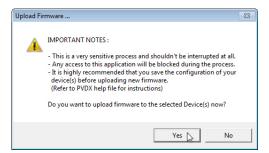
Customizing PortVision DX

You can customize how PortVision DX displays the devices. You can even create sessions tailored for specific audiences. You can also add shortcuts to other applications using Tools > Applications > Customize feature.

The following illustrates how you can customize your view.

PV PortVision DX							.
File Manage View Tools Help							
Scan Refresh All Properties Save	Load Upload Rebo	ot Webpage	Notes Help	l 🚽			
Scall Relies All Properties Save		or weapage	· · · ·	About			
IPORTVISION®	First Floor [1] / 11] ●	10] / 3] IT [1 / 1] IS P5534 Camera M T T T E System	the <i>L</i> See t proce	<i>Device List</i> pa the PortVision edures on org	a DX help syste anizing your de iew in PortVisio	m for vices and	E
		ort COM Ports [0 /		1			
	Device Name	Model	 IP Addr 		Software Version	Status	
	ES9528-XT	ES9528-XT	192.168.11.105			ON-LINE	
	SH8 Console Port COM P		192.168.11.14	00:C0:4E:1C:FF:FD		ON-LINE	
	IOLM-4-EIP #1	4-EIP	192.168.11.198			ON-LINE	
	PRO8 Console Port COM RTS4 Spare COM Ports	RTS-4P (DB9)	192.168.11.20 192.168.11.23	00:C0:4E:17:FF:FB	SocketServer 9.30	ON-LINE ON-LINE	
	RTS4 Spare COM Ports RTS-1P Printer#10	RTS-1P (5-30V)	192.168.11.23		SocketServer 9.30 SocketServer 9.35	ON-LINE ON-LINE	
	RTS-IP Printer#10	RTS-2P (2E)	192.168.11.40	00:C0:4E:42:FF:F8 00:C0:4E:29:FF:F5		ON-LINE ON-LINE	
	Modbus/TCP	UP-1P (5V)	192.168.11.52	00:C0:4E:29:PP:PS		ON-LINE	
	Modbus Server System #2		192.168.11.54		Modbus Server 4.04	ON-LINE	
	Modbus Server System #2	UP-1P (5-30V)	192.168.11.55		Modbus Server 4.04	ON-LINE	
	DM-LT16 PM Lab	DM-LT16	192.168.11.60		SocketServer 9.33	ON-LINE	
			De	evice List	Pane		
	•						•
For Help, press F1					Γ	First Floor 1 Read	y .

See the PortVision DX Help system for detailed information about modifying the view. For example, the above screen shot illustrates devices layered in folders.



Accessing DeviceMaster Documentation from PortVision DX

You can use this procedure in PortVision DX to <u>download</u> and <u>open the previously downloaded documents</u> for the DeviceMaster. You can also check to see if you have the latest version of the documentation using PortVision DX.

How to Download Documentation

Use this procedure to initially download a document or documents.

- 1. If necessary, open PortVision DX: **Comtrol > PortVision DX** or use the desktop shortcut.
- 2. Click Help > Documentation.
- 3. Optionally, click the **DOWNLOAD THE CURRENT DOCUMENTATION CATALOG ONLINE** button to make sure that the latest documentation is available to PortVision DX.

Documentat	ion	
Once yo	use the following drop-down menus to locate the u are there, you will be able to either open the lo st edition.	
Ca	ategory :	•
Subca	ategory :	_
Docume	entation :	
	Open the local copy of this document	Download the latest edition from the web
	Browse the folder for already d	ownloaded documentation
	DOWNLOAD THE CURRENT DOCUM	

Hel	p
	Help Contents F1 Search
	Documentation
	ہی About PortVision DX

- 4. Select the product Category from the drop list.
- 5. Select the document you want to download from the Documentation drop list.
- 6. Click the Download the latest edition from the web button.

ocumentat	ion
Once yo	use the following drop-down menus to locate the documentation you need. Nu are there, you will be able to either open the local copy, if any, or download st edition.
Ca	ategory : DeviceMaster RTS
Subca	ategory : 📃 🔻
Docume	entation: DeviceMaster Installation and Configuration Guide
	Open the local copy of this document Download the latest edition from the web
	DOWNLOAD THE CURRENT DOCUMENTATION CATALOG ONLINE

Note: It may take a few minutes to download, depending on your connection speed. The document opens automatically after it has downloaded.

7. Click Close if you have downloaded all of the documents that you wanted.

How to Open Previously Downloaded Documents

Use the following procedure to access previously downloaded documents in PortVision DX.

- *Note:* Optionally, you can browse to the Program Files (x86) > Comtrol > PortVision DX > Docs subdirectory and open the document.
- 1. If necessary, open PortVision DX: Comtrol > PortVision DX or use the desktop shortcut.
- 2. Click **Help > Documentation**.
- 3. Click the Open the local copy of the document button to view the document.

Documentation		×
	following drop-down menus to locate the documentation you need. ere, you will be able to either open the local copy, if any, or download n.	Close
Category Subcategory Documentation	;	-
Oper	Download the latest edition from the web Browse the folder for already downloaded documentation DOWNLOAD THE CURRENT DOCUMENTATION CATALOG ONLINE	

- **Note:** If the document fails to open, it may be that your browser has been disabled. You can still access the document by clicking the **Browse the folder for already downloaded documentation** button and opening the document with your custom browser.
- 4. Click **Close** in the *Documentation*... popup, unless you want to open or download other documents.

Device Driver (NS-Link) Installation

This section discusses the following topics:

- *Linux Installations* on Page 47
- <u>Windows Installations</u> on Page 49

Overview

The following subsections discuss procedures that need to be done before installing and configuring the NS-Link device driver.

Before Installing the NS-Link Driver

Before installing the NS-Link device driver for the Linux and Windows operating systems, the following conditions must be met:

- The DeviceMaster is connected to the network and powered on (*Hardware Installation* on Page 13).
- The network information has been configured in the DeviceMaster (*Configuring the Network Settings* on Page 38).
- Checked to see if the latest version of SocketServer resides on the DeviceMaster (<u>Checking the</u> <u>SocketServer Version</u> on Page 41 using PortVision DX or you can open your browser, enter the DeviceMaster IP address to view the version on the Server Status page.
- If necessary, uploaded the latest version of SocketServer (*Uploading SocketServer with PortVision DX* on Page 42.
- **Note:** Technical Supports recommends that you update to the latest version of SocketServer before installing any NS-Link device driver.

After NS-Link driver installation and configuration, the same ports can be configured as TCP/IP sockets using an NS-Link version of the SocketServer web page (*Socket Port Configuration* on Page 61).

Linux Installations

Download the latest device driver for Linux: <u>fhttp://downloads.comtrol.com/dev_mstr/rts/drivers/linux</u>.

 downloads.comtrol.com - /dev_mstr/rts/drivers/linux/

 [To Parent Directory]

 6/28/2016
 2:05 PM

 115464
 devicemaster-linux-7.15.tar.gz

 8/12/2016
 2:27 PM

 831
 dm kernel versions.txt

Note: Although the download link displays rts in the path, the driver supports the DeviceMaster models discussed in this User Guide.

Refer to the $\ensuremath{\textbf{README}}$ file packaged with the Linux driver for driver installation and configuration procedures.

Before you install the Linux NS-Link device driver:

- 1. Make sure that you have programmed an appropriate network address into the DeviceMaster.
- 2. Make sure that you verify that you have the latest version of SocketServer loaded on the DeviceMaster. If you do not want to install PortVision DX (Page 35) to check the SocketServer version, you can:
 - a. Open SocketServer to check the version by opening your browser and entering the IP address of the DeviceMaster.

Comtrol' Ho	ome Port Network	Diagnostics	System	Help		Log
				_		_
)eviceMaster I	info					
Firmware	e: SocketServer 11	.20				
Hostname	e: RTS-4					
MAC Address	s: 00:c0:4e:07:ff:f	ic 🛛				
System Uptime	e: 00:00:03					
IPv4 Config	g: Static					
Addres	s: 10.0.0.23					
Netmas	k: 255.255.0.0					
Gateway	y: 0.0.0.0					
IPv6 Config	g: Disabled					
Address	s: ::/0					
Gateway	y: ::					
					© Copyright Com	trol C

b. Check the download site for the latest version: $\frac{http://downloads.comtrol.com/dev_mstr/rts/software/SocketServer.}{bttp://downloads.comtrol.com/dev_mstr/rts/software/SocketServer.}$

c. If necessary, download the latest version.

Note: Technical Supports recommends that you update to the latest version of SocketServer before installing an NS-Link device driver.

3. Install and configure the Linux device driver using the Readme file packaged with the driver.

Windows Installations

This subsection provides an installation overview for the NS-Link device driver for Windows. For detailed installation and configuration information, see the <u>DeviceMaster Device Driver (NS-Link) User Guide for</u> <u>Windows</u>, which is available on the <u>download site</u>.

Supported Operating Systems

The NS-Link device driver for Windows supports Windows 2008 R2 through Windows 10.

If you are updating the driver or need to remove the NS-Link device driver, you can refer to the <u>DeviceMaster</u> <u>Device Driver (NS-Link) User Guide</u> or the help system.

Note: Administrative privileges are required to install device drivers on Windows systems.

Installation Overview for Windows

The following NS-Link device driver installation and configuration procedures are discussed in this subsection:

- Install the NS-Link device driver and *DeviceMaster Drivers Management Console* using the *Installation Wizard*.
- Configure the COM ports using the *DeviceMasterDrivers Management Console*.
- Configure device properties using the DeviceMaster Drivers Management Console.

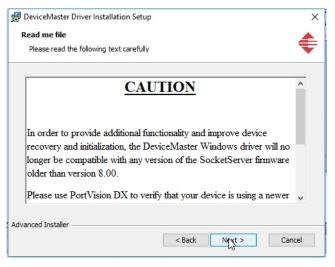
NS-Link for Windows Installation

1. If necessary, locate the NS-Link device driver and make it available to the host system. The driver assembly is available at:

http://downloads.comtrol.com/dev_mstr/rts/drivers/win7.

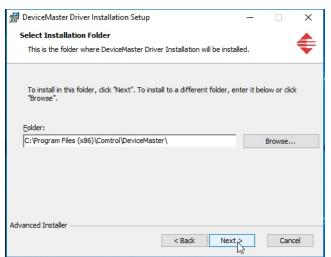
Note: Although the download link displays win7 in the path, the driver supports the previously listed <u>Windows operating systems</u>.

- 2. Execute the driver assembly **DeviceMaster_Windows_x.xx.exe** file and click **Next** to start the installation.
- 3. If included in this driver version, read the caution or notice:

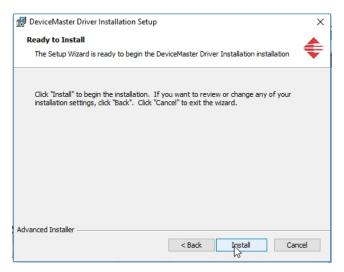




4. Click Next to install in the default location.



5. Click Install



6. Leave the Launch DeviceMaster Driver Installation box checked.

If you do not check this box, you can use the shortcut under the **Start** button at: **Comtrol > DeviceMaster Driver Installation Wizard**.

7. Click **Finish** to complete the installation of the wizard.



8. Click Next to start the driver installation.



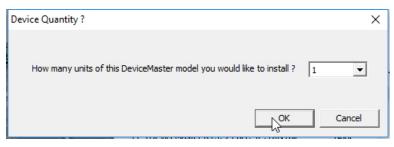
9. Click Install and Next.



10. Select the DeviceMaster model that you are installing from the list.

Comtrol Driver Installation w	izard		×
	install a New Comtrol Dev	ice	
	You are about to install a new Comtrol Device Drive computer.	er on this	
	As part of this process all previous installations of updated as well.	this driver wil	lbe
	Please select the DeviceMaster models you want to identify their quantities as well.	o install and	
Distant of the state of	DeviceMaster Model	Quantity	
HOW AL	V DeviceMaster RTS, 1 Port	1	· · · · · · · · · · · · · · · · · · ·
	DeviceMaster RTS, 1 Port, 1E, DIN rail	None	
	DeviceMaster RTS, 1 Port, DB9, 1E, DIN rail	None	
	DeviceMaster RTS, 2 Port, 1E, DIN rail	None	~
	DaviesMaster DTC 2 Dert DR0 1E DTM roll	Nono	
COMTROL	Click Next to continue or Cancel to exit this Wizard		
	<back next=""> Procee</back>	d Car	ncel

11. Enter the quantity of this DeviceMaster model that you want to install and click Ok.



12. Repeat Steps 10 and 11 for each DeviceMaster that you are installing and then click Next.

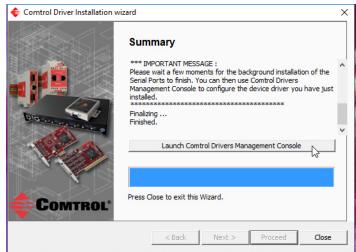
	Install a New Comtrol Dev	ice	
	You are about to install a new Comtrol Device Drive computer.	er on this	
	As part of this process all previous installations of updated as well.	this driver wil	l be
Distance of the second	Please select the DeviceMaster models you want to identify their quantities as well.	Ouantity	^
Month A	DeviceMaster RTS, 1 Port	1	
	DeviceMaster RTS, 1 Port, 1E, DIN rail	None	
	DeviceMaster RTS, 1 Port, DB9, 1E, DIN rail	None	
	DeviceMaster RTS, 2 Port, 1E, DIN rail	None	
	DoviceMaster DTC 2 Dort DP0 15 DTM sail	Nees	~
COMTROL	Click Next to continue or Cancel to exit this Wizard		

13. Click Proceed.

Comtrol Driver Installation w	vizard	×
	Summary	
	Driver Package : DeviceMaster Selected Action : Install Device(s) : 1 DeviceMaster Unit(s)	^
BO- CO	IT IS HIGHLY RECOMMENDED TO CLOSE ANY ACTIVE SERIAL PORT/APPLICATION BEFORE YOU PROCEED. FAILURE TO DO SO WILL RESULT IN DATA LOSS !	
	Launch Comtrol Drivers Management Console	
Comtrol'	Click Proceed to continue or Cancel to exit this Wizard.	
	< Back Next > Proceed Ca	ncel

You may see the popup at the right for each port, depending on the operating system.

14. Return to the *Installation Wizard* and click Close.



15. Go to the next subsection for NS-Link driver configuration procedures.

Configuring the NS-Link Driver for Windows

This subsection provides a configuration overview for the NS-Link driver. For detailed information or if the DeviceMaster is on a different physical segment, refer to the help system or the *DeviceMaster Device Driver* (*NS-Link*) User Guide, which is available on the <u>download site</u>.

The DeviceMaster must be connected to the local network segment or directly to a NIC on the host system to operate in MAC mode to perform the following configuration steps.

- 1. Access the *Drivers Management Console* using the desktop shortcut or under the start menu > Comtrol > DeviceMaster Driver Management Console.
- 2. Highlight the *Device Name* of the DeviceMaster that you want to configure.
- 3. Select the MAC address from the drop-down list or enter the address from the MAC address label on the DeviceMaster. If you programmed the IP address using PortVision DX, the IP address displays in the IP Mode text box after you select the MAC address.

Comtrol Drivers Management Console		? ×
DeviceMaster DeviceMaster PRO, 8 Port Section 2010 (COM3)	General Advanced	
Section (COM3) Section (COM3) Section (COM4) Port 03 - Spare port (COM4)	MAC Mode D0 C0 4E # # # Fetch 1 Fetch 1	IP Address
Port 04 (COM5) ES8510 (COM103) ES9528-XT V2 #3 (COM113)	O IPV4 Mode 00 C0 4E 15 0C 8B Networ O IPV6 Mode 00 C0 4E 15 20 66 00 C0 4E 20 0A 7C	rk Settings
	Enable SSL Md 00 C0 4E 21 05 CD 00 C0 4E 21 EE 02 00 C0 4E 41 FF FA	tificates
Port 01 (COM8)	Device Settings 00 C0 4E 41 FF FF 00 C0 4E 42 02 75 00 C0 4E 42 02 FF F8 00 C0 4E 42 FF F8 00 C0 4E 42 FF FP	
J Port 01 (COM6) J ES8520-XT (COM116) J ES8814-XT (COM117)	User-F(00 C0 4E # # #) 1 Port Keep Alive Timeout (seconds): 120 (Default: 120	
ES7810-XT (COM118)	TCP Timeout Multiplier: 1 (Default: 10)	
ES9528-XT V2 (COM112)	Scan Rate (ms): 0 (Default: 10)	
→ ES7510-XT #1 (COM107) → ES7528 (COM101) → ES7510-XT (COM111)	Verbose Event Log (Troubleshooting Only)	
ES7510-XT (COM111) ES9528-XT (COM105) ES8510-XTE (COM106)		Defaults
Comtrol Drivers Management Console version 4.05 Copyright © Comtrol Corporation. All rights reserved.	Save Configuration Load Configuration OK Cancel	Apply Help

Note: If you enter the MAC address, make sure that you use the correct format: 00 C0 4E xx xx xx. A space must separate each pair of digits. The MAC address is located on a label on the DeviceMaster or you can view it using PortVision DX.

If the appropriate MAC address is not displayed in the drop-down list, then it can be one of the following reasons:

- Not on the same network segment
- DeviceMaster not powered on or connected
- The wrong DeviceMaster model was selected during the driver installation
- Device failure

4. Click Apply to program the driver with the MAC address of the DeviceMaster or Ok to save the change and close the *Drivers Management Console*.

If you do not Apply the changes before leaving this screen, you will be prompted to Apply, Ignore, or Cancel the changes.

Comtrol Drivers Management Console	Сом	? >
DeviceMaster Port 01 (COM3) Port 01 (COM3) Port 03 - Spare port (COM4) Port 04 (COM5) The red frame indicates that changes have not been applied. DeviceMaster RTS, 1 Port Port 04 (COM5) DeviceMaster RTS, 4 Port	General Advanced Network Connection Mode Image: Connection Mode Image: Mac Mode Image: Connection Mode Image: Image: Image: Connection Mode Image: Connection Mode Image: Image: Image: Image: Connection Mode Image: Connection Mode Image: Image: Image: Image: Image: Connection Mode Image: Connection Mode Image: Ima	gs
Port 01 (COM6) ES8520-XT (COM116) ES8520-XT (COM117) ES8520-XT (COM118) DeviceMaster Serial Hub, 8 Port ES9528-XT V2 (COM112) Dead Port (COM500) ES7510-XT (COM110) ES9528-XT (COM111) ES9528-XT (COM111) ES9528-XT (COM105) ES9528-XT (COM105) Comtrol Drivers Management Console version 4.05 Copyright © Comtrol Drivers Management Console version 4.05	User-Friendly Device Name: DeviceMaster RTS, 1 Port Keep Alive Timeout (seconds): 120 (Default: 120) TCP Timeout Multiplier: 1 (Default: 1) Scan Rate (ms): 10 (Default: 10) Verbose Event Log (Troubleshooting Only) Default: Save Configuration Load Configuration OK Cancel Areply	faults

- Now that the MAC address has been associated to the DeviceMaster, you can use the Network Settings screen to:
 - Change the IP address, set the DeviceMaster to DHCP, or Disable IP communications using the Network Settings button
 - Reboot the DeviceMaster on the General tab
 - Access network statistics on the Advanced tab

5. If you want use **IP mode** and the **IP** address is configured for your network, click the **IPv4** or **IPv6** Mode radio button and click **Apply**. If you want to use **SSL** Mode, you must set the DeviceMaster to **IP mode**.

	> `	EAC.			Comtrol
DeviceMaster		General	Advanced	9 111 (C)	
DeviceMaster PRO, 8 Port Port 01 (COM3)		Network Connect	an Mada		
ES8508 (COM108)			00 C0 4E 42 FF F8		Fetch IP Address
Port 03 - Spare port (COM4)		O MAC Mode			Fetch IP Address
Port 04 (COM5)		IPv4 Mode	10.0.0.40		Network Settings
ES8510 (COM103)		O IPv6 Mode	FE80::2C0:4EFF:FE4	2:FFF8	
NXP-1P (COM17)		Enable SSL M	lode		Reboot Device
ES8508F-MM (COM115)					Certificates
DeviceMaster RTS, 1 Port DeviceMaster RTS, 1 Port		Device Settings			
DeviceMaster RTS, 4 Port			Device Name:	DeviceMaster RTS, 1	Port
Port 01 (COM6)		User-	Friendly Device Name:	DeviceMaster RTS, 1	Port
ES8520-XT (COM116)					
ES8814-XT (COM117)		Keep Ali	ve Timeout (seconds):	120 (D	efault: 120)
DeviceMaster Serial Hub, 8 Port			CP Timeout Multiplier:	1 (D	efault: 1)
ES9528-XT V2 (COM112)			Scan Rate (ms):	10 ~ (0	efault: 10)
Dead Port (COM500)					
ES7510-XT #1 (COM107) ES7528 (COM101)			Verbose Event Log	(Troubleshooting	Only)
S7510-XT (COM101)					
ES9528-XT (COM105)					Defaults
ES8510-XTE (COM106)	~				

- 6. Optionally, click the Network Settings button and click Modify to make any network settings changes for DHCP or MAC mode (Disable IP).
- 7. Optionally, click Enable SSL Mode if you want to configure secure COM ports.

The DeviceMaster must be configured using IP Mode (IPv4 or IPv6) before you can Enable SSL Mode.

If **SSL Mode** is enabled, TCP connections that carry data to/from the serial ports are encrypted using SSL or TLS security protocols. This includes the following:

- TCP connections to the per-serial-port TCP ports (default is 8000, 8001, 8002, ...) are encrypted using SSL/TLS.
- TCP connections to TCP port 4606 on which the DeviceMaster implements the Comtrol proprietary serial driver protocol are encrypted using SSL/TLS.
- Since SSL/TLS can not be used for either UDP data streams or for the Comtrol proprietary MAC mode Ethernet driver protocol, both UDP and MAC mode serial data transport features are disabled.

In addition to encrypting the data streams, it is possible to configure the DeviceMaster so that only authorized client applications can connect using SSL/TLS.

For this option to function, you must also Enable Secure Data Mode in the NS-Link web page.

Note: See the help system or the <u>DeviceMaster NS-Link User Guide for Windows</u> if you need additional information on SSL and the corresponding options.

- 8. If you are using a server certificate, click the Certificates button.
 - a. Click the Server Certificate check box if you want to enter a Server Certificate.
 - b. Enter the name in the Server Certificate text box.
 - c. If you are using a client certificate, click the drop list and browse to the appropriate client certificate file.
 - d. Click the Ok button to close the Certificates pop up window.

- 9. Configure the remainder of the device properties:
 - a. If desired, change the User-Friendly Device Name.
 - b. Optionally, set a different **Keep Alive Timeout** period. You can set the amount of time in seconds that this DeviceMaster waits until it closes this connection and frees all the ports associated with it.
 - c. Optionally, set the TCP Timeout Multiplier value.
 - d. Optionally, click a different Scan Rate (ms).
 - e. Optionally, click Verbose Event Log if you want to log additional DeviceMaster information into the event log.
 - f. After making your changes, click **Apply** if you have additional configuration procedures or click **Ok** if you have completed configuring your DeviceMaster.

Note: You can refer to the help system if you need information about any of the options or features.

10. Optionally, you can click the Advanced tab and verify that the *Device Status* message indicates that the DeviceMaster is active and Ok.

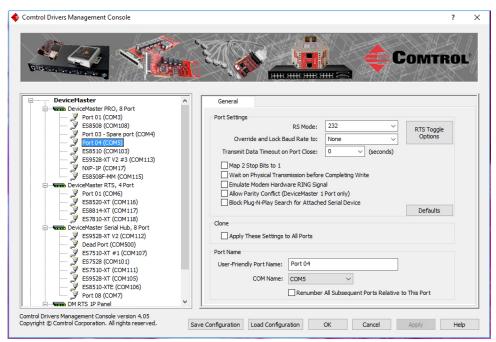
Comtrol Drivers Management Console	?	×
	ROI	
General Advanced		
ESSID (COM103) Device Status		
ES9528-XT V2 #3 (COM113)		
ESSSOR-MM (COM115)		
History		
S8520-XT (COM116)		
57510-XT (COM118)		
Network Statistics		
ES9528-XT V2 (COM112)		
PC Network Interface Details		
ES7528 (COM101) Device Network Interface Details		
ES7510-XT (COM111)		
→ y ES9526×1 (COM105) → y ES8510-YTE (COM106)		
Port 08 (COM7)		
DMRTS IP Panel		
Port 01 (COM8) RocketPort Infinity/Express		
B RocketPort RocketPort RocketPort		
Comtrol Drivers Management Console version 4.05 Copyright © Comtrol Corporation. All rights reserved. Save Configuration Load Configuration OK Cancel Apply	Help	

11. Go to the next subsection to configure COM port properties.

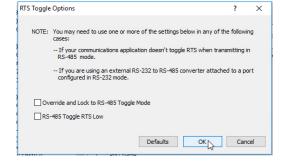
Configuring COM Port Properties for Windows

The following is a COM port properties configuration overview. Use the <u>DeviceMaster Device Driver (NS-Link)</u> <u>User Guide</u> or the NS-Link **Help** system for detailed configuration information. You can download the NS-Link User Guide from the download site: <u>http://downloads.comtrol.com</u>.

1. Highlight the first port you want to configure.



- 2. Complete the screen appropriately for the serial device that you plan on connecting to the port and click the Ok button.
 - a. Select the appropriate communications mode.
 - b. Enable the features that you want to use.
 - c. Optionally, click the **RTS Toggle Options** button:
 - If your communications application does not toggle RTS when transmitting in RS-485 mode.
 - If you are using an external RS-232 to RS-485 converter, which is attached to a port that is configured for RS-232.
 - d. Click the appropriate options for your environment.
 - e. Click **OK** to save the changes and return to the port **General** tab.
- 3. If desired, click the **Clone** check box to set all of the ports on this DeviceMaster to these characteristics.



- 4. Optionally, change the User-Friendly Port Name.
- 5. If desired, select a different COM Name (COM port number). The drop-down list displays (in use) next to COM port numbers that are already in use in this system. Do not duplicate COM port numbers as this will cause the ports to not function.
- 6. Click Apply to save these changes.

Note: If you selected RS-422 mode, make sure that there is not a device attached to the port and click Ok.

- 7. Highlight the next port that you want to configure and perform <u>Steps 1</u> through 6.
- 8. Refer to <u>Connecting Serial Devices</u> on Page 87 to attach your serial device.

9. Optionally, you may need to configure one or more ports for socket mode (<u>Socket Port Configuration</u> on Page 61).

Enabling Secure Data Mode

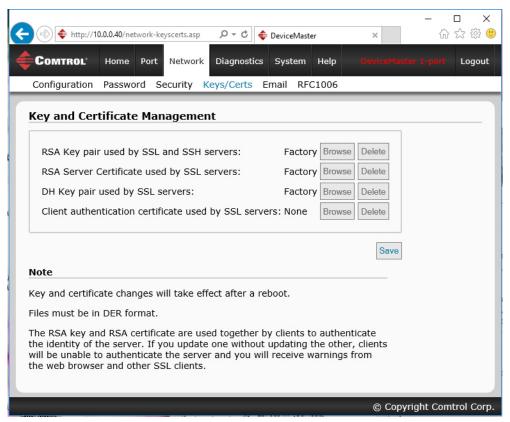
In addition to enabling SSL Mode in the driver, you must Enable Secure Data Mode in the NS-Link web page. Use the following procedure to implement the Enable Secure Data Mode option.

- 1. Access the NS-Link web page using one of these methods:
 - Open your web browser, enter the IP address, and press Enter.
 - Right-click the DeviceMaster in the *Device List* pane in PortVision DX and click Webpage.
- 2. Click Network | Security.
- 3. Click Enable Secure Data Mode and Save.

Security Set	tings						_
	nable Secur	e Data Mo	de				
	nable Secur	e Config M	ode				
✓ E	nable Telne	t/ssh					
🗆 E	nable Monit	oring Secu	re Data via T	lenet			
✓ E	nable SNMF						
SSLv3.0 V	linimum Alle	owed SSL/	LS Version				
□ A	llow TCP co	nnections o	only from the	address	blocks belov	N	
[Block	Address / V)				
lote						Save	
he address blo ddress and m	ask width se	parated by	a slash.	·	-		
or IPv4: a ma			ines a single fines 4, a wic				

4. Click Keys/Certs to configure your security key and certificate.

5. Click the appropriate Browse button to locate your key or certificate and click Save when you are done



Click the Help button if you need information about key and certificate management.

Socket Port Configuration

This section provides an overview of SocketServer and provides basic operating procedures. SocketServer and DeviceMaster security are discussed in detail in <u>DeviceMaster Security</u> on Page 65.

Note: Technical Supports recommends that you update to the latest version of SocketServer before installing an NS-Link device driver or configuring socket ports.

SocketServer Overview

SocketServer is the name of the TCP/IP socket web page that is integrated in the firmware that comes preinstalled on your DeviceMaster. When you install an <u>NS-Link device driver</u>, an NS-Link version of SocketServer loads on the DeviceMaster.

The SocketServer home page (*Server Info*) provides basic information about the DeviceMaster including whether it is functioning in socket mode (SocketServer) or in NS-Link (driver). See <u>SocketServer Architecture</u> on Page 62 for more information about socket port support.

The following menus are available in the web interface:

- **Port**, which includes the following pages:
 - **Port Overview** of all of the serial port settings
 - **Port Configuration** for each port that includes Serial, TCP connection, and UDP connection configuration capabilities
 - Network, which includes the following pages:
 - Configuration for general, IPv4 and IPv6 settings (after initial configuration)
 - Password to set a device password
 - <u>Security</u>, which is discussed in detail starting on Page 65
 - Keys/Certs to manage security keys and certificates
 - Email for notification services
 - **RFC1006** (ISO over TCP)
- **Diagnostics**, which includes:
 - System Log
 - Port Monitor
- **System**, which includes:
 - Update Firmware
 - Configuration File
 - Device Snapshot
 - Restore Defaults
 - Reboot

Note: For socket service configuration procedures or information, see the web page Help system.

Web Page Help System

The web page *Help* system is available separately for your convenience. The web page Help system contains detailed information and configuration procedures for each mode discussed in <u>SocketServer Architecture</u> on Page 62.

The *Help* system for the web page is available at: <u>http://downloads.comtrol.com/dev_mstr/rts/software/</u><u>socketserver/help/ssvr_help.zip</u>.

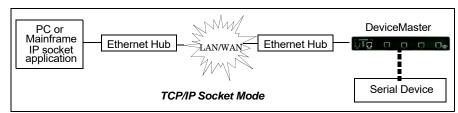
To use the help system:

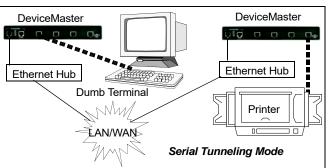
- 1. Unzip the files in a folder.
- 2. Open the ssvr_help.htm file.
- 3. Use your browser find function to locate the option or information for which are searching.

SocketServer Architecture

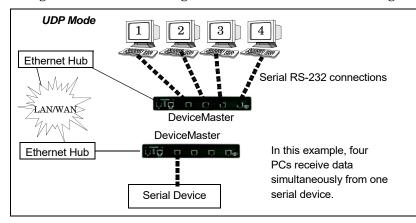
TCP/IP socket mode operation is used to connect serial devices with an application that supports TCP/IP socket communications addressing.

Serial tunneling mode is used to establish a socket connection between two DeviceMasters through an Ethernet network.





UDP mode is designed for applications that need faster data transmission, or that make use of UDP's broadcast capabilities. UDP differs from TCP in that a UDP transmission does not first require a connection to be opened before sending data and the receiving device does not issue acknowledgments to the sender.



Accessing Socket Configuration

There are several ways to access the socket configuration pages. Use the method that fits your environment best.

- Web Browser
- PortVision DX

Web Browser

To access the socket configuration web interface for the DeviceMaster, follow this procedure.

- 1. Start your web browser.
- 2. Enter the IP address of the DeviceMaster in the URL field.

Note: If you do not know the IP address, you can view and highlight the IP address in PortVision DX and click the **Webpage** button.

- 3. If necessary, enter admin as the *username*, your password, and then click the Login button.
- 4. Click the **Port** menu.
- 5. Click the port number that you want to configure socket port settings (serial, TCP connection configuration, and UDP connection configuration).
- Note: Refer to the web page Help system, if you need information about configuring sockets or serial tunneling, which contains detailed configuration procedures and descriptions for all fields. See <u>Web Page Help</u> <u>System</u> on Page 62 for information about downloading the help file separately.
- 6. After changing the appropriate settings for your environment, click Save.
- 7. Click the Network tab to access the following pages if you need to configure additional settings:
 - Configuration page to change the network settings.
 - Password page to configure a password for the DeviceMaster.
 - Security page to enable DeviceMaster security.
 - Keys/Certs page to configure security certificates and keys.
 - Email page to configure email notification services.
 - **RFC1006** page to configure RFC1006 settings.

PortVision DX

There are several ways to access the socket configuration page for the DeviceMaster using PortVision DX.

- 1. If necessary, start PortVision DX, right-click the DeviceMaster that you want to configure, and click Webpage.
- 2. Follow <u>Steps 3</u> through 7 from the previous procedure above (<u>Web Browser</u>).

SocketServer Versions

The <u>SocketServer Overview</u> discusses the that the default SocketServer web page is the same as the NS-Link web page. If the NS-Link driver is not running (not installed or disabled), SocketServer loads when you open a web browser session.

		-	System	Help	DeviceMaster 4-port	Lo
eviceMaster In	fo					
Firmware:	SocketServer 11.20					
Hostname:	RTS-4					
MAC Address:	00:c0:4e:07:ff:fc					
System Uptime:	00:00:03					
IPv4 Config:	Static					
Address:	10.0.0.23					
Netmask:	255.255.0.0					
Gateway:	0.0.0.0					
IPv6 Config:	Disabled					
Address:						
Gateway:	::					

Note: The top illustration shows the web page before an NS-Link device driver installation and the bottom illustration shows the web page after a device driver installation.

Your SocketServer or NS-Link version may be different than these examples.

COMTROL Hon	ne Port Network	Diagnostics	System	Help	Logout
DeviceMaster In	fo				
Firmware:	NS-Link 11.17.02				
Hostname:	SerialHub8				
MAC Address:	00:c0:4e:1c:ff:fd				
System Uptime:	21 days 00:39:40)			
IPv4 Config:	Static				
Address:	10.0.0.14				
Netmask:	255.255.0.0				
Gateway:	0.0.0.0				
IPv6 Config:	Disabled				
Address:	::/0				
Gateway:	::				

DeviceMaster Security

This subsection provides a basic understanding of the DeviceMaster security options, and the repercussions of setting these options. See <u>Removing DeviceMaster Security Features</u> on Page 169 if you need to reset DeviceMaster security options. See <u>Returning the DeviceMaster to Factory Defaults</u> on Page 171 if you want to return the DeviceMaster settings to their default values.

Understanding Security Methods and Terminology

The following table provides background information and definitions.

	Term or Issue Explanation				
	If configured with a CA certificate, the DeviceMaster requires all SSL/TLS clients to present an RSA identity certificate that has been signed by the configured CA certificate. As shipped, the DeviceMaster is not configured with a CA certificate and all SSL/TLS clients are allowed.				
CA (Client Authentication certificate) †	This uploaded CA certificate that is used to validate a client's identity is sometimes referred to as a <i>trusted root certificate</i> , a <i>trusted authority certificate</i> , or a <i>trusted CA certificate</i> . This CA certificate might be that of a trusted commercial certificate authority or it may be a privately generated certificate that an organization creates internally to provide a mechanism to control access to resources that are protected by the SSL/TLS protocols.				
	See <u>Key and Certificate Management</u> on Page 83 for more information. This section does not discuss the creation of CA Certificates.				
Client Authentication	A process using paired keys and identity certificates to prevent unauthorized access to the DeviceMaster. Client authentication is discussed in <u>Client Authentication</u> on Page 75 and <u>Changing Keys and Certificates</u> on Page 86.				
DH Key Pair Used by SSL Servers <u>†</u>	This is a private/public key pair that is used by some cipher suites to encrypt the SSL/TLS handshaking messages. Possession of the private portion of the key pair allows an eavesdropper to decrypt traffic on SSL/TLS connections that use DH encryption during handshaking.				
	The DH (Diffie-Hellman) key exchange, also called exponential key exchange, is a method of digital encryption that uses numbers raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted, making the task of a would-be code breaker mathematically overwhelming.				
	The most serious limitation of Diffie-Hellman (DH key) in its basic or <i>pure</i> form is the lack of authentication. Communications using Diffie-Hellman all by itself are vulnerable to <u>man in the middle attacks</u> . Ideally, Diffie-Hellman should be used in conjunction with a recognized authentication method such as digital signatures to verify the identities of the users over the public communications medium.				
	See <u>Certificates and Keys</u> on Page 75 and <u>Key and Certificate Management</u> on Page 83 for more information.				
identical, self Authenticatio	ster units are shipped from the factory with identical configurations. They all have the f-signed, Comtrol Server RSA Certificates, Server RSA Keys, Server DH Keys, and no Client on Certificates. For maximum data and access security, you should configure all DeviceMaster				

units with custom certificates and keys.

	Term or Issue Explanation (Continued)
Digital Certificate	A digital certificate is an electronic <i>credit card</i> that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys.
	See <u>Key and Certificate Management</u> on Page 83 for more information.
	A public key infrastructure (PKI) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on.
PKI (public key infrastructure)	The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message. Traditional cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This secret or private key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the public key infrastructure is the preferred approach on the Internet. (The private key system is sometimes known as symmetric cryptography and the public key system as asymmetric cryptography.)
	A public key infrastructure consists of:
	• A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key
	• A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor
	• One or more directories where the certificates (with their public keys) are held
	A certificate management system
	For more information, see <u>SSL Authentication</u> on Page 74, <u>SSL Performance</u> on Page 76, <u>SSL Cipher Suites</u> on Page 77, and <u>DeviceMaster Supported Cipher Suites</u> on Page 77.

	Term or Issue Explanation (Continued)
	This is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption. RSA is widely used in electronic commerce protocols, and is believed to be sufficiently secure given sufficiently long keys and the use of up-to-date implementations. The system includes a communications channel coupled to at least one terminal having an encoding device, and to at least one terminal having a decoding device.
	• Public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures.
	Private Key
PSA Koy Doint	- One half of the <i>key pair</i> used in conjunction with a public key
RSA Key Pair†	- Both the public and the private keys are needed for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet.
	- The private key is used to decrypt text that has been encrypted with the public key.
	Thus, if User A sends User B a message, User A can find out User B's public key (but not User B's private key) from a central administrator and encrypt a message to User B using User B's public key. When User B receives it, User B decrypts it with User B's private key. In addition to encrypting messages (which ensures privacy), User B can authenticate User B to User A (so that User A knows that it is really User B who sent the message) by using User B's private key to encrypt a digital certificate.
	See <u>Key and Certificate Management</u> on Page 83 for more information.
SSH (Secure Shell)	Secure Shell (SSH) allows data to be exchanged using a secure channel between two networked devices. Replaces telnet which has no security. SSH requires password authentication – even if the password is empty.
	See <u>SSH Server</u> on Page 73 for more information.
	The Secure Sockets Layer (SSL) is the predecessor of (TLS) Transport Layer Security.
	SSL is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers.
SSL (Secure Sockets Layer)	SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security.
	SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.
	See Pages 74 through 77 for detailed information about SSL.
	Note: Two slightly different SSL protocols are supported by the DeviceMaster: SSLv3 and TLSv1.
TLS (Transport Layer	Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).
Security)	TLS and SSL are not interoperable. The TLS protocol does contain a mechanism that allows TLS implementation to back down to SSL 3.0.
Secure Data Mode	TCP connections that carry data to/from the DeviceMaster serial ports are encrypted using SSL or TLS security protocols. See <u>Security Modes</u> on Page 71 and <u>Configure / Enable</u> . <u>Security Features Overview</u> on Page 79 for more information.

	Term or Issue Explanation (Continued)
Secure Config Mode	Unencrypted access to administrative and diagnostic functions are disabled. See <u>Security</u> <u>Modes</u> on Page 71 and <u>Configure / Enable Security Features Overview</u> on Page 79 for more information.
Secure Monitor Data Mode via Telnet	Allows monitoring of a single serial port on the DeviceMaster while the port is configured for Secure Data Mode. For more information see, the Enable Monitoring Secure Data via Telnet option on Page 81.
	A man in the middle attack is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other.
Man in the Middle attack	The attack gets its name from the ball game where two people try to throw a ball directly to each other while one person in between them attempts to catch it. In a man in the middle attack, the intruder uses a program that appears to be the server to the client and appears to be the client to the server. The attack may be used simply to gain access to the message, or enable the attacker to modify the message before retransmitting it.
	In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority (CA).
	The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access.
How Public and Private Key Cryptography Works	The private key is never shared with anyone or sent across the Internet. You use the private key to decrypt text that has been encrypted with your public key by someone else (who can find out what your public key is from a public directory).
	Thus, if User A sends User B a message, User A can find out User B's public key (but not User B's private key) from a central administrator and encrypt a message to User B using User B's public key. When User B receives it, User B decrypts it with User B's private key. In addition to encrypting messages (which ensures privacy), User B can authenticate User B to User A (so User A knows that it is really User B who sent the message) by using User B's private key to encrypt a digital certificate. When User A receives it, User A can use User B's public key to decrypt it.
	A number of products are offered that enable a company or group of companies to implement a PKI. The acceleration of e-commerce and business-to-business commerce over the Internet has increased the demand for PKI solutions. Related ideas are the virtual private network (VPN) and the IP Security (IPsec) standard. Among PKI leaders are:
	• RSA, which has developed the main algorithms used by PKI vendors.
Who Provides	• Verisign, which acts as a certificate authority and sells software that allows a company to create its own certificate authorities.
the Infrastructure?	• GTE CyberTrust, which provides a PKI implementation methodology and consultation service that it plans to vend to other companies for a fixed price.
	• Xcert, whose Web Sentry product that checks the revocation status of certificates on a server, using the Online Certificate Status Protocol (OCSP).
	• Netscape, whose Directory Server product is said to support 50 million objects and process 5,000 queries a second; Secure E-Commerce, which allows a company or extranet manager to manage digital certificates; and Meta-Directory, which can connect all corporate directories into a single directory for security management.

Term or Issue Explanation (Continued)

The following topic references are from: <u>http://searchsecurity.techtarget.com/</u>

- PKI (public key infrastructure)
- How Public/Private Key Cryptography Works
- Who Provides the Infrastructure
- Digital Certificate
- DH Key
- Man in the Middle attack

The RSA Key pair topic reference is from: http://en.wikipedia.org/wiki/RSA

TCP and UDP Socket Ports Used by the DeviceMaster

	Socket Port Number Descriptions			
22 SSH	TCP Ports 22 (ssh) and 23 (telnet) are used for administrative and diagnostic purposes and aren't required for normal use and are enabled by default and Port			
23 Telnet	23 may be disabled.			
80 HTTP	TCP Ports 80 (http) and 443 (https) are used by the web server for administration			
443 SSL or HTTPS	and configuration and are enabled by default and cannot be disabled.			
102 RFC1006	TCP Port 102 is used for RFC1006 (ISO over TCP) serial port access. Not used for normal NS-Link SocketServer access. The RFC1006 server can be disabled by setting the server port number to -1 and is enabled by default.			
161 SNMP	UDP Port 161 is used by the SNMP agent if SNMP is enabled which is the default.			
4606	TCP Port 4606 is required if you want to use NS-Link or PortVision DX if you want to update firmware without setting up a TFTP server and this port cannot be disabled.			
	TCP Port 4607 is only used for diagnostic purposes and isn't required for normal operation and this port cannot be disabled.			
4607	If SocketServer is to be used, then the user may enable usage of TCP or UDP ports for access to the serial ports. These ports are not enabled by default and are also user configurable to different values. Defaults for TCP would begin at 8000 and for UDP would begin at 7000.			
TCP 8000 - 8xxx	Incremented per serial port on the DeviceMaster.			
101 0000 - 0XXX	For example: A DeviceMaster 16- port would have Ports 8000 through 8015.			
UDP 7000 - 7xxx	Incremented per serial port on the DeviceMaster.			
	For example: A DeviceMaster 16- port would have Ports 7000 through 7015.			

Following list is all of the logical TCP and UDP socket ports implemented in DeviceMasters.

DeviceMaster Security Features

The following subsections provide information about DeviceMaster security features.

Security Modes

The DeviceMaster supports two security modes.

Security Mode Descriptions				
	SSL encryption for serial port data streams for both NS-Link and SocketServer. Secure Data mode:			
Secure Data	 Requires SSL encryption of TCP connections to SocketServer (Ports 8000, 8001, 8002 and so forth). 			
	Disables UDP access to SocketServer.			
	• Disables RFC1006 (ISO-over-TCP) access to SocketServer.			
	• Disables MAC-mode access to serial ports. MAC mode admin and ID commands are still allowed.			
	• Requires SSL encryption of NS-Link TCP connections (Port 4606). Not directly supported by NS-Link drivers for Windows and Linux. The Linux driver has been tested using stunnel, but manual setup is required.			
	• Requires SSH instead of telnet connection to the diagnostic log (TCP Port 4607).			
	• Two values for http READ and WRITE commands: A2: Enable.			
Secure Config	Encrypts/authenticates configuration and administration operations (web server, IP settings, load SW, and so forth.). Secure Config mode:			
	• Disables MAC mode admin commands except for ID request [†] .			
	• Disables TCP/IP admin commands except for ID request [†] .			
	• Disables telnet console access (Port 23) [†] .			
	• Disables unencrypted http:// access via Port 80.			
	• Disables e-mail notification and SNMP features.			
	• Two values for http READ and WRITE commands: A3: Enable.			
† Affects both I	RedBoot and SocketServer/NS-Link applications.			

Secure Data Mode and Secure Config Mode Comparison

Feature	Secure Data	Secure Config	Secure Data/ Secure Config
MAC (admin)	enabled	disabled †	disabled †
MAC (async)	disabled	enabled	disabled
TCP 4606 (admin)	SSL, enabled	clear, disabled †	SSL, disabled †
TCP 4606 (async)	SSL	clear	SSL
UDP	disabled	user-configured	disabled
telnet/RFC2217	user-configured	user-configured	user-configured
RFC1006	disabled	user-configured	disabled
4607 (diag log)	SSH	telnet	SSH
8000 (serial port)	SSL	clear	SSL
console (config)	telnet on Port 23 SSH on Port 22	SSH on Port 22	SSH on Port 22
web	clear on Port 80 SSL on Port 443	SSL on Port 443	SSL on Port 443
SMTP, SNMP	user-configured	disabled	disabled
RedBoot MAC	enabled	disabled †	disabled †
RedBoot 4606	enabled	disabled †	disabled †
RedBoot telnet	user-configured	disabled	disabled

This table provides information that compares Secure Data and Secure Config modes.

Security Comparison

	Veakest	Strongest				
	0	1	2	3	3	4
Supported by	None	Password	Authentication	Secure Config	Secure Data	Key & Certificate
RedBoot	yes	yes	yes	no	yes	no
SocketServer	yes	yes	yes	yes	yes	yes
NS-Link Driver/MAC	yes	yes	yes	no	no	no
NS-Link Driver/IP	yes	yes	yes	yes		
Serial Monitoring	yes	yes	yes	no	yes \dagger	no
TCP to Serial Ports	yes	yes	yes	no	no	no
SSH to Serial Ports	no	no	no	yes	yes	yes
UDP to Serial Ports	yes	yes	yes	disabled	disabled	disabled
Telnet/Port23	yes	yes	yes	disabled	yes †	disabled
SSH Telnet/Port 22	yes	yes	yes	yes	yes	yes
Telnet Port 4607	yes	yes	yes	disabled	yes	yes
SSH (PuTTY) 4607	no	no	no	yes	disabled	disabled
HTTP (Port 80)	yes	yes	yes	disabled	disabled	disabled
HTTPS (Port 443)	no	no	no	yes	yes	yes
Email	yes	yes	yes	disabled	disabled	disabled
SNMP	yes	yes	yes	disabled	disabled	disabled
RFC1006	yes	yes	yes	disabled	disabled	disabled

This table displays addition information about security feature comparisons.

† Enable Monitoring Secure Data via Telnet must be enabled. SSH does not support port monitoring. You can set the **securemon enable** option.

admin commands are disabled except for read-only ID command required by NS-Link to identify the device.

The intention is to allow NS-Link to operate through an SSL connection to Port 4606 while is in Secure Data Mode, and to allow NS-Link to operate through a MAC connection with Secure Config Mode enabled and Secure Data Mode disabled.

SSH Server

The DeviceMaster SSH server has the following characteristics:

- Requires password authentication even if the password is empty.
- Enabled/disabled along with telnet access independently of Secure Data and Secure Config Modes.
- The DeviceMaster uses third-party MatrixSSH library from PeerSec Networks: http://www.peersec.com/.

SSL Overview

DeviceMaster SSL provides the following features:

- Provides both encryption and authentication.
 - Encryption prevents a third-party eavesdropper from viewing data that is being transferred.
 - Authentication allows both the client (that is, web browser) and server (that is. DeviceMaster) to ensure that only desired parties are allowed to establish connections. This prevents both unauthorized access and <u>man-in-the-middle</u> attacks on the communications channel.
- Several slightly different SSL protocols are supported by the DeviceMaster, SSLv3, TLSv1.0, TLS1.1, and TLS1.2.
- The DeviceMaster uses third-party MatrixSSL library from PeerSec Networks: <u>http://www.peersec.com/</u> <u>matrixssl.htm</u>l.

SSL Authentication

DeviceMaster SSL authentication has the following features:

- Authentication means being able to verify the identity of the party at the other end of a communications channel. A username/password is a common example of authentication.
- SSL/TLS protocols allow authentication using either RSA certificates or DSS certificates. DeviceMaster supports only RSA certificates.
- Each party (client and server) can present an ID certificate to the other.
- Each ID certificate is signed by another *authority* certificate or key.
- Each party can then verify the validity of the other's ID certificate by verifying that it was signed by a trusted authority. This verification requires that each party have access to the certificate/key that was used to sign the other party's ID certificate.

Server Authentication

Server Authentication is the mechanism by which the DeviceMaster proves its identity.

- The DeviceMaster (generally an SSL server) can be configured by uploading an ID certificate that is to be presented to clients when they connect to the DeviceMaster.
- The private key used to sign the certificate must also be uploaded to the DeviceMaster.

Note: Possession of that private key will allow eavesdroppers to decrypt all traffic to and from the DeviceMaster.

- The corresponding public key can be used to verify the ID certificate but not to decrypt traffic.
- All DeviceMaster are shipped from the factory with identical self-signed ID certificates and private keys. This means that somebody could (with a little effort) extract the factory default private key from the DeviceMaster firmware and use that private key to eavesdrop on traffic to/from any other DeviceMaster that is being used with the default private key.
- The public/private key pairs and the ID certificates can be generated using openssl command-line tools.
- If the server authentication certificate in the DeviceMaster is not signed by an authority known to the client (as shipped, they are not), then interactive SSL clients such as web browsers will generally warn the user.
- If the name in server authentication certificate does not match the *hostname* that was used to access the server, then interactive SSL clients such as web browsers will generally warn the user.

Client Authentication

Client Authentication is the mechanism by which the DeviceMaster verifies the identity of clients (that is, web browsers and so forth).

- Clients can generally be configured to accept a particular unknown server certificate so that the user is not subsequently warned.
- The DeviceMaster (generally an SSL server) can be configured by uploading a trusted *authority* certificate that will be used to verify the ID certificates presented to the DeviceMaster by SSL clients. This allows you to restrict access to the DeviceMaster to a limited set of clients which have been configured with corresponding ID certificates.
- DeviceMaster units will be shipped without an authority certificate and will not require clients to present ID certificates. This allows any and all SSL clients to connect to the DeviceMaster.

Certificates and Keys

To control access to the DeviceMaster's SSL/TLS protected resources you should create your own custom CA certificate and then configure authorized client applications with identity certificates signed by the custom CA certificate.

This uploaded CA certificate that is used to validate a client's identity is sometimes referred to as a *trusted root certificate*, a *trusted authority certificate*, or a *trusted CA certificate*. This CA certificate might be that of a trusted commercial certificate authority or it may be a privately generated certificate that an organization creates internally to provide a mechanism to control access to resources that are protected by the SSL/TLS protocols.

The following is a list that contains additional information about certificates and keys:

- By default, the DeviceMaster is shipped without a CA (Certificate Authority) and therefore allowing connections from any SSL/TLS client. If desired, controlled access to SSL/TLS protected features can be configured by uploading a client authentication certificate to the DeviceMaster.
- Certificates can be obtained from commercial certificate authorities (VeriSign, Thawte, Entrust, and so forth.).
- Certificates can be created by users for their own use by using **openssi** command line tools or other applications.
- Certificates and keys to be uploaded to the DeviceMaster must be in the **.DER** binary file format, not in the **.PEM** ASCII file format. (The **openssi** tools can create files in either format and can convert files back and forth between the two formats.)
- Configuring Certificates and keys are configured by four uploaded files on the bottom *Key and Certificate Management* portion of the *Edit Security Configuration* web page:
 - RSA Key Pair used by SSL and SSH servers

This is a private/public key pair that is used for two purposes:

- It is used by some cipher suites to encrypt the SSL/TLS handshaking messages. Possession of the private portion of this key pair allows an eavesdropper to both decrypt traffic on SSL/TLS connections that use RSA encryption during handshaking.
- It is used to sign the Server RSA Certificate in order to verify that the DeviceMaster is authorized to use the server RSA identity certificate. Possession of the private portion of this key pair allows somebody to pose as the DeviceMaster.

If the Server RSA Key is replaced, a corresponding RSA server certificate must also be generated and uploaded as a matched set or clients are not able to verify the identity certificate.

- RSA Server Certificate used by SSL servers
 - This is the RSA identity certificate that the DeviceMaster uses during SSL/TLS handshaking to identify itself. It is used most frequently by SSL server code in the DeviceMaster when clients open connections to the DeviceMaster's secure web server or other secure TCP ports. If a DeviceMaster serial port configuration is set up to open (as a client), a TCP connection to another server device, the DeviceMaster also uses this certificate to identify itself as an SSL client if requested by the server.
 - In order to function properly, this certificate must be signed using the Server RSA Key. This means that the server RSA certificate and server RSA key must be replaced as a pair.

- DH Key pair used by SSL servers

This is a private/public key pair that is used by some cipher suites to encrypt the SSL/TLS handshaking messages.

Possession of the private portion of the key pair allows an eavesdropper to decrypt traffic on SSL/TLS connections that use DH encryption during handshaking.

- Client Authentication Certificate used by SSL servers

If configured with a CA certificate, the DeviceMaster requires all SSL/TLS clients to present an RSA identity certificate that has been signed by the configured CA certificate. As shipped, the DeviceMaster is not configured with a CA certificate and all SSL/TLS clients are allowed.

SSL Performance

The DeviceMaster has these SSL performance characteristics:

• Encryption/decryption is a CPU-intensive process, and using encrypted data streams will limit the number of ports that can be maintained at a given serial throughput. For example, the table below shows the number of ports that can be maintained by SocketServer at 100% throughput for various cipher suites and baud rates.

	9600	38400	57600	115200
RC4-MD5	32	16	10	5
RC4-SHA	32	13	9	4
AES128-SHA	28	7	5	2
AES256-SHA	26	7	4	2
DES3-SHA	15	3	2	1

- **Note:** These throughputs required 100% CPU usage, so other features such as the web server are very unresponsive at the throughputs shown above. To maintain a usable web interface, one would want to stay well below the maximum throughput/port numbers above.
- The overhead required to set up an SSL connection is significant. The time required to open a connection to SocketServer varies depending on the public-key encryption scheme used for the initial handshaking. These are typical setup times for the three public-key encryption schemes for the DeviceMaster:
 - RSA 0.66 seconds
 - DHE 3.84 seconds
 - DHA 3.28 seconds
- Since there is a certain amount of overhead for each block of data sent/received on an SSL connection, the SocketServer polling rate and size of bocks that are written to the SocketServer also has a noticeable effect on CPU usage. Writing larger blocks of data and a slower SocketServer polling rate will decrease CPU usage and allow somewhat higher throughputs.

SSL Cipher Suites

This subsection provides information about SSL cipher suites.

- An SSL connection uses four different facilities, each of which can use one of several different ciphers or algorithms. A particular combination of four ciphers/algorithms is called a "cipher suite".
- A Cipher Suite consists of
 - Public Key Encryption Algorithm
 - Used to protect the initial handshaking and connection setup.
 - Typical options are RSA, DH, DHA, DHE, EDH, SRP, PSK. The DeviceMaster supports RSA, DHA, DHE.
 - Authentication Algorithm
 - Used to verify the identities of the two parties to each other.
 - Typical options are RSA, DSA, ECDSA. The DeviceMaster supports only RSA.
 - Stream Cipher
 - Used to encrypt the user-data exchanged between the two parties.
 - Typical options: RC4, DES, 3DES, AES, IDEA, Camellia, NULL. The DeviceMaster supports RC4, 3DES, AES.
 - Message Authentication Code
 - Hash function (checksum) used to verify that each message frame has not be corrupted or changed while in transit.
 - Typical options include MD5, SHA, MD2, MD4. The DeviceMaster supports MD5, SHA
- In the design of the SSL/TLS protocols the choices of four of the above are not independent of each other: only certain combinations are defined by the standards. The standard combinations of protocol (SSL or TLS) and cipher suites support by DeviceMaster are shown in the following table.

DeviceMaster Supported Cipher Suites

The DeviceMaster supports the cipher suites:

Protocol	Public Key	Authentication	Cipher	MAC
SSL	RSA	RSA	3DES	SHA
SSL	RSA	RSA	RC4	SHA
SSL	RSA	RSA	RC4	MD5
SSL	DHE	RSA	3DES	SHA
SSL	DHA	RSA	RC4	MD5
SSL	RSA	RSA	NULL	MD5
SSL	RSA	RSA	NULL	SHA
TLS	RSA	RSA	AES128	SHA
TLS	RSA	RSA	AES256	SHA
TLS	DHE	RSA	AES128	SHA
TLS	DHE	RSA	AES256	SHA
TLS	DHA	RSA	AES128	SHA
TLS	DHA	RSA	AES256	SHA

SSL Resources

You can refer to the following SSL resources for more information:

- Standard reference book is SSL and TLS by Eric Rescorla
- Wikipedia page on SSL/TLS provides a good overview: <u>http://en.wikipedia.org/wiki/TLS</u>
- **openssl** contains command-line tools to do the following. More information is available at: <u>http://www.openssl.org/</u>
 - Create/examine keys/certificates
 - Act as client or server
- ssldump is a -command line tool that displays a human-readable dump of an SSL connection's handshaking and traffic:. More information can be found at: <u>http://www.rtfm.com/ssldump/.</u>
 - If provided with server's private key, can decrypt data stream
 - Can display decoded data stream in ASCII/hex
 - Can display contents of handshaking packets (including ID certificates)

Configure/Enable Security Features Overview

You can enable DeviceMaster security features the web page (SocketServer or the NS-Link version). *Key and Certificate Management* must be done using the *Security* tab in the DeviceMaster web pages.

If you want secure COM ports, you must also **Enable SSL Mode** and enter any applicable server or client certificates in the NS-Link device driver for Windows. See <u>Device Driver (NS-Link) Installation</u> on Page 47.

The following illustration shows the Security Settings page under the Network menu and is discussed in the following table.

Comtrol'	Home	Port	Network	Diagnostic	s Syst	tem	Help	DeviceMaster 1-port	Logout
Configuration	Passwo	ord Se	ecurity	Keys/Certs	Email	RF	C1006		
Security Set	tings								
			Data Mode Config Mo						
☑ E	nable Te	elnet/s	sh -						
			ng Secure	e Data via T	lenet				
	nable SI								
SSLv3.0 V M				S Version	addrog	c blo	cke bok		
			iress / Wi	Sector and the sector of the sector	addres	S DIO	CKS Delo	JW .	
	BIO		/ 0 / 0						
Note								Save	
The address blo address and ma					ition cor	mpris	sing an i	IP	
For IPv4: a mas defines 2 addre									
For IPv6: a mas defines 2 addre defines 8, etc.									
								2004-0-1 (A. 12	
								© Copyright Com	trol Corp

	Security Option Descriptions
	If Secure Data Mode is enabled TCP connections which carry data to/from the serial ports will be encrypted using SSL or TLS security protocols. This includes the following:
	• TCP connections to the per-serial-port TCP ports (default is 8000, 8001, 8002, and so forth) are encrypted using SSL/TLS.
Enable Secure Data	• TCP connections to TCP Port 4606 on which the DeviceMaster implements the Comtrol proprietary serial driver protocol are encrypted using SSL/TLS.
Mode	• Since SSL/TLS can not be used for either UDP data streams or for the Comtrol proprietary MAC mode Ethernet driver protocol, both UDP and MAC mode serial data transport features are disabled.
	• In order to minimize possible security problems, e-mail and RFC1006 features are also disabled in <i>Secure Data</i> mode.
	In addition to encrypting the data streams, it is possible to configure the DeviceMaster so that only authorized client applications can connect using SSL/TLS. See the <u>Client</u> <u>Authentication</u> discussion on Page 75 for details.
	If Secure Config Mode is enabled, unencrypted access to administrative and diagnostic functions is disabled. Secure Config Mode changes DeviceMaster behavior as follows:
	• Telnet access to administrative and diagnostic functions is disabled. SSH access is still allowed.
	• Unencrypted access to the web server via Port 80 (http://URLs) is disabled.
Enable Secure Config	• Encrypted access to the web server via Port 443 (https://URLs) is still allowed.
Mode	• Administrative commands that change configuration or operating state which are received using the Comtrol proprietary TCP driver protocol on TCP Port 4606 are ignored.
	• Administrative commands that change configuration or operating state that are received using the Comtrol MAC mode proprietary Ethernet protocol number 0x11FE are ignored.

	Security Option Descriptions (Continued)
	When checked, this allows the monitor command to be used while Secure Data Mode is enabled. When unchecked, the monitor command can only be used if Secure Data Mode is not enabled. You must click Save and reboot the DeviceMaster for the change to go into affect. This option is disabled by default.
	The Enable Monitoring Secure Data via Telnet feature allows you to monitor serial data being sent/received on a serial port (either via NS-Link or SocketServer). The monitoring is done by telnetting to the DeviceMaster and using the following commands:
	monitor [-ac] portnumber
Enable Monitoring	Display a live hex dump of TX/RX data for the specified serial port. You can only monitor one port at a time. The live dump will continue until the Enter key is pressed. See the following detailed description and examples. The data is logged when it is written/read to/from the serial port driver's TX/RX buffers as such, the relative timing between RX/TX bytes is not precise, but it should be sufficient to debug most problems (especially frame-oriented, command/response serial protocols).
Secure Data via Telnet	Monitoring serial data through a telnet connection does generate extra network traffic and may have small effects on the timing of DeviceMaster operations when large amounts of data are being logged at high baud rates. See <u>Example 1</u> on Page 81 for more information.
	- The -a option enables displaying of ASCII representation of data in a column to the right the hex representation. See <u>Example 2</u> on Page 82.
	- The -c option enables the use of color instead of < and > to indicate the data flow direction. Tx is green and Rx is red. See <i>Example 3</i> on Page 82.
	securemon [enable disable]
	By default, monitoring of TX/RX data when in Secure Data Mode is not allowed through telnet (an insecure protocol). This command allows you to override that default when securemon is enabled it will allow monitoring of secure data via an insecure protocol like telnet.
	<i>Note:</i> Optionally, you can use the Port Monitor function in the web interface. Click Diagnostics Port Monitor.
Enable Telnet/ssh	This option enables or disables the telnet security feature after you click Save and the DeviceMaster has been rebooted. <i>This option is enabled by default</i> .
Enable SNMP	This option enables or disables the SNMP security feature after you click Save and the DeviceMaster has been rebooted. <i>This option is enabled by default</i> .

Example 1

The following example shows how to monitor output using a loopback plug and a program that repeatedly sends the string abcABC123 to Port 1:

dm> monitor 1
Serial monitoring started for port 1 -- press [Enter] to stop.
> 61 62 63 41 42 43 31 32 33
< 61 62 63 41 42 43 31 32 33
> 61 62 63 41 42 43 31 32 33
< 61 62 63 41 42 43 31 32 33
< 61 62 63 41 42 43 31 32 33
< 61 62 63 41 42 43 31 32 33
< 61 62 63 41 42 43 31 32 33
< 61 62 63 41 42 43 31 32 33
< 61 62 63 41 42 43 31 32 33
< 61 62 63 41 42 43 31 32 33
< 61 62 63 41 42 43 31 32 33
</pre>

Example 2

The following example shows how the **-a** option enables displaying of ASCII representation of data in a column to the right the hex representation:

```
dm> monitor -a 1
Serial monitoring started for port 1 -- press [Enter] to stop.
> 61 62 63 41 42 43 31 32 33
                                                    > abcABC123
< 61 62 63 41 42 43 31 32 33
                                                     < abcABC123
> 61 62 63 41 42 43 31 32 33
                                                    > abcABC123
< 61 62 63 41 42 43 31 32 33
                                                     < abcABC123
> 61 62 63 41 42 43 31 32 33
                                                     > abcABC123
< 61 62 63 41 42 43 31 32 33
                                                     < abcABC123
> 61 62 63 41 42 43 31 32 33
                                                     > abcABC123
< 61 62 63 41 42 43 31 32 33
                                                    < abcABC123
> 61 62 63 41 42 43 31 32 33
                                                    > abcABC123
< 61 62 63 41 42 43 31 32 33
                                                     < abcABC123
> 61 62 63 41 42 43 31 32 33
                                                     > abcABC123
< 61 62 63 41 42 43 31 32 33
                                                     < abcABC123
```

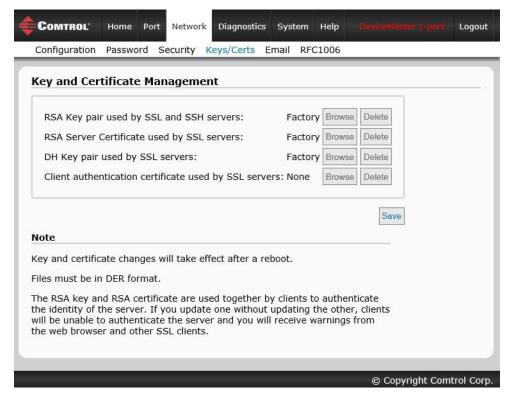
Example 3

The -c option enables the use of color instead of < and > to indicate the data flow direction. Tx is green and Rx is red.

```
dm> monitor -c 1
Serial monitoring started for port 1 -- press [Enter] to stop.
61 62 63 41 42 43 31 32 33 61 62 63 41 42 43 31
32 33 61 62 63 41 42 43 31 32 33 61 62 63 41
                                             42
43 31 32 33 61 62 63 41 42 43 31 32 33 61 62 63
41 42 43 31 32 33 61 62 63 41 42 43 31 32 33 61
62 63 41 42 43 31 32 33 61 62 63 41 42 43 31 32
33 61 62 63 41 42 43 31 32 33 61 62 63 41 42 43
31 32 33 61 62 63 41 42 43 31 32 33 61 62 63 41
42 43 31 32 33 61 62 63 41 42 43 31 32 33 61 62
63 41 42 43 31 32 33 61 62 63 41 42 43 31 32 33
The -a and -c options can be used together:
dm> monitor -ac 1
Serial monitoring started for port 1 -- press [Enter] to stop.
61 62 63 41 42 43 31 32 33 61 62 63 41 42 43 31
                                                   abcABC123abcABC1
32 33 61 62 63 41 42 43 31 32 33 61 62 63 41 42
                                                    23abcABC123abcAB
43 31 32 33 61 62 63 41 42 43 31 32 33 61 62 63
                                                   C123abcABC123abc
41 42 43 31 32 33 61 62 63 41 42 43 31 32 33 61
                                                   ABC123abcABC123a
62 63 41 42 43 31 32 33 61 62 63 41 42 43 31 32
                                                   bcABC123abcABC12
33 61 62 63 41 42 43 31 32 33 61 62 63 41 42 43
                                                   3abcABC123abcABC
31 32 33 61 62 63 41 42 43 31 32 33 61 62 63 41
                                                   123abcABC123abcA
42 43 31 32 33 61 62 63 41 42 43 31 32 33 61 62
                                                   BC123abcABC123ab
63 41 42 43 31 32 33 61 62 63 41 42 43 31 32 33
                                                   cABC123abcABC123
```

Key and Certificate Management

Key and Certificate management is only available in Network | Keys/Cert web page.



Ке	y and Certificate Management Option Descriptions
	This is a private/public key pair that is used for two purposes:
RSA Key pair used by SSL and SSH servers	It is used by some cipher suites to encrypt the SSL/TLS handshaking messages. Possession of the private portion of this key pair allows an eavesdropper to both decrypt traffic on SSL/TLS connections that use RSA encryption during handshaking.
	It is used to sign the Server RSA Certificate in order to verify that the DeviceMaster is authorized to use the server RSA identity certificate. Possession of the private portion of this key pair allows somebody to pose as the DeviceMaster.
	If the Server RSA Key is to be replaced, a corresponding RSA identity certificate must also be generated and uploaded or clients are not able to verify the identity certificate.
RSA Server Certificate used by SSL servers	This is the RSA identity certificate that the DeviceMaster uses during SSL/TLS handshaking to identify itself. It is used most frequently by SSL server code in the DeviceMaster when clients open connections to the DeviceMaster's secure web server or other secure TCP ports. If a DeviceMaster serial port configuration is set up to open (as a client) a TCP connection to another server device, the DeviceMaster also uses this certificate to identify itself as an SSL client if requested by the server. In order to function properly, this certificate must be signed using the Server RSA Key. This means that the server RSA certificate and server RSA key must be replaced as a pair.

Key and (Certificate Management Option Descriptions (Continued)			
DH Kou pair used by SSI	This is a private/public key pair that is used by some cipher suites to encrypt the SSL/TLS handshaking messages.			
DH Key pair used by SSL servers	Note: Possession of the private portion of the key pair allows an eavesdropper to decrypt traffic on SSL/TLS connections that use DH encryption during handshaking.			
Client Authentication Certificate used by SSL servers	If configured with a CA certificate, the DeviceMaster requires all SSL/TLS clients to present an RSA identity certificate that has been signed by the configured CA certificate. As shipped, the DeviceMaster is not configured with a CA certificate and all SSL/TLS clients are allowed.			
	See <u>Client Authentication</u> on Page 75 for more detailed information			
• All DeviceMaster units are shipped from the factory with identical configurations. They all have the identical, self-signed, Comtrol Server RSA Certificates, Server RSA Keys, Server DH Keys, and no Client Authentication Certificates.				
• For maximum data an certificates and keys.	d access security, you should configure all DeviceMaster units with custom			

Using a Web Browser to Set Security Features

The follow procedures are discussed below:

- <u>Changing Security Configuration</u>
- <u>Changing Keys and Certificates</u> on Page 86

Changing Security Configuration

Use the following steps to change security settings in the DeviceMaster.

- 1. Enter the IP address of the DeviceMaster in the *Address* field of your web browser and press the Enter key.
- 2. Click Network | Security.
- 3. Click the appropriate check boxes to enable or disable security for your environment.

	nable Secu	ire Data Mode	3				
E	nable Secu	ire Config Mo	de				
✓ E	nable Teln	et/ssh					
🗆 E	nable Mon	toring Secure	e Data via Tle	net			
<u></u>	nable SNM	Р					
		lowed SSL/TL					
□ <i>F</i>	llow TCP c	onnections or	nly from the a	ddress blo	ocks belo	w	
		/ 0					
						Save	
Note							
Note The address blo	ale dafiniti				ialaa aa T	D	

Refer to the help system or <u>Configure / Enable Security Features Overview</u> on Page 79 for detailed information.

4. After making changes, click Save.

Changing Keys and Certificates

Use the following steps to update security keys and certificates in the DeviceMaster. Refer to the help system or <u>Key and Certificate Management</u> subsection on Page 86 for detailed information.

- 1. If necessary, enter the IP address of the DeviceMaster in the *Address* field of your web browser and press the **Enter** key.
- 2. Click Network | Keys/Certs.
- 3. Click Browse to locate the key or certificate file, highlight the file, and click Open.
- 4. Click Upload.
- Click Save, but changes will not take effect until the DeviceMaster is rebooted.
 Note: The key or certificate notation changes from factory or none to User when the DeviceMaster is secure.
 You can reboot the DeviceMaster by clicking System | Reboot or use the PortVision DX reboot optione.

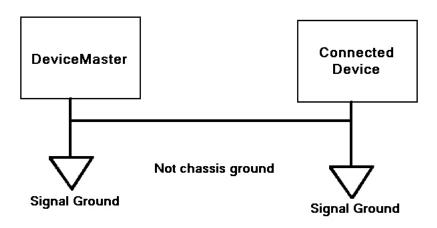
Connecting Serial Devices

This section discusses connecting your serial devices to the DeviceMaster. It also provides you with information to build serial or test cables and loopback connectors to test the serial ports.

- DB9 Connectors
- <u>*RJ45 Connectors*</u> on Page 91
- Four Screw Terminals (DM-2202) on Page 94
- <u>Eight Screw Terminals (DM-2402)</u> on Page 97
- Nine Screw Terminals (DM-2201) on Page 100

Caution Make sure that you have configured the ports for the correct communications mode before connecting any devices. The default mode is RS-232. There is a remote possibility that connecting a serial device for the wrong mode could damage the serial device.

Note: The DeviceMaster LT provides different RJ45 pin outs and is not discussed in this guide. Refer to the DeviceMaster LT User Guide for product-specific information.



DB9 Connectors

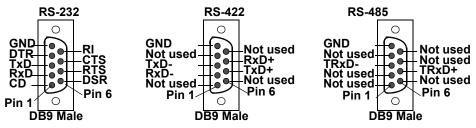
This subsection provides the following information:

- Connector pin assignments (below)
- <u>DB9 Null-Modem Cables (RS-232)</u> on Page 89
- <u>DB9 Null-Modem Cables (RS-422)</u> on Page 89
- <u>DB9 Straight-Through Cables (RS-232/485)</u> on Page 89
- <u>DB9 Loopback Plugs</u> on Page 90
- <u>Connecting DB9 Serial Devices</u> on Page 90

DB9 Connector Pin Outs						
Pin	RS-232	RS-422 and RS-485 Full-Duplex (Master/Slave)†	RS-485 Half-Duplex			
1	DCD	Not used	Not used			
2	RxD	RxD-	Not used			
3	TxD	TxD-	TRxD-			
4	DTR	Not used	Not used			
5	Signal GND	Signal GND	Signal GND			
6	DSR	Not used	Not used			
7	RTS	TxD+	TRxD+			
8	CTS	RxD+	Not used			
9	RI	Not used	Not Used			
† 1	The following mod	els support RS-485 full-duplex:				
•	1-Port DIN rail	models				
•	2-Port DIN rail	models				
•	4-Port DIN rail	models				

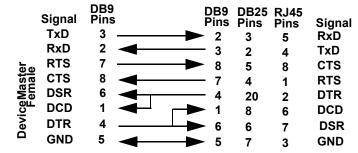
Note: The DeviceMaster Serial Hub only supports RS-232.

Refer to the hardware manufacturer's installation documentation if you need help with connector pin outs or cabling for the serial device. This illustrates the DB9 connector signals.



DB9 Null-Modem Cables (RS-232)

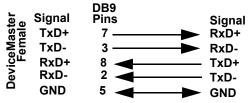
Use the following figure if you need to build an RS-232 null-modem cable. A null-modem cable is required for connecting DTE devices.



Note: You may want to purchase or build a straight-through cable and purchase a null-modem adapter.

DB9 Null-Modem Cables (RS-422)

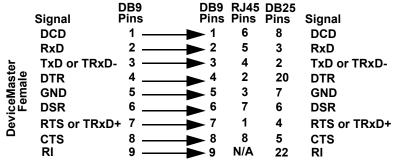
Use the following figure if you need to build an RS-422 null-modem cable.



Note: RS-422 pin outs are not standardized. Each peripheral manufacturer uses different pin outs. Refer to the peripheral documentation to determine the pin outs for the signals above.

DB9 Straight-Through Cables (RS-232/485)

Use the following figure if you need to build an RS-232 or RS-485 straight-through cable. Straight-through cables are used to connect modems and other DCE devices. For example, a straight-through cable can be used to connect COM2 to a modem.



DB9 Loopback Plugs

Loopback connectors are DB9 female serial port plugs with pins wired together that are used in conjunction with application software (Test Terminal or minicom) to test serial ports. The DeviceMaster is shipped with a a single loopback plug (RS-232/422).

Note: You can use Test Terminal (Windows) or minicom (Linux) to test the serial port. You can refer to Testing Ports Using Test Terminal on Page 154 for Windows systems.

Wire the following pins together to build additional plugs or replace a missing RS-232 loopback plug:

- Pins 1 to 4 to 6
- Pins 2 to 3
- Pins 7 to 8 to 9

Wire the following pins together for an RS-422 loopback plug:

- Pins 2 to 3
- Pins 7 to 8

Connecting DB9 Serial Devices

You can use this information to connect serial devices to DB9 connectors.

Connect your serial devices to the appropriate serial port on the DeviceMaster using the appropriate 1 cable.

Note: Refer to the hardware manufacturer's installation documentation if you need help with connector pin outs or cabling for the peripheral device.

- $\mathbf{2}$. DeviceMaster 4-port, 8-port models, and the DeviceMaster Serial Hub 16-port: verify that the devices are communicating properly.
 - Note: DeviceMaster 1-port, 2-port models, and the 4-port DIN models do not have TX/RX LEDs.

The RX (yellow) and TX (green) LEDs function accordingly when the cable is * Represents port number. attached properly to a serial device.

- After power cycling the DeviceMaster (appropriate models), the RX/TX LEDs are off.
- The LEDs do not function as described until the port has been opened by an application. You can use Test Terminal to open a port or ports if you want to test a port or ports (Testing Ports Using Test. Terminal on Page 154).

Mode	Serial Number Below xxxx-030000	Serial Number Above xxxx-030000				
RS-232	RX LEDs (yellow) are lit when connected to a valid RS-232 device					
RS-422	TX LEDs (green) are lit during active data transmission	RX LEDs (yellow) are lit while receiving data TX LEDs (green) are lit during active data				
	RX LEDs (yellow) are lit while receiving data	transmission				
RS-485	TX LEDs (green) are lit during active data transmission					
Where xx.	Where xxxx is the first four digits of the product serial number.					

You can refer to <u>Network and Device LEDs</u> on Page 167 for information about the remaining LEDs. 3.

Pin 1 Pin 5 Pin 6 Pin 9

Pin 1 Pin 5 RS-232 Only Pin 6 Pin 9 (Back View)

RS-422 Only (Back View)

The RS-232 loopback plug

DB9 LEDs

also works for RS-422.

RJ45 Connectors

This subsection provides the following information:

- Connector pin assignments (below)
- <u>RJ45 Null-Modem Cables (RS-232)</u>
- <u>RJ45 Null-Modem Cables (RS-422)</u> on Page 92
- <u>*RJ45 Straight-Through Cables (RS-232/485)*</u> on Page 92
- <u>*RJ45 Loopback Plugs*</u> on Page 92
- <u>*RJ45 RS-485 Test Cable*</u> on Page 92
- <u>Connecting RJ45 Devices</u> on Page 93

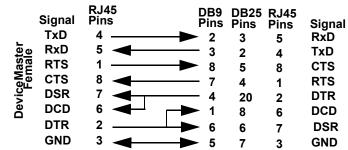
You can build your own null-modem or straight-through RJ45 serial cables if you are using the DB9 to RJ45 adapters using the following subsections.

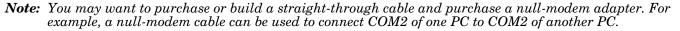
		RS-232	RS-422	RS-485
10- T	Pin 1	RTS	TxD+	TxD/RxD+
		DTR	Not Used —	
The second se	20120-00120	- Signal GND -	Signal GND-	Signal GND
		- TxD	TxD	TxD/Rxd-
	And a month of the	-RxD	RxD	Not Used
	200 22 mm - 51	DCD	Not Used	Not Used
	(M.S	DSR	Not Used	Not Used
THE REPORT OF A DESIGNATION OF A DESIGNA		CTS	RxD+	Not Used

Pin	RS-232	RS-422	RS-485
1	RTS	TxD+	TRxD+
2	DTR	Not used	Not used
3	Signal GND	Signal GND	Signal GND
4	TxD	TxD-	TRxD-
5	RxD	RxD-	Not used
6	DCD	Not used	Not used
7	DSR	Not used	Not used
8	CTS	RxD+	Not used

RJ45 Null-Modem Cables (RS-232)

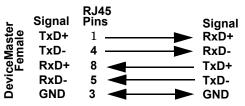
Use the following figure if you need to build an RS-232 null-modem cable. A null-modem cable is required for connecting DTE devices.





RJ45 Null-Modem Cables (RS-422)

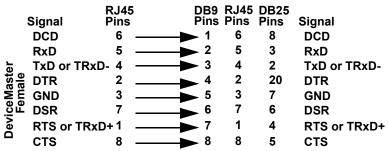
Use the following figure if you need to build an RS-422 null-modem RJ45 cable. A null-modem cable is required for connecting DTE devices.



Note: RS-422 pin outs are not standardized. Each peripheral manufacturer uses different pin outs. Please refer to the documentation for the peripheral to determine the pin outs for the signals above.

RJ45 Straight-Through Cables (RS-232/485)

Use the following figure if you need to build an RS-232 or RS-485 straight-through cable. Straight-through cables are used to connect modems and other DCE devices. For example, a straight-through cable can be used to connect COM2 of one PC to COM2 to a modem.



RJ45 Loopback Plugs

Loopback connectors are RJ45 serial port plugs with pins wired together that are used in conjunction with application software (Test Terminal for Windows or Minicom for Linux) to test serial ports. The DeviceMaster is shipped with a a single loopback plug (RS-232/422).

Plug

Top View

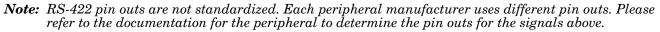
Cable

- Pins 4 to 5
- Pins 1 to 8
- Pins 2 to 6 to 7
- **Note:** You can use Test Terminal (Windows) or minicom (Linux) to test the serial port. You can refer to <u>Testing</u> <u>Ports Using Test Terminal</u> on Page 154 for Windows systems.

RJ45 RS-485 Test Cable

You can use a straight-through cable as illustrated previously, or build your own cable.





The RS-232 loopback plug also

works for RS-422.

Connecting RJ45 Devices

You can use this information to connect serial devices to RJ45 connectors.

1. Connect your serial devices to the appropriate serial port on the DeviceMaster using the appropriate cable.

Note: Refer to the hardware manufacturer's installation documentation if you need help with connector pin outs or cabling for the peripheral device.

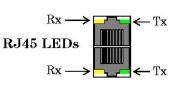
2. If the DeviceMaster has RX/TX LEDs, verify that the devices are communicating properly.

The RX (yellow) and TX (green) LEDs function accordingly when the cable is attached properly to a serial device.

- After power cycling the DeviceMaster, the RX/TX LEDs are off.
- The LEDs do not function as described until the port has been opened by an application. You can use Test Terminal to open a port or ports if you want to test a port or ports (<u>Testing Ports Using Test</u> <u>Terminal</u> on Page 154).

Mode	Serial Number Below xxxx-030000	Serial Number Above xxxx-030000
RS-232 RS-422	RX LEDs (yellow) are lit when connected to a valid RS-232 device TX LEDs (green) are lit during active data transmission	RX LEDs (yellow) are lit while receiving data
RS-485	RX LEDs (yellow) are lit while receiving data TX LEDs (green) are lit during active data transmission	TX LEDs (green) are lit during active data transmission
Where xxx	xx is the first four digits of the product serial n	umber.

3. You can refer to <u>Network and Device LEDs</u> on Page 167 for information about the remaining LEDs.



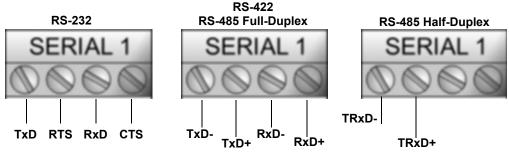
Four Screw Terminals (DM-2202)

This subsection discusses the following topics for the DM-2202 with 4 serial screw terminals. See <u>*Eight Screw*</u><u>*Terminals (DM-2402)*</u> on Page 97 if the DeviceMaster has eight serial terminals.

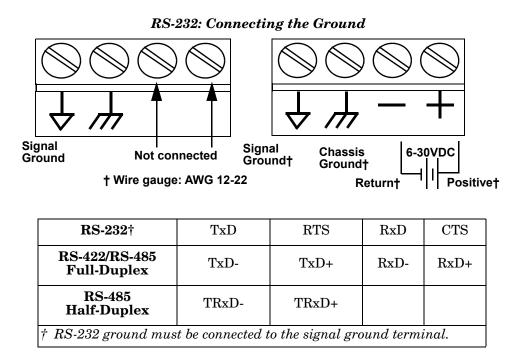
- <u>Serial Terminal (4) Connectors</u> on Page 94
- <u>Serial Terminal (4) Null-Modem Cables (RS-232)</u> on Page 95
- <u>Serial Terminal (4) Null-Modem Cables (RS-422)</u> on Page 95
- <u>Serial Terminal (4) Straight-Through Cables (RS-232/485)</u> on Page 96
- <u>Serial Terminal (4) Loopback Signals</u> on Page 96
- <u>Connecting Serial Devices</u> on Page 96

Serial Terminal (4) Connectors

Use the following table or drawings for signal information. The signals for SERIAL2 are the same as SERIAL1.



† Ground must be connected to the appropriate signal ground terminal.



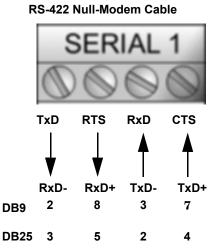
Serial Terminal (4) Null-Modem Cables (RS-232)

		SERIAL 1						
	0)	0	0				
	TxD	RTS	RxD	CTS				
	┥	↓		≜				
	RxD	стѕ	TxD	RTS				
DB9	2	8	3	7				
DB25	3	5	2	4				

An RS-232 null-modem cable is required for connecting DTE devices. RS-232 Null-Modem Cable

Serial Terminal (4) Null-Modem Cables (RS-422)

An RS-422 null-modem cable is required for connecting DTE devices.

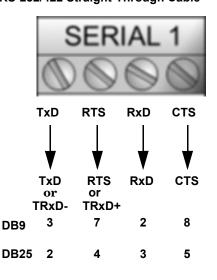


DB25 3 5 2 4 Note: PS 422 nin outo are not standardized. Each peripheral manufacturer uses different nin outs. Place

Note: RS-422 pin outs are not standardized. Each peripheral manufacturer uses different pin outs. Please refer to the documentation for the peripheral to determine the pin outs for the signals above.

Serial Terminal (4) Straight-Through Cables (RS-232/485)

RS-232 or RS-485 straight-through cables are used to connect modems and other DCE devices. RS-232/422 Straight-Through Cable

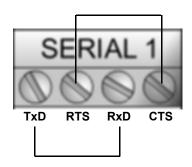


Serial Terminal (4) Loopback Signals

Use this drawing to wire a loopback, which is used in conjunction with application software (Test Terminal for Windows or minicom for Linux) to test serial ports.

Wire the terminals together to create a loopback.

- TxD to RxD
- RTS to CTS
- **Note:** You can use Test Terminal (Windows) or minicom (Linux) to test the serial port. You can refer to <u>Testing Ports Using Test Terminal</u> on Page 154 for Windows systems.



Connecting Serial Devices

Use the following information to connect the DM-2202 with serial terminals.

- 1. Connect your serial devices to the appropriate serial port on the DM-2202 using the appropriate cable. You can build your own cables or loopbacks using the appropriate discussions.
- **Note:** Refer to the hardware manufacturer's installation documentation if you need help with connector pin outs or cabling for the serial device.
- 2. You can refer to Network and Device LEDs on Page 167 for information about the LEDs.

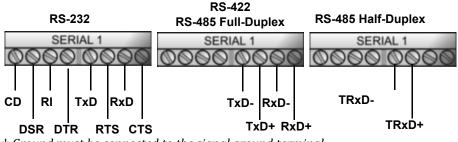
Eight Screw Terminals (DM-2402)

This subsection discusses the following topics for the DeviceMaster with 8 serial screw terminals.

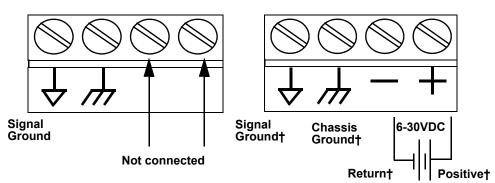
- <u>Screw Terminal (8) Connectors</u> on Page 97
- <u>Screw Terminal (8) Null-Modem Cables (RS-232)</u> on Page 98
- <u>Screw Terminal (8) Null-Modem Cables (RS-422)</u> on Page 98
- <u>Screw Terminal (8) Straight-Through Cables (RS-232/485)</u> on Page 99
- <u>Screw Terminal (8) Loopback Signals</u> on Page 99
- <u>Connecting Serial Devices</u> on Page 99

Screw Terminal (8) Connectors

Use the following drawings or table for signal information. The signals for SERIAL2 are the same as SERIAL1.



+ Ground must be connected to the signal ground terminal.



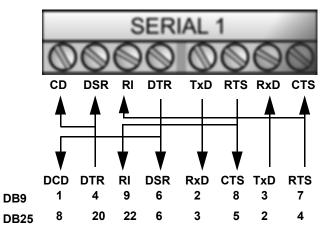




RS-232	CD	DSR	RI	DTR	TxD	RTS	RxD	CTS
RS-422/RS-485 Full-Duplex	N/A	N/A	N/A	N/A	TxD-	TxD+	RxD-	RxD+
RS-485 Half- Duplex	N/A	N/A	N/A	N/A	TRxD-	TRxD+	N/A	N/A
† Ground must be con	inected	to the a	ppropri	ate sig	nal ground	terminal.		

Screw Terminal (8) Null-Modem Cables (RS-232)

An RS-232 null-modem cable is required for connecting DTE devices.

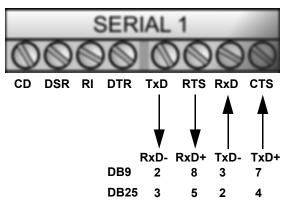


RS-232 Null-Modem Cable

Screw Terminal (8) Null-Modem Cables (RS-422)

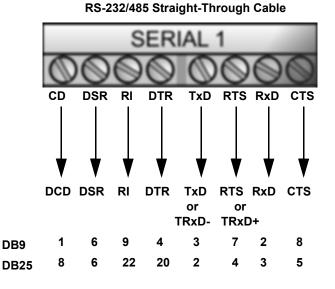
An RS-422 null-modem cable is required for connecting DTE devices.

RS-422 Null-Modem Cable



Screw Terminal (8) Straight-Through Cables (RS-232/485)

RS-232 or RS-485 straight-through cables are used to connect modems and other DCE devices.



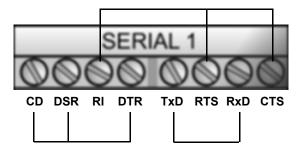
Screw Terminal (8) Loopback Signals

Use the drawing below to wire a loopback, which is used in conjunction with application software (Test Terminal or minicom) to test serial ports.

Wire the terminals together to create a loopback.

- TxD to RxD
- RTS to CTS to RI
- DTR to CD to DSR

Note: You can use Test Terminal (Windows) or minicom (Linux) to test the serial port. You can refer to <u>Testing</u> <u>Ports Using Test Terminal</u> on Page 154 for Windows systems.



Connecting Serial Devices

Use the following information to connect the DeviceMaster with 8 serial screw terminals.

- 1. Connect your serial devices to the appropriate serial port on the DeviceMaster using the appropriate cable.
- **Note:** Refer to the hardware manufacturer's installation documentation if you need help with connector pin outs or cabling for the serial device.
- 2. You can refer to <u>Network and Device LEDs</u> on Page 167 for information about the LEDs.

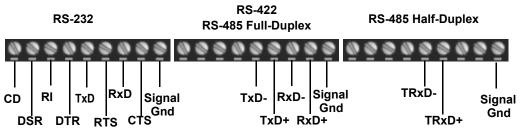
Nine Screw Terminals (DM-2201)

This subsection discusses the following topics for the DM-2201 with 9 serial screw terminals.

- <u>Screw Terminal Connectors (9)</u> on Page 100
- <u>Screw Terminal (9) Null-Modem RS-232 Cables</u> on Page 100
- <u>Screw Terminal (9) Null-Modem RS-422 Cables</u> on Page 101
- <u>Screw Terminal (9) RS-232/485 Straight-Through Cables</u> on Page 101
- <u>Screw Terminal (9) Loopback Signals</u> on Page 102
- <u>Connecting Serial Devices</u> on Page 102

Screw Terminal Connectors (9)

Use the following table or drawings for signal information.

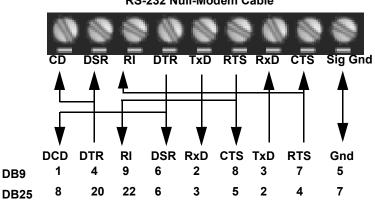


+ Ground must be connected to the signal ground terminal.

RS-232	CD	DSR	RI	DTR	TxD	RTS	RxD	CTS	Signal GND
RS-422/RS-485 Full-Duplex	N/A	N/A	N/A	N/A	TxD-	TxD+	RxD-	RxD+	Signal GND
RS-485 Half- Duplex	N/A	N/A	N/A	N/A	TRxD-	TRxD+	N/A	N/A	Signal GND
† Ground must be co	onnected	l to the s	ignal g	round te	rminal.				

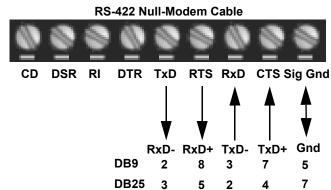
Screw Terminal (9) Null-Modem RS-232 Cables

An RS-232 null-modem cable is required for connecting DTE devices.



RS-232 Null-Modem Cable

Screw Terminal (9) Null-Modem RS-422 Cables



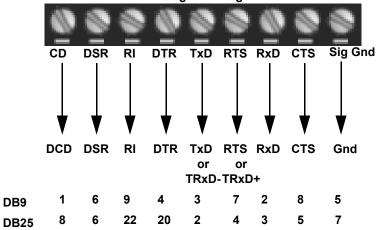
An RS-422 null-modem cable is required for connecting DTE devices.

Note: RS-422 pin outs are not standardized. Each peripheral manufacturer uses different pin outs. Please refer to the documentation for the peripheral to determine the pin outs for the signals above.

Screw Terminal (9) RS-232/485 Straight-Through Cables

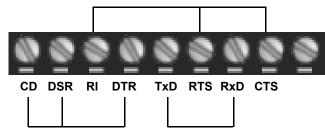
RS-232 or RS-485 straight-through cables are used to connect modems and other DCE devices.

RS-232/485 Straight-Through Cable



Screw Terminal (9) Loopback Signals

Use this drawing to wire a loopback, which is used in conjunction with application software (Test Terminal for Windows or minicom for Linux) to test serial ports.



Wire the terminals together to create a loopback.

- TxD to RxD
- RTS to CTS to RI
- DTR to CD to DSR

Note: You can use Test Terminal (Windows) or minicom (Linux) to test the serial port. You can refer to <u>Testing</u> <u>Ports Using Test Terminal</u> on Page 154 for Windows systems.

Connecting Serial Devices

Use the following information to connect the DeviceMaster with serial terminals.

- 1. Connect your serial devices to the appropriate serial port on the DeviceMaster using the appropriate cable. You can build your own cables or loopbacks using the appropriate discussions.
- **Note:** Refer to the hardware manufacturer's installation documentation if you need help with connector pin outs or cabling for the serial device.
- 2. You can refer to <u>Network and Device LEDs</u> on Page 167 for information about the LEDs.

Managing the DeviceMaster

This section discusses the following DeviceMaster maintenance procedures:

- Rebooting the DeviceMaster
- <u>Uploading SocketServer to Multiple DeviceMasters</u> on Page 104
- <u>Configuring Multiple DeviceMasters Network Addresses</u> on Page 105
 - **Note:** You can configure the network addresses for multiple DeviceMasters, configure common settings for the DeviceMasters, and save the settings to a configuration file that you can use to load settings up to all or selected DeviceMasters.
- <u>Adding a New Device in PortVision DX</u> on Page 105
- <u>Using the SocketServer Configuration Files</u> on Page 107
- <u>Using Driver Configuration Files</u> on Page 110
- <u>Changing the Bootloader Timeout</u> on Page 114, which discusses changing the Bootloader timeout
- <u>Managing Bootloader</u> on Page 116, which also discusses checking the Bootloader version and downloading the latest Bootloader
- <u>Restoring Factory Defaults (Specific Models)</u> on Page 119
- <u>Checking the NS-Link Version</u> on Page 118
- <u>Restoring Factory Defaults (Specific Models)</u> on Page 119
- Accessing SocketServer Commands in Telnet / SSH Sessions (PortVision DX) on Page 122
- <u>Accessing RedBoot Commands in Telnet / SSH Sessions (PortVision DX)</u> on Page 126
- **Note:** You can optionally refer to <u>RedBoot Procedures</u> on Page 131 if you want to perform procedures at the RedBoot level.

Rebooting the DeviceMaster

Method	Procedure
PortVision DX	Right-click the DeviceMaster or DeviceMasters in the <i>Device List</i> pane, click Advanced >Reboot and then Yes.
Portvision DX	<i>Note:</i> If security has been enabled in the web page, you will need to reboot the DeviceMaster in the web page.
Web page	System Reboot: You have 10 seconds to Cancel before the DeviceMaster automatically reboots. Optionally, you can click Reboot Now .
Telnet	Type reset.
	DeviceMaster DIN rail models have a Reset/Restore switch.
DeviceMaster DIN Rail Models	• If the Reset/Restore switch is depressed for less than 2 seconds, the DeviceMaster reboots.
	• If the Reset/Restore switch is depressed for greater than approximately 5 seconds it restores the DeviceMaster to the factory default values.

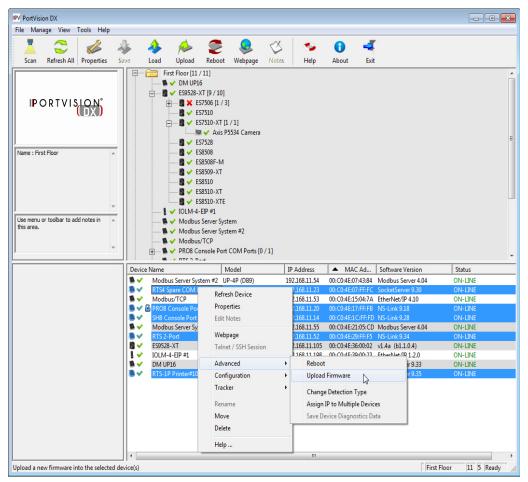
There are many ways to reboot the DeviceMaster.

Uploading SocketServer to Multiple DeviceMasters

If an older version of the NS-Link driver for Windows (before v9.xx) has been installed, make sure that the driver is disabled through the *Device Manager* before uploading SocketServer.

You can use this procedure if your DeviceMaster is connected to the host PC, laptop, or if the DeviceMaster resides on the local network segment.

- 1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 35) and Scan the network.
- 2. Shift-click the multiple DeviceMasters on the Main screen that you want to update and use one of the following methods:
 - Click the Upload button.
 - Right-click and then click Advanced > Upload Firmware.
 - Click Advanced >Upload Firmware in the Manage menu.



3. Browse, click the firmware (.cmtl) file, Open (*Please locate the new firmware*), and then click Yes (*Upload Firmware*).

It may take a few moments for the firmware to upload onto the DeviceMaster. The DeviceMaster reboots itself during the upload process.

4. Click Ok to the advisory message about waiting to use the device until the status reads ON-LINE.

In the next polling cycle, PortVision DX updates the *Device List* pane and displays the new firmware version.

Configuring Multiple DeviceMasters Network Addresses

You can configure the network addresses for multiple DeviceMasters using the Assign IP to Multiple Devices option.

In addition, you can also configure common settings for the DeviceMaster SocketServer or NS-Link web page and save the settings to a configuration file that you can load to all or selected DeviceMasters. See <u>Configuration File</u> on Page 124 for more information.

The DeviceMasters must be on the same network segment for this procedure to work. Use the following steps to configure multiple DeviceMasters.

- 1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 35) and **Scan** the network.
- 2. Shift-click the DeviceMasters for which you want to program network information, right-click, and click Advanced > Assign IP to Multiple Devices.
- 3. Enter the starting IP address, subnet mask, IP Gateway and click **Proceed**.

PortVision DX displays the programmed IP addresses in the *Device List* pane after the next refresh cycle.

Assign IP Addresses to Multiple Devices WARNING: Using invalid and/or duplicate IP addresses may cause serious network problems. It can also eliminate all TCP connections you have with these units. Cancel				
>>> Selected units will be rebooted after receiving the new IP information				
Use the same IP address	for all the selected devices			
Use the same IP address	for all the selected devices			

Adding a New Device in PortVision DX

You can add a new DeviceMaster manually, if you do not want to scan the network to locate and add new DeviceMasters, but there may be cases where you want to use the *Add New Device* window to:

- Configure DeviceMaster units that are not on the local network (remote) using <u>Remote Using the IP</u> <u>Address</u> on Page 105.
- Pre-configure a DeviceMaster in PortVision DX (local) using <u>Local Using the IP Address or MAC Address</u> on Page 106.

Remote Using the IP Address

Use the following procedure to add a remote DeviceMaster to PortVision DX.

- 1. Access the *New Device* window using one of these methods:
 - Click Add New > Device in the *Manage* menu.
 - Right-click a folder or a RocketLinx switch in the *Device Tree* pane (anywhere in the pane, as long as a DeviceMaster is not highlighted and you are in a valid folder) and click Add New > Device.
- 2. Select the appropriate DeviceMaster in the Device Type drop list.
- 3. Select the appropriate model in the **Device Model** drop list.
- 4. Enter a friendly device name in the Device Name list box.
- 5. Select **REMOTE** for the *Detection Type*.
- 6. Optionally, enter the serial number in the Serial Number list box.

7. Enter the IP Address for the DeviceMaster. It is not necessary to enter the Subnet Mask and Default Gateway.

dd New Device							x
General Settings						OK	1
Device Type : Dev	riceMaster RTS			-		Cancel	Sav
Device Model : Dev	iceMaster RTS 32-I	Port (RM)		•		Help	1
Device Name : First	Floor Print Server				-		_
Network Settings							
Detection Type :	REMOTE	•	IP Address :	192.	168.20	. 23	
Identification Mode :	IP	~	Subnet Mask :	255 .	255 . 0	. 0	
Serial Number :	89882-100053		Default Gateway :	192 .	168.0	. 254	
MAC Address :	00:C0:4E:	_					

- 8. Click Ok to close the Add New Device window. It may take a few moments to save the DeviceMaster.
- 9. If necessary, click **Refresh** for the new DeviceMaster to display in the *Device Tree* or *Device List* panes. The DeviceMaster shows OFF-LINE if it is not attached to the network or if an incorrect IP address was entered.

Local Using the IP Address or MAC Address

Use the following procedure to add a local DeviceMaster to PortVision DX if you do not want to scan the network.

- 1. Locate the network information or MAC address of the DeviceMaster you want to add.
- 2. Access the *New Device* window using one of these methods:
 - Click Add New > Device in the *Manage* menu.
 - Right-click a folder or a RocketLinx switch in the *Device Tree* pane (anywhere in the pane, as long as a DeviceMaster is not highlighted and you are in a valid folder) and click Add New > Device.
- 3. Select the appropriate DeviceMaster in the Device Type drop list.

d New Device				_ 0 🛃
General Settings Device Type : DeviceMaster RTS Device Model : DeviceMaster RTS 2-Port (2E) Device Name : Station #17		•		OK Cancel Help
Network Settings Detection Type : LOCAL	IP Address :			
Identification Mode : MAC	Subnet Mask :			
Serial Number : 006255	Default Gateway :		Ŀ.	
MAC Address : 00:C0:4E:29:FF:F2				

- 4. Select the appropriate model in the Device Model drop list.
- 5. Enter a friendly device name in the Device Name list box.
- 6. Select LOCAL for the *Detection Type*.

7. Enter the MAC address or network information.

Note: A MAC address label is attached to all DeviceMaster units. The first three pairs of digits start with 00 C0 4E.

- 8. Optionally, enter the serial number in the Serial Number list box.
- 9. Click Ok.
- 10. If necessary, click **Refresh** for the new DeviceMaster to display in the *Device Tree* or *Device List* panes. The DeviceMaster shows OFF-LINE if it is not attached to the network or if an incorrect IP address was entered.

Using the SocketServer Configuration Files

If you are deploying multiple DeviceMaster units that share common SocketServer values, you can save and load the configuration file (.dc) using either PortVision DX or the web interface.

- <u>PortVision DX Saving a SocketServer Configuration File</u>
- PortVision DX Loading a SocketServer Configuration File on Page 108
- <u>SocketServer Saving Configuration Files</u> on Page 109
- <u>SocketServer Loading Configuration Files</u> on Page 109
- **Note:** Configuration files saved before SocketServer 9.xx cannot be loaded onto a DeviceMaster with SocketServer versions above 9.xx.

If you save a configuration file using PortVision DX, you can choose what settings you want to save or load.

You may want to program the network settings in multiple DeviceMasters using <u>Configuring Multiple</u> <u>DeviceMasters Network Addresses</u> on Page 105.

Note: You can save device driver configuration settings if you have driver version 9.02 or higher. See <u>Using</u> <u>Driver Configuration Files</u> on Page 110 for procedures for saving and loading device driver configuration settings.

PortVision DX - Saving a SocketServer Configuration File

Use this procedure to save a configuration file using the PortVision DX Main screen.

- *Note:* Optionally, you can save a configuration file by accessing the Software Settings tab in the Properties screen and then clicking the Save Settings to a File button.
- 1. If you have not done so, install PortVision DX (*Installing PortVision* <u>DX</u> on Page 35) and **Scan** the network.
- 2. Highlight the DeviceMaster in the *Device List* pane that you want to save its configuration and use one of the following methods:
 - Click the Save button.
 - Right-click and then click **Configuration > Save**.
- 3. Browse to the location you want to save the file, enter a file name, and click **Save**.

Save Configuration	
Please select the fields you want to save.	
All All Default Galaxy SocketServer Settings SocketServer Settings	
Done	

- 4. Click the All check box or click only the properties that you want saved for each property page in the configuration file and click **Done**.
- 5. Click Ok to close the Save Configuration Completed message.

PortVision DX - Loading a SocketServer Configuration File

Use the following procedure to load a previously saved a DeviceMaster configuration file. Load a configuration file and apply it to a selected DeviceMaster or DeviceMasters from the *Main* screen or the **Software Settings** tab on the *Properties* screen.

Note: Configuration files saved before SocketServer 9.xx cannot be loaded onto a DeviceMaster with SocketServer versions above 9.xx.

Use this procedure to load a configuration file using the *Device List* pane to one or more DeviceMaster units.

- **Note:** The configuration file does not need to be the same model or port density. For example, the saved configuration file could be from a DeviceMaster PRO 8-port that you want to load on a DeviceMaster RTS 1-port.
- 1. Highlight the device or devices in the *Device List* pane that you want to load and use one of the following methods:
 - Click the Load button
 - Right-click and then click Configuration > Load
- 2. Click **Yes** to the warning that it will take 25 seconds per device and it may also reboot the devices.
- 3. Browse to the location of the configuration file, click the file name (.dc) and then **Open**.
- 4. Click the All check box or click only the properties that you want to load for each property page in the configuration file and then click Done.

Note: If you click All, every selected DeviceMasters will be programmed with the same IP address.

5. Close the Load Configuration popup message.

Save Configuration	
Please select the fields you want to save.	
All All Constraints All Constraints All Constraints Constraints Constraints Constraints Constraints Constraints Constraints Constraints	
Done	

Load Configuration
Please select the fields you want to Load.
- All - SocketServer Settings - NETWORK - SERVER - MAIL - PORT_1 - PORT_2
Done

SocketServer - Saving Configuration Files

You can use the procedure to save a configuration files using the web page.

- 1. If necessary, access SocketServer by entering the IP address in your web browser.
- 2. Click System | Configuration File.
- 3. Click the **Save Configuration** button.

COMTROL Home Port Network Diagnostic Update Firmware Configuration File System Sn Configuration File	
Save Configuration To save this DeviceMaster's configuration to a file on your PC, click "Save Configuration".	Load Configuration To load a configuration file to this DeviceMaster, select the file, and then click "Load Configuration". Configuration file: Browse Load Configuration
	© Copyright Comtrol Corp.

4. Save the configuration file to an appropriate location.

SocketServer - Loading Configuration Files

You can use this procedure to load SocketServer configuration files using SocketServer.

Note: You must have previously saved a configuration file to load.

- 1. If necessary, access SocketServer by entering the IP address in your web browser.
- 2. Click System | Configuration File.
- 3. Click the **Browse** button, highlight the configuration file, and click the **Open** button.
- 4. Click the Load Configuration button.

COMTROL	Home	Port N	letwork	Diagnostics	System	Help	DeviceMaster 8-pert Logout
Update Firmwa		nfiguratio	n File	System Snap	shot Re	store Defa	ults Reboot
Save Config To save this file on your F	, DeviceM	aster's co	onfigurat		To loa select	the file, a	ation uration file to this DeviceMaster, nd then click "Load Configuration". e: dm_SerialHub8.ds Browse
							© Copyright Comtrol Corp.

Using Driver Configuration Files

This subsection discusses how to create (save) and load driver configuration files. You may want to create driver configuration files for these reasons:

- Save the driver configuration settings so that you can load them on similar DeviceMasters to save configuration time
- Save the driver configuration settings because you need to remove a driver version to install a new driver version and you want to reload the driver configuration settings into the new driver

Device driver configuration files must be for the same model with the same port density. For example, you cannot load a DeviceMaster PRO configuration file onto a DeviceMaster RTS or a configuration file for a 32-port DeviceMaster RTS onto a 4-port DeviceMaster RTS.

Saving Driver Configuration Files

You must save the driver configuration file in portions:

- Device-level configuration parameters.
- Port configuration parameters. You must upload each port's configuration parameters separately.

Saving Device-Level Configuration

Use the following procedure to create and save a configuration file.

- 1. If necessary, open the *Driver Management Console* located under Comtrol> DeviceMaster Driver Management Console.
- 2. Depending on your operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* User Account Control message.
- 3. Highlight the DeviceMaster for which you want to save the driver configuration.
- 4. Click Save Configuration.

ACC STR		иtrol
DeviceMaster	General Advanced	
Port 1 (COM99)	Network Connection Mode	
Dead Port (COM500)	OMAC Mode 00 C0 4E 1C FF FD V Fetch IP Add	fress
	IPv4 Mode 10.0.0.14	
- S7510-XT (COM111)	I PV6 Mode FE80::2C0:4EFF:FE1C:FFFD	ings
ES9528-XT (COM105)	Reboot Dev	rice
ES8510-XTE (COM106)	Enable SSL Mode	
10.0.0.20 PRO	Certificate	is .
🖉 Port 01 (COM3)	Device Settings Device Name: DeviceMaster Serial Hub, 8 Port	
ES8508 (COM108)		
Port 03 - Spare port (COM4) Port 04 (COM5)	User-Friendly Device Name: 10.0.0.14_SH-8	
ES8510 (COM103)	Keep Alive Timeout (seconds): 120 (Default: 120)	
🦉 Open (COM98)	TCP Timeout Multiplier: 1 (Default: 1)	
	TCP Timeout Multiplier: 1 (Default: 1)	
= 10.0.0.22 # DIN->1	Scan Rate (ms): 10 V (Default: 10)	
Port 01 (COM15)	Verbose Event Log (Troubleshooting Only)	
ES9528-XT_v2 #2 (COM212)		
ES9528-XT_v2 #3 (COM213)		Defaults
(

5. Optionally, change the default file name and click Save.

흊 Save As				×
C→ × 1.	Vork_Files 🕨 Backup_Config_Files 🔹 😽	Search Backup_C	onfig_Files	٩
Organize 🔻 Ne	w folder		₩ •	•
📜 Libraries	^ Name	Date modified	Туре	
Documents Music Pictures Videos	No items match you	ır search.		
Description of the second seco				
	▼ €			۴
File name:	PRO-Console Ports.DCF			-
Save as type:	Driver Configuration File (*.DCF)			-
Hide Folders	[Save	Cancel	

6. Repeat the previous steps for each DeviceMaster for which you want to save the driver configuration.

Saving Port-Level Configuration

Use the following procedure to create and save a port configuration file. Port configuration, must be saved on a port-by-port basis.

- 1. If necessary, open the *Driver Management Console* located under Comtrol> DeviceMaster Driver Management Console.
- 2. Depending on your operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* User Account Control message.
- 3. Highlight the DeviceMaster for which you want to save the port-level configuration.
- 4. Highlight the port for which you want to save port configuration.

mtrol Drivers Management Console		¢.	OMTRO			
DeviceMaster	General					
Port 01 (COM5)	Port Settings BS Mode:	232 👻				
Port 03 (COM11)	Override and Lock Baud Rate to:	None -	RTS Toggle Options			
Port 05 (COM19) Port 05 (COM21) Port 07 (COM22)	Transmit Data Timeout on Port Close:	Terminator				
Port 08 (COM23) Port 09 (COM24) Port 10 (COM34) Port 10 (COM35) Port 11 (COM36) Port 11 (COM36) Port 12 (COM37)	Wait on Physical Transmission before Emulate Modem Hardware RING Sign Allow Parity Conflict (DeviceMaster 1 Block Plug-N-Play Search for Attache	al L Port only)	Defaults			
	Clone					
Control (COM41) C	Port Name User-Friendly Port Name: Port 01 COM Name: COM6 Renumber	All Subsequent Ports Relative	to This Port			
trol Drivers Management Console version 3.00 yright (C) 2011-2014 Comtrol Corporation.	Save Co	OK Cancel	Apply			

- 5. Click Save Configuration.
- 6. Repeat this process for each port for which you want to save the configuration settings.

Loading Driver Configuration Files

You must have previously saved a driver configuration file before you can load a configuration file.

The driver configuration file uploads in portions:

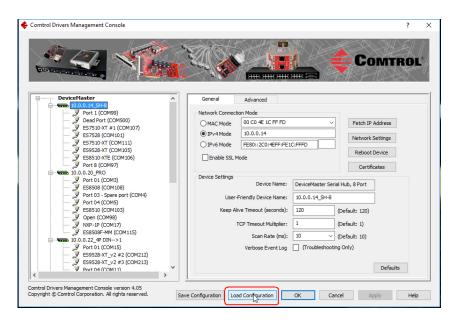
- Device-level configuration parameters.
- Port configuration parameters. You must upload each port's configuration parameters separately.

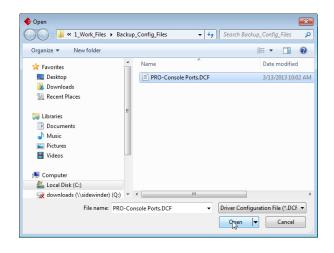
Loading Device Configuration

Use the following procedure to load the configuration file for device-level information for your DeviceMaster.

- 1. If necessary, open the *Driver Management Console* located under Comtrol> DeviceMaster Driver Management Console.
- 2. Depending on your operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* User Account Control message.
- 3. In the left pane, highlight the DeviceMaster for which you want to load the device-level settings from the configuration file.
- 4. Click Load Configuration.
- 5. Browse to the location of the configuration file that you want to load.
- 6. Highlight the configuration file and click **Open**. The configuration file loads in a few moments.
- 7. Make the appropriate choice for your situation:
 - Click No to the *ComtrolApplet* message, if you are using the file to set up multiple DeviceMasters with the same device-level settings.
 - Click Yes to the *ComtrolApplet* message, if you are using the file to restore a specific DeviceMaster. For example, you needed to remove and then reinstall the DeviceMaster NS-Link device driver.

ComtrolAp	plet	8
?	"MAC address", "IP address", "User-Friendly Device Name" may conflict with your current settings. Do you want to load these settings?	
	Yes No	6





- 8. Click Apply so that the configuration is saved on the DeviceMaster.
- 9. Go to the next procedure if you want to restore port settings from a configuration file.

Loading Port Configuration

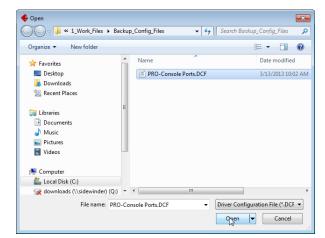
Use the following procedure to load the configuration file for port-level settings for your DeviceMaster.

- **Note:** Device driver configuration files must be for the same model with the same port density. For example, you cannot load a DeviceMaster PRO configuration file onto a DeviceMaster RTS or a configuration file for a 32-port DeviceMaster RTS onto a 4-port DeviceMaster RTS.
- 1. If necessary, open the *Driver Management Console* located under Comtrol> DeviceMaster Driver Management Console.
- 2. Depending on your operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* User Account Control message.
- 3. In the left pane, highlight the port for which you want to load the port-level settings from the configuration file.

E Comtrol Drivers Management Console			? 🔀		
		18278387 11	MTROL		
DeviceMaster	General				
DeviceMaster LT, 16 Port DeviceMaster RTS, 2 Port, 2E	Port Settings				
PRO - RocketLinx Console Ports	RS Mode:	232 T	TS Toggle		
ES8509-XT (COM102) ES8508 (COM108)	Override and Lock Baud Rate to:		Options		
Port 03 = Spare Port (COM12)	Transmit Data Timeout on Port Close:	0 v (seconds)			
Ess510-XTE (COM10) Ess510-XTE (COM10) Es7510 (COM104) Nor-IP (COM17) Ess508-MM (COM105) Ess508-MM (COM105) Ess608-MM (COM105)	Map 2 Stop Bits to 1 Mat on Physical Transmission before Completing Write Emulate Modern Hardware RING Signal Alow Parity Conflict (DeviceMaster 1 Port only) Block Plug-N-Play Search for Attached Serial Device Defaults				
RocketPort/RocketModem	Clone				
	Apply These Settings to All Ports				
	Port Name				
	User-Friendly Port Name: ES8510				
	COM Name: COM103	•			
	Renumber	r All Subsequent Ports Relative to This P	Port		
Comtrol Drivers Management Console version 3.00 Copyright (C) 2011-2014 Comtrol Corporation.	ve Configuration	OK Cancel Apply	y Help		

- 4. Click Load Configuration.
- 5. Browse to the location of the configuration file that you want to load.
- 6. Highlight the configuration file and click **Open**. The configuration file loads in a few moments.
- 7. Make the appropriate choice for your situation:
 - Click No to the *ComtrolApplet* message, if you are using the file to set up multiple DeviceMasters with the same port-level settings.
 - Click Yes to the *ComtrolApplet* message, if you are using the file to restore a specific DeviceMaster. For example, you needed to remove and then reinstall the DeviceMaster NS-Link device driver.





- 8. Click Apply so that the configuration is saved on the DeviceMaster.
- 9. Repeat <u>Steps 3</u> through 8 for each port that you want to restore.

Changing the Bootloader Timeout

If SocketServer fails during the upload process, you should change the Bootloader timeout value to 45 seconds.

Note: The DeviceMaster must be able to communicate using an IP address, which is compatible with this local network. If necessary, refer to <u>Configuring the Network Settings</u> on Page 38.

You must meet these requirement to use this procedure.

- NS-Link device driver assembly v10.xx or higher installed
- SocketServer v11.xx or higher loaded on the DeviceMaster
- PortVision DX installed
- Note: If you cannot meet these requirements, you can use RedBoot to change the timeout value. See <u>Changing</u> <u>the Bootloader Timeout</u> on Page 135.

PortVision DX - Changing Bootloader Timeout

Use the following procedure to change the Bootloader timeout to 45 seconds. You can use this procedure to return the Bootloader timeout to 15 seconds after you have successfully uploaded SocketServer.

- 1. If necessary, start PortVision DX, from Comtrol > PortVision DX > PortVision DX.
- 2. Right-click the DeviceMaster in the Device Tree or Device List pane and click Properties.
- 3. Type 45 in the **Bootloader Timeout** text box and click **Apply**.

General Software Settings \	Veb Interface						
		DeviceMas	ter PRO 8-Port (I	DB9)			
La construction	() () () () () () () () () ()	Rose TXS RATI TXI TXI TXI	Trase Trase Trase Trase Trase	7 RAT 7 TA7 107 3 TA3 70 70 70 70 70 70 70 70 70 70 70 70 70	۵ (:: 4	Posi • TX8 • CR44 • TX4 •	PWR
Device Name :	PRO - 17:FF:FB						
	00:C0:4E:17:FF	FB					
MAC Address :							
MAC Address : Serial Number :							
	ON-LINE	_			1.		
Serial Number :		▼ ▼			M		
Serial Number : Device Status :		v			M		
Serial Number : Device Status : Detection Type :	LOCAL	v			M		
Serial Number : Device Status : Detection Type : Network Settings	LOCAL	▼ ▼ . 11 . 20			V CE-MAST		
Serial Number : Device Status : Detection Type : Network Settings IP Mode :	LOCAL Static IP 192 . 168	▼ ▼ . 11 . 20 . 0 . 0		have the Bo	ootloader	Timeout	
Serial Number : Device Status : Detection Type : Network Settings IP Mode : IP Address :	LOCAL Static IP 192 . 168 255 . 255		it is in		ootloader hown in tl	Timeout his exam	ple, that

Note: You should return the Bootloader Timeout value back to 15 seconds after you upload SocketServer.

SocketServer - Changing Bootloader Timeout

Use the following procedure to change the Bootloader timeout to 45 seconds. You can use this procedure to return the Bootloader timeout to 15 seconds after you have successfully uploaded SocketServer.

- 1. If necessary, use your browser to access the DeviceMaster using the IP address.
- 2. Click Network.
- 3. Enter 45 in the **Boot Timeout** field and click **Save**.

COMTROL Home Port Network	Diagnostics System Help	DeviceMaster 1-port Logout
Configuration Password Security K Network Configuration	eys/Certs Email RFC1006	
General Host Name: RTS-1P Rx Polling: 50 ms TCP Keepalive: 60 s Boot Timeout: 45 S Telnet Timeout: 300 S	IPv4 Ouse DHCP Disable IPv4 networking Use static config below: Address: 10.0.0.65 Subnet Mask: 255.255.0.0 Gateway:	IPv6 Use DHCPv6 Disable IPv6 networking Use static config below: Address: :: Prefix Length: 64 Gateway: :: Link-Local: fe80::2c0:4eff:fe42:fff8
		© Copyright Comtrol Corp.

Note: You should return the Bootloader Timeout value back to 15 seconds after you upload the firmware.

Managing Bootloader

Bootloader refers to the operating system that runs on the DeviceMaster hardware during the power on phase, which then loads SocketServer.

Note: Typically, you should not update the Bootloader unless advised to do so by Comtrol Technical Support.

There are several methods and tools that you can use to check the Bootloader version or update the Bootloader.

- PortVision DX is the easiest way to check the Bootloader version and upload the latest version.
- Optionally, RedBoot can be used to check the Bootloader version and update the Bootloader. See <u>RedBoot</u> <u>Procedures</u> on Page 131 for procedures.

Checking the Bootloader Version

The following procedure uses PortVision DX to check the Bootloader version. Optionally, you can use RedBoot, see <u>Determining the Bootloader Version</u> on Page 135.

- 1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 35) and Scan the network.
- 2. Right-click the DeviceMaster in the *Device List* pane and click Advanced > Reboot.
- 3. Click Yes to the Confirm Reboot query.
- 4. Right-click the DeviceMaster in the *Device List* pane, click **Refresh.** You may need to do this several times until you catch the reboot cycle in the *Device List* pane. The Bootloader version is briefly displayed during the reboot cycle before <u>SocketServer</u> loads.
- 5. Check the Comtrol web site to see if a <u>later versionn</u> is available.
- 6. Go to the next subsection if you need upload a new version of Bootloader.

Uploading Bootloader

Use the following procedure to upload Bootloader to the DeviceMaster. Typically, you should not update the Bootloader unless advised to do so by Comtrol Technical Support or a notice has been posted to the firmware download page on the ftp site.

Note: Technical Support does not recommend updating Bootloader across a WAN. For best results, connect the DeviceMaster directly to a PC or laptop to upload Bootloader.



Make sure that power is not interrupted while uploading Bootloader. Power interruption while uploading Bootloader will require that the DeviceMaster must be sent into Comtrol so that it can be reflashed.

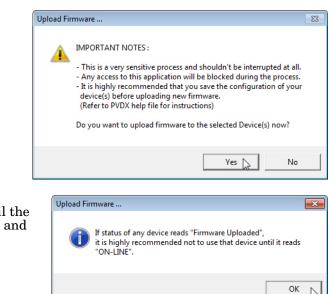
If you are not successful uploading SocketServer into the DeviceMaster, do not upload Bootloader.

If an older version of the NS-Link driver for Windows (before v9.xx) has been installed, make sure that the driver is disabled through the *Device Manager* before uploading Bootloader.

- 1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 35) and Scan the network.
- 2. If necessary, check the Bootloader version (*Checking the Bootloader Version*) and download the latest version.
- 3. Right-click the DeviceMaster for which you want to update, click Advanced > Upload Firmware, browse to the Bootloader .cmtl file, and then click Open.

IPV PortVis												<
File Mar	nage View	Tools Help										
	\sim	5	<u></u>	1		S 🙎	$\mathbf{\nabla}$	- Carlos - C	🔒 🚽			
Scan	Refresh All	O/	Save	Load	, -		-	Help				
Scan	Kerresh Ali	Properties				leboot Webpa	ige Notes	нер	About Exit			_
IP (ORTVIS	LON [°] (DX)		Fo	rst Floor [11 / 11 ourth Floor [28 / an Results [13 / cond Floor [4 / 4 hird Floor [2 / 4]	29] 13]						
Name : Fir	st Floor											
		-										
		lal as a base ba	- 11									
Use menu this area.	or toolbar to ad	id notes in 🔺	`									
		-			Righ	nt-click the	DeviceMa	ster that	you want to u	ipdate.		
			Devic	e Name		Model	1	P Address	A MAC Ad	Software Version	Status	-
					us Server System	#2 UP-4P (DB9		92.168.11.54		Modbus Server 4.04	ON-LINE	
				RTC	00110	DTO 10 /01		92.168.11.23		SocketServer 9.35	ON-LINE	
				Mc	Refresh Devic	ce		92.168.11.53	00:C0:4E:15:04:7A		ON-LINE	
	شه دونه دونه	in an		🕄 PR	Properties)) 1	92.168.11.20	00:C0:4E:17:FF:FB	NS-Link 9.35	ON-LINE	
		-	🖉 🖉 🗸	SH	Edit Notes		1	92.168.11.14	00:C0:4E:1C:FF:FD	NS-Link 9.35	ON-LINE	
				Mc				92.168.11.55		Modbus Router 6.05	ON-LINE	
				RT	Webpage			92.168.11.52	00:C0:4E:29:FF:F5		ON-LINE	
	or toolbar to ad	ld notes in 🛛 🔺	T 🖣 🌱	ESS	Telnet / SSH	Session		92.168.11.105	00:C0:4E:36:00:02		ON-LINE	
this area.								92.168.11.198	00:C0:4E:39:00:23	EtherNet/IP 1.2.0 SocketServer 9.35	ON-LINE ON-LINE	
					Advanced		Reboot			SocketServer 9.35	ON-LINE ON-LINE	
				NI.	Configuratio	n 🕨	Opload	Firmware		SUCKELSEIVER 5.55	ON-LINE	
					Tracker	+	Change	Detection Typ	pe			
					Rename		Assign I	P to Multiple I	Devices			
					Move		Save De	vice Diagnosti	ics Data			
					Delete							
					Help							
		-		_	ricip		1					F
Upload a n	ew firmware in	nto the selected	device(s)							Fi	rst Floor 11 1 Ready	

4. Click **Yes** to the *Upload Firmware* message that warns you that this is a sensitive process.



- 5. Click Ok to the second Upload Firmware message.
- 6. Right-click the DeviceMaster and click **Refresh** until the Bootloader version displays in the *Device List* pane and verify that the new version loaded.

Checking the NS-Link Version

Use this procedure to check the NS-Link web page version. Remember, an NS-Link version displays when the NS-Link device driver has been installed and configured, NS-Link is the same firmware as SocketServer.

- 1. Start PortVision DX.
- 2. If necessary, click Scan to locate the DeviceMaster.

IPV PortVision DX							×
File Manage View Tools Help							-
Scan Refresh All Properties Save	Load Upload Rebo	ot Webpage Note	s Help	6 4 About Exit			
Name : First Floor	This shows the fo DeviceMaster P DeviceMaster R	3] (1 / 1) s P5534 Camera f f llowing: serial Hub with th RO with the dev iTS 2-Port with S	ice driver lo SocketServe	aded using S er 7.31.			ж.
	 Device Master R Device Master R 	TS 4-Port with S TS 1-Port with S					-
Devi	ice Name	Model	IP Address	MAC Address	▲ Software Versio	n Status	
	IOLM-4-EIP #1	4-EIP	192.168.11.198	00:C0:4E:39:00:23	EtherNet/IP 1.2.0	ON-LINE	
		UP-1P (5V)	192.168.11.53	00:C0:4E:15:04:7A		ON-LINE	
		UP-1P (5-30V)	192.168.11.55	00:C0:4E:21:05:CD	Modbus Router 6.05	ON-LINE	
= 1 🕵 🗸		UP-16P (2E)	192.168.11.60	00:C0:4E:40:00:5D	Modbus Router 6.05	ON-LINE	
	Modbus Server System #2	UP-4P (DB9)	192.168.11.54	00:C0:4E:07:43:84	Modbus Server 4.04	ON-LINE	
S	SH8 Console Port COM P	SH-8P (DB9)	192.168.11.14	00:C0:4E:1C:FF:FD	NS-Link 8.04	ON-LINE	
B 🗸	PRO8 Console Port COM	PRO-8P (DB9)	192.168.11.20	00:C0:4E:17:FF:FB	NS-Link 9.18	ON-LINE	
	RTS 2-Port	RTS-2P (2E)	192.168.11.52	00:C0:4E:29:FF:F5	SocketServer 7.31	ON-LINE	
N	RTS4 Spare COM Ports	RTS-4P (DB9)	192.168.11.23	00:C0:4E:07:FF:FC	SocketServer 9.18	ON-LINE	
1 No. 1		RTS-1P (5-30V)	192.168.11.40	00:C0:4E:42:FF:F8		ON-LINE	
- B -	ES9528-XT	ES9528-XT	192.168.11.105	00:C0:4E:36:00:02	vi.4a (b1.1.0.4)	ON-LINE	
<							•
For Help, press F1					Fir	st Floor 11 0 Ready	1 //.

The Device List pane displays the NS-Link (SocketServer) version.

3. Check the Comtrol ftp site to see if a later version is available.

To check the NS-Link version, you will need to check to see what version of SocketServer is available.

You can use this link to check to see what version of SocketServer/NS-Link is available at: <u>http:/</u> <u>downloads.comtrol.com/</u> <u>dev_mstr/rts/software/</u> SocketServer/. downloads.comtrol.com -/dev_mstr/rts/software/socketserver/ [To Parent Directory] 10/14/2015 10:54 AM 148450 1800456 SocketServer History.pdf 9/2/2014 9:50 AM 172465 DeviceMaster Binary Format.pdf 5/7/2015 12:44 PM 92973 DeviceMaster ProductNotice.pdf 5/8/2015 11:10 AM <dir> help 10/13/2015 5:27 PM 1188657 socketServer-10.06.cmt1

4. Compare the version number displayed in PortVision DX to the version displayed in the downloads directory.

- 5. If a higher version of SocketServer is available and you want to update the DeviceMaster with the latest software:
 - a. Update SocketServer using <u>Uploading SocketServer with PortVision DX</u> on Page 42.
 - b. Download the latest driver from <u>http://downloads.comtrol.com/dev_mstr/rts/drivers/win7</u>.



c. Update to the latest driver using the <u>DeviceMaster Device Driver (NS-Link) User Guide</u>, which can be downloaded using<u>Locating Software and Documentation</u> on Page 11.

Restoring Factory Defaults (Specific Models)

Use the following procedures to restore the DeviceMaster DIN rail models to the factory defaults.

To return to default port settings, see <u>Restoring Serial Port Settings</u> on Page 120.

Note: For other models, see <u>Returning the DeviceMaster to Factory Defaults</u> on Page 171.

If Technical Support advises you to restore the DeviceMaster factory defaults, depress the **Reset/Restore** switch for greater than 5 seconds.

Restoring the DeviceMaster DIN rail models resets the following to their factory defaults:

- Port settings
- Network settings
- Password
- Telnet enable
- Start up time-out
- SSL enable
- Telnet time-out

Restoring Serial Port Settings

Use the web page and/or the NS-Link device driver for Windows to restore the serial port settings to their default values.

The NS-Link serial port settings are independent of the socket serial port settings on the web page. If you are using COM ports and also have configured the port for socket services, you must restore the default port settings in the driver and web page.

NS-Link COM Port

You can use this procedure to reset NS-Link serial port settings.

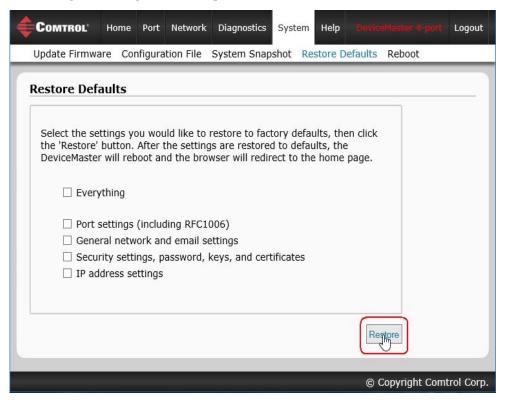
- 1. Open the *Driver Management Console* using Comtrol > DeviceMaster Driver Management Console.
- 2. Highlight the first port that you want reset to default values.
- 3. Click the **Defaults** button (and if appropriate, **Clone**).
- 4. Click Apply or Ok.

If necessary, you can reset DeviceMaster device properties to their defaults on the *Device General* tab using the **Defaults** button.

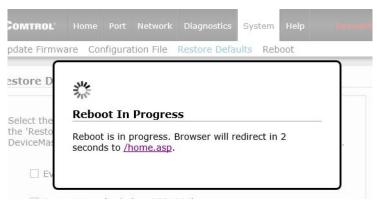
Socket Port

Use the following procedure to reset the socket port serial settings.

- 1. Open the DeviceMaster web page (Accessing Socket Configuration on Page 63).
- 2. Click System | Restore Defaults.
- 3. Click the Port Settings (including RFC1006) option and then click Restore.



You will be able to log in after the reboot cycle.



Accessing SocketServer Commands in Telnet/SSH Sessions (PortVision DX)

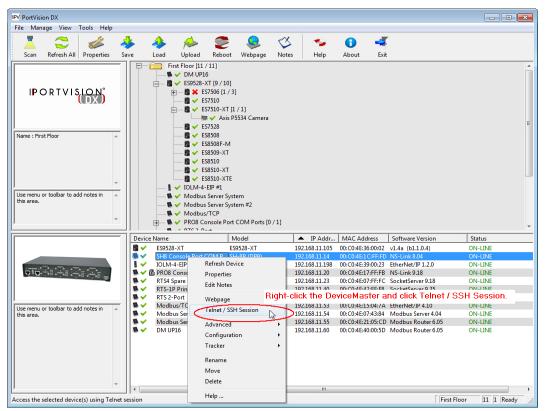
You can open a Telnet or SSH session using PortVision DX. Use the appropriate procedure for your site:

- <u>Telnet Session</u> (below)
- <u>SSH Session</u> on Page 124

Telnet Session

Use the following procedure to access a telnet session with PortVision DX.

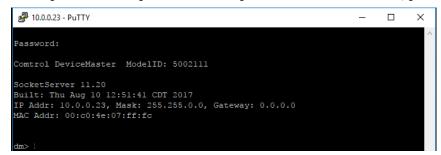
1. In PortVision DX, PortVision DX, right-click the DeviceMaster in the *Device List* pane for which you want to open a telnet session, and click **Telnet/SSH Session**.



2. Leave the popup set to Telnet and Selected Port 23, and click Ok.

Telnet / SSH Settin	gs	×
☞ Telnet ⊂ SSH	Selected Port : 23	
	OK Cancel	

3. If necessary, enter the password and press Enter. If a password has not been set, press Enter.



4. You can type help to refer to available commands supported by SocketServer/NS-Link.

dm> help	
auth	 Set the authentication method used by web server
help	- help [cmd] - Display help information
ірб	- Set IPv6 configuration
ip	- Set IP configuration
logdump	- Dump diagnostic log
mac	- Show MAC address
model	- View the Model ID
monitor	- Monitor seral port data
password	- Set the password
reset	- Resets the device
secureconf	- Enable/disable encryption for config
securedata	- Enable/disable encryption for data
securemon	- Enable/disable monitoring of secure data via telnet
setbaud	- Set the baud on any or all ports
nshosts	- Show connected NSLink hosts
showtables	- show config tables
snmp	- Enable/disable SNMP
telnet	- Enable/disable telnet
teltimeout	- Set the telnet timeout period (seconds)
timeout	- Set time (seconds) until default application loads automatically
ver	- Display firmware revision
quit	- Exit session

SSH Session

Use the following procedure to access an SSH session with PortVision DX.

1. In PortVision DX, PortVision DX, right-click the DeviceMaster in the *Device List* pane for which you want to open an SSH session, and click **Telnet/SSH Session**.

IPV PortVision DX								×
File Manage View Tools Help								
		. 👝 🍙		-	6 4	r		
📥 🥣 🍼	ፉ 🦑 آ				· ·			
Scan Refresh All Properties Sav	e Load Uplo	ad Reboot Webp	age Notes	Help	About Exit			
	🖃 🚞 First Floor	[11 / 11]						*
	🐌 🛩 DM							
		528-XT [9 / 10]						
PORTVISION		K ES7506 [1 / 3]						
		ES7510						
		ES7510-XT [1 / 1] ES7510-XT [1 / 1] Axis P5534 Car						
		AXIS P3354 Car ES7528	nera					E
Name : First Floor		ES8508						
Name : Filst floor		ES8508F-M						
		ES8509-XT						
	n n n n n n n n n n n	ES8510						
		ES8510-XT						
_		ES8510-XTE						
-		M-4-EIP #1						
Use menu or toolbar to add notes in 🔺		dbus Server System						
		dbus Server System #2						
-		dbus/TCP						
P	🕀 👘 💭 PRC	8 Console Port COM Po	rts [0 / 1]					-
	Device Name	Model		IP Addr	MAC Address	Software Version	Status	
	■ ✓ ES9528-XT	ES9528-XT		92.168.11.105	00:C0:4E:36:00:02	v1.4a (b1.1.0.4)	ON-LINE	
	SH8 Console			92.168.11.14	00:C0:4E:1C:FF:FD		ON-LINE	
	IOLM-4-EIP	Refresh Device		92.168.11.198	00:C0:4E:39:00:23		ON-LINE	
	PRO8 Conse RTS4 Spare	Properties		92.168.11.20 92.168.11.23	00:C0:4E:17:FF:FB	NS-Link 9.18 SocketServer 9.18	ON-LINE ON-LINE	
	RTS-1P Prin	Edit Notes		02.100.11.25 02.168.11.40		SocketServer 9.10	ON-LINE	
	RTS 2-Port	Webpage				nd click Telnet I		
Use menu or toolbar to add notes in	Modbus/TC			92.168.11.53	00:C0:4E:15:04:7A		ON-LINE	
this area.	🐞 🖌 🛛 Modbus Ser 🗠	Telnet / SSH Sessior		92.168.11.54		Modbus Server 4.04	ON-LINE	
	📕 🖌 🛛 Modbus Ser	Advanced	+ 1	92.168.11.55		Modbus Router 6.05	ON-LINE	
	Sec. 2010 DM UP16	Configuration	▶ ¹	92.168.11.60	00:C0:4E:40:00:5D	Modbus Router 6.05	ON-LINE	
		Tracker						
		Rename						
		Move						
		Delete						
	•	11.1.						P.
Access the selected device(s) using Telnet se	ssion	Help				First	Floor 11 1 Ready	1.

- 2. Click SSH and leave the port number at the default.
- 3. If necessary (depending on the operating system), respond to the security notification.

PuTTY Sec	curity Alert	×
	The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is. The server's rsa2 key fingerprint is: ssh-rsa 1024 ad:c8:06:61:b1:19:28:04:5f:86:32:20:7d:91:d8:b1 If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting. If you want to carry on connecting just once, without adding the key to the cache, hit No. If you do not trust this host, hit Cancel to abandon the connection.	
	Yes N Cancel Hel	,

Telnet / SSH Settings	—
C Telnet ☞ SSH	Selected Port : 22
(DK Cancel

- 4. Press Enter.
 - Note: The DeviceMaster does not have a user name.
- 5. If necessary, enter the password and press Enter. If a password has not been set, press Enter.

6. You can type help to refer to available SocketServer/NS-Link commands.

🗬 10.0.0.23 - P	ם – דיזע איזדע	×
Password:		^
Comtrol Devi	iceMaster ModelID: 5002111	
SocketServer	r 11.20	
Built: Thu 7	Aug 10 12:51:41 CDT 2017	
	.0.0.23, Mask: 255.255.0.0, Gateway: 0.0.0.0	
):c0:4e:07:ff:fc	
dm> help		
auth	- Set the authentication method used by web server	
help	- help [cmd] - Display help information	
ip6	- Set IPv6 configuration	
ip	- Set IP configuration	
Logdump	- Dump diagnostic log	
nac	- Show MAC address	
model	- View the Model ID	
monitor	- Monitor seral port data	
password	- Set the password	
reset	- Resets the device	
secureconf		
securedata		
securemon	 Enable/disable monitoring of secure data via telnet 	
setbaud	 Set the baud on any or all ports 	
nshosts	- Show connected NSLink hosts	
showtables		
snmp	- Enable/disable SNMP	
telnet	- Enable/disable telnet	
teltimeout		
timeout		ΥΥ
ver	- Display firmware revision	
quit	- Exit session	
dm>		

Accessing RedBoot Commands in Telnet/SSH Sessions (PortVision DX)

You can open a Telnet or SSH session using PortVision DX to access RedBoot commands.

Use the following procedure to access a telnet or SSH session with PortVision DX.

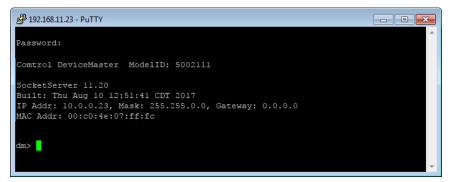
1. In PortVision DX, PortVision DX, right-click the DeviceMaster in the *Device List* pane for which you want to open a telnet session, and click **Telnet/SSH Session**.

IPV PortVision DX								×
File Manage View Tools Help								
Scan Refresh All Properties	interior in the second	-	age Notes	🥌 Help	About Exit			
PORTVISION®		[11 / 11]		<u> </u>				
this area.	■ ✓ Mo ■ ✓ Mo	dbus Server System #2 dbus/TCP 08 Console Port COM Pe	orts [0 / 1]					÷
	Device Name	Model		IP Addr	MAC Address	Software Version	Status	
	■ 🗸 ES9528-XT	ES9528-XT	19	2.168.11.105	00:C0:4E:36:00:02	v1.4a (b1.1.0.4)	ON-LINE	
	SH8 Console		1.	2.168.11.14	00:C0:4E:1C:FF:FD		ON-LINE	
11	IOLM-4-EIP	Refresh Device		2.168.11.198	00:C0:4E:39:00:23		ON-LINE ON-LINE	
	RTS4 Spare	Properties		2.168.11.20	00:C0:4E:17:FF:FB 00:C0:4E:07:EE:EC	SocketServer 9.18	ON-LINE ON-LINE	
	RTS-1P Prin	Edit Notes	10	2 168 11 /0	00-C0-4E-42-EE-E8	SocketSenier 0.35	ONLUNE	
	RTS 2-Port	Webpage	-			nd click Telnet /		
Use menu or toolbar to add notes in 🔺	Modbus/TC	Telnet / SSH Session		2.168.11.53	00:C0:4E:15:04:/A	EtherNet/IP 4.10 Modbus Server 4.04	ON-LINE	
this area.	Modbus Ser			2.168.11.54		Modbus Server 4.04 Modbus Router 6.05	ON-LINE ON-LINE	
	DM UP16	Advanced	1	2.168.11.60		Modbus Router 6.05	ON-LINE	
		Configuration						
		Tracker	•					
		Rename						
		Move						
-		Delete						
Ľ		Help						+
Access the selected device(s) using Telnet	session	neip				First	t Floor 11 1 Ready	1 //

2. Select Telnet or SSH, leave the Selected Port number, and click Ok.

Telnet / SSH Settings	Telnet / SSH Settings
Telnet Selected Port: 23 SSH	C Telnet Selected Port : 22
OK Cancel	OK Cancel

3. If necessary, enter the password and press Enter. If a password has not been set, press Enter. If using an SSH session, press Enter to the login as prompt.



- **Note:** If the PuTTY screen flashes in the background and does not appear as shown above, make sure that **Enable Telnet/ssh** has not been disabled in SocketServer. To check this, return to PortVision DX, right-click the DeviceMaster in the Device List pane, and click **Webpage**. Click the **Security** tab and if necessary, verify that the **Enable Telnet/ssh** option is enabled, If it is not, click the option and then click **Save**, and close SocketServer.
- 4. Type **Reset**, press **Enter**, and close the telnet session.

子 192.168.11.23 - PuTTY	x
Password:	^
Comtrol DeviceMaster ModelID: 5002111	
SocketServer 11.20 Built: Thu Aug 10 12:51:41 CDT 2017 IP Addr: 10.0.0.23, Mask: 255.255.0.0, Gateway: 0.0.0.0 MAC Addr: 00:c0:4e:07:ff:fc	
dm> reset	-

5.	Quickly re-oper	the telnet or	SSH session	using the	previous steps.
.	quitting 10 open		0011 00001011	un and and	providence Stopst

IPV PortVision DX						
File Manage View Tools Help						
Scan Refresh All Properties Sa	sve Load Upload	Reboot Webpage	Notes Help	🚹 🚽		
IPORTVISION Name : First Floor		16 -XT [9 / 10] ES7506 [1 / 3] ES7510 K[/ 1] ■ ✓ Axis P5534 Camera ES510-XT [1 / 1] ■ ✓ ES508 ES508-M ES509-XT ES509-XT ES510-XT ES51	//1]			E
	Device Name	Model	IP Addr	MAC Address	Software Version	Status
	ES9528-XT	ES9528-XT	192.168.11.105	-		ON-LINE
	Image: SH8 Console Date Image: SH8 Console Date	COM D SHARD (DRO) Refresh Device Properties Edit Notes	192.168.11.14 192.168.11.198 192.168.11.20 192.168.11.23 192.168.11.40	00:C0:4E:39:00:23 00:C0:4E:17:FF:FB	EtherNet/IP 1.2.0 NS-Link 9.18 SocketServer 9.18	ON-LINE ON-LINE ON-LINE ON-LINE
	RTS 2-Port	Webpage	light-click the De			SSH Session.
Use menu or toobar to add notes in 🔺	Modbus/TC Modbus Ser Modbus Ser Modbus Ser	Telnet / SSH Sersion	192.168.11.53 192.168.11.54 192.168.11.55 192.168.11.60	00:C0:4E:21:05:CD	EtherNet/IP 4.10 Modbus Server 4.04 Modbus Router 6.05 Modbus Router 6.05	ON-LINE ON-LINE ON-LINE ON-LINE
		Move Delete				, , , , , , , , , , , , , , , , , , ,
Access the selected device(s) using Telnet s	ession	Help			First	Floor 11 1 Ready

6. Select Telnet or SSH, leave the Selected Port number, and click Ok.

Telnet / SSH Settings	Telnet / SSH Settings	x
© Telnet Selected Port : 23	C Telnet Selected Port : 22	
OK Cancel	OK Cancel	

7. Press Enter. You can type help to review the RedBoot commands. You can also refer to <u>RedBoot Command</u>. <u>Overview</u> on Page 137.

P 10.0.0.23 - PuTTY	<u></u>	×
ver		^

<pre>** Comtrol DeviceMaster Bootloader 4.25 ** Platform: Comtrol DeviceMaster (ARM 7TDMI) ** RedBoot(tm) environment - built 17:03:01, Oct 25 2016 ** Portions Copyright (C) 2000, Red Hat, Inc. ** Portions Copyright (C) Comtrol Corp. **</pre>		

<pre>RAM: 0x0000000-0x007c0000 [0x0000000-0x007b0000 available] FLASH: 0x0500000-0x053fffff, 64 x 0x10000 blocks RedBoot> help Set/show web authentication auth [noaccess,none,basic,md5,invalid] Show/set Board revision boardrev [rev-number] Manage machine caches cache [ON OFF] Display/switch console channel</pre>		
channel [-1 <channel number="">]</channel>		
Show chassis type (RTS, DM2, LT or UP) chassis		
Compute a 32bit checksum [POSIX algorithm] for a range of memory cksum -b <location> -1 <length> Clear application configuration clearconfig</length></location>		
Disable program loading (auto/default and ns-link)		
disable Manage FLASH images fis (cmds)		
Show flash info		
flash Execute code at a location		
<pre>go [-w <timeout>] [-c] [-n] [entry] Help about help?</timeout></pre>		
help [<topic>]</topic>		
Display command history		
history		
Show/set IP address config		
ip [addr mask gateway]		×

Note: The dm prompt should be replaced by a redboot prompt. If not, you can reset the Bootloader timeout for a longer time period and retry this procedure.

RedBoot Procedures

You can use this section as a reference if you want to perform tasks in RedBoot.

- <u>Accessing RedBoot Overview</u> on Page 131
- <u>Establishing a Serial Connection</u> on Page 132
- <u>Establishing a Telnet Connection</u> on Page 133
- <u>Determining the Network Settings</u> on Page 134
- <u>Configuring the Network Settings</u> on Page 134
- <u>Changing the Bootloader Timeout</u>, Page 135
- <u>Determining the Bootloader Version</u> on Page 135
- <u>Resetting the DeviceMaster</u> on Page 136
- <u>Configuring Passwords</u> on Page 136
- <u>RedBoot Command Overview</u> on Page 137.

Optionally, you can install PortVision DX on a Windows system on the network and perform all of these tasks. PortVision DX provides a Telnet/SSH session, which is discussed in <u>Accessing RedBoot Commands in Telnet/SSH Sessions (PortVision DX)</u> on Page 126.

Accessing RedBoot Overview

To access RedBoot, you can use one of the following methods:

• A *serial* connection between Port 1 on the DeviceMaster and a COM port on a PC (Page 132). If you plan on using the serial method, you will need a null modem cable, a terminal program installed and configured on the PC, and a **Bootloader Timeout** value in excess of 15 seconds. If the **Bootloader Timeout** value has been reduced to 1 second, this procedure will NOT be possible.

Note: Use the serial connection method, if the DeviceMaster is not on the same Ethernet network segment as the PC.

If you do not know the IP address of the DeviceMaster you must use a serial connection to communicate with the DeviceMaster.

• A *telnet* connection (Page 133), if the DeviceMaster is locally accessible by Ethernet. A *telnet* connection requires that you know the IP address. In addition, the IP address must also be valid for the network to which it is attached.

For example: The network segment must be 192.168.250.x to telnet to the DeviceMaster default IP address if you have not changed the IP address to operate on your network.

Establishing a Serial Connection

Use the following procedure to set up a serial connection with a terminal server program. You can use HyperTerminal (Windows) or Minicom (Linux) or optionally, Test Terminal (WCom2), which can be accessed from PortVision DX using Tools > Applications > Test Terminal (WCom2).

- Connect a null-modem cable from an available COM port on your PC to Port 1 on the DeviceMaster. Note: See <u>Connecting Serial Devices</u> on Page 87, if you need to build a null-modem cable.
- 2. Configure the terminal server program to the following values:
 - Bits per second = 57600
 - Data bits = 8
 - Parity = None
 - Stop bits = 1
 - Flow control = None
 - Note: If you do not disable Bootloader from loading (Steps 3 through 5) within the time-out period (default is fifteen seconds), an application will be loaded from flash and started. If this happens, repeat Steps 3 through 5. The #!DM command is the only case-sensitive command and must be in uppercase.
- 3. Reset the DeviceMaster.

Note: Depending on the model, disconnect and reconnect the power cable (external power supply and no power switch) or turn the power switch on and then off (internal power supply).

4. Immediately type #!DM and press Enter in the terminal program.

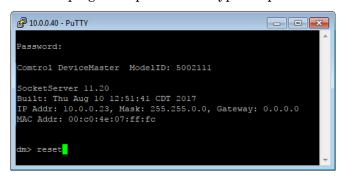


- 5. At the **RedBoot>** prompt, type **dis**, and press **Enter**.
- 6. Verify that loading has been disabled.
- 7. You can use the appropriate procedure listed on Page 131 or use the <u>*RedBoot Command Overview*</u> on Page 137 to perform the desired task.

Establishing a Telnet Connection

Use the following procedure to telnet to the DeviceMaster.

- Open a telnet session, enter the DeviceMaster IP address. If using Windows, you can use PortVision DX, see <u>Accessing RedBoot Commands in Telnet / SSH Sessions</u> (<u>PortVision DX</u>) on Page 126.
- 2. Press the Enter key if you did not program a password or type the password and press Enter.



Note: The DeviceMaster does not come pre-programmed with a password.

- 3. Type reset, and close the session.
- 4. Open a new telnet session, enter the DeviceMaster IP address, and the password.
- 5. Type **dis** to disable the Bootloader.
- 6. Verify that the system responds with a Loading disabled message.

學 10.0.0.40 - PuTTY	
ver	

* *	
** Comtrol DeviceMaster Bootloader 4.25	
** Platform: Comtrol DeviceMaster (ARM 7TDMI)	
<pre>** RedBoot(tm) environment - built 17:03:01, Oct 25</pre>	2016
** Portions Copyright (C) 2000, Red Hat, Inc.	
** Portions Copyright (C) Comtrol Corp.	
**	
******************	=
RAM: 0x10000000-0x10018000 [0x1000168c-0x1000bb46 ava	ilable]
0x10080000-0x1008a000 [0x10080000-0x1008a000 ava	
0x20000000-0x20010000 [0x20000000-0x20010000 ava	ilable]
0x28000000-0x29000000 [0x28000000-0x29000000 ava	ilable]
FLASH: 0x14000000-0x147fffff, 2048 x 0x1000 blocks	
RedBoot> dis	
Loading disabled	
RedBoot>	-

Determining the Network Settings

If you are not sure what the network information is on a DeviceMaster, you can perform the following procedure.

The default network settings are:

- IP address: 192.168.250.250
- Subnet mask: 255.255.0.0
- Gateway address: 192.168.250.1
- 1. Establish communications with the DeviceMaster using the serial (Page 132) or telnet (Page 133) method.
- 2. At the RedBoot prompt, type ip.



The IP address, subnet mask, and IP gateway values will display.

Note: Optionally, you can install PortVision DX on a Windows system on the network and see the IP information in the Device List pane.

Configuring the Network Settings

Use the following procedure to program the IP address using RedBoot.

- 1. Establish communications with the DeviceMaster using the serial (Page 132) or telnet (Page 133) method.
- 2. Enter ip [addr mask gateway] and press the Enter key to configure the IP address. Where:

addr = IP address you want to use

mask = matches you network subnet mask

gateway = assigned by your network administrator

Make sure that each value is separated by a space.

```
RedBoot>dis
Loading disabled
RedBoot> ip 192.168.11.152 255.255.0.0 192.168.0.254
RedBoot>
IP: 192.168.11.152
Mask: 255.255.00
Gateway: 192.168.0.254
RedBoot> reset
.. Resetting
```

- 3. Verify that RedBoot responds with your configured network information or reissue the command.
- 4. Type reset to reset the DeviceMaster, if you do not have any other related RedBoot tasks.

Changing the Bootloader Timeout

Use the following procedure to change the Bootloader timeout value.

- 1. Establish communications with the DeviceMaster using the serial (Page 132) or telnet (Page 133) method.
- 2. At the **RedBoot** prompt, type **timeout**.

```
RedBoot> dis
Loading disabled
RedBoot> timeout
Timeout 15 seconds
RedBoot> timeout 45
timeout 45 seconds
RedBoot>_
```

RedBoot responds with the current Bootloader timeout value.

3. Type **timeout** and a value to change the timeout value. For example, **timeout 45** to change the Bootloader timeout to 45 seconds.

Determining the Bootloader Version

Use the following procedure to determine what Bootloader version is loaded in the DeviceMaster.

- 1. Establish communications with the DeviceMaster using the serial (Page 132) or telnet (Page 133) method.
- 2. At the **RedBoot** prompt, type version.

🛃 10.0.40 - PuTTY	- • • •
RedBoot> ver	
**	
** Comtrol DeviceMaster Bootloader 4.25	
** Platform: Comtrol DeviceMaster (ARM 7TDMI)	
** RedBoot(tm) environment - built 17:03:01, Oct 25 2016	
** Portions Copyright (C) 2000, Red Hat, Inc.	
** Portions Copyright (C) Comtrol Corp.	

RAM: 0x10000000-0x10018000 [0x1000168c-0x1000bb46 available]	
0x10080000-0x1008a000 [0x10080000-0x1008a000 available]	
0x20000000-0x20010000 [0x20000000-0x20010000 available]	
0x28000000-0x29000000 [0x28000000-0x29000000 available]	
FLASH: 0x14000000-0x147fffff, 2048 x 0x1000 blocks	
RedBoot>	

The Bootloader information displays.

- 3. Type reset to reset the DeviceMaster, if you do not have any other related RedBoot tasks.
- **Note:** Optionally, you can install PortVision DX on a Windows system on the network and see the Bootloader version in the Device List pane. Reboot the DeviceMaster, right-click the DeviceMaster and click Refresh Device until the Bootloader version displays. The Bootloader version is only displayed for a few moments.

Resetting the DeviceMaster

When you have completed your tasks in RedBoot, you must enter a **reset** command at the **RedBoot**> prompt for the DeviceMaster to begin operation.

Note: The <u>LEDs</u> on the DeviceMaster will go through the power up sequence. The DeviceMaster has completed its reset cycle when the **PWR** or **Status** LED is lit and it stops flashing.



Configuring Passwords

This section discusses how to configure a password for the web and telnet server.

Note: See the PortVision DX or SocketServer Help system for information about email notification.

Use the following procedure to establish the DeviceMaster password for the Web and telnet server. Establishing a password prevents unauthorized changes to the DeviceMaster configuration.

- 1. Establish communications with the DeviceMaster using the serial (Page 132) or telnet method (Page 133).
- 2. Type password [your_password] and press Enter.

Note: If you forget your password, you can reprogram the password using the serial method which bypasses the password.

📴 10.0.0.40 - PuTTY
ver

**
** Comtrol DeviceMaster Bootloader 4.25
** Platform: Comtrol DeviceMaster (ARM 7TDMI)
** RedBoot(tm) environment - built 17:03:01, Oct 25 2016
** Portions Copyright (C) 2000, Red Hat, Inc.
** Portions Copyright (C) Comtrol Corp.

RAM: 0x1000000-0x10018000 [0x1000168c-0x1000bb46 available]
0x10080000-0x1008a000 [0x10080000-0x1008a000 available]
0x20000000-0x20010000 [0x2000000-0x20010000 available]
0x28000000-0x29000000 [0x28000000-0x29000000 available]
FLASH: 0x14000000-0x147fffff, 2048 x 0x1000 blocks
RedBoot> dis
Loading disabled
RedBoot> password dev1313
Password 'dev1313'
RedBoot>

Note: The Bootloader version on your DeviceMaster may be different than the version displayed in this graphic.

See the **auth** command in the <u>*RedBoot Command Overview*</u> on Page 137, if you want to set up Web browser authentication.

RedBoot Command Overview

The following table is an overview of RedBoot commands available. After accessing RedBoot, you can review the list of commands online by entering **help** and pressing the **Enter** key.

For more detailed information, see the *eCos Reference Manual* that you can download from: <u>http://downloads.comtrol.com/dev_mstr/rts/software/redboot/user_guide</u>.

RedBoot Commands		
	Sets or displays web authentication. The default is set to none , which means that there is no authentication required to access the web server.	
autii	To deny access to the web server, click noaccess or invalid . If access is attempted, a message appears to notify the user that access is denied.	
{noaccess, none, basic, md5, invalid}	To configure the web server to request an un-encrypted password, click basic . To configure the web server to request an encrypted password, click md5 . (Some browsers do not support the md5 command.)	
boardrev†	Displays the board revision.	
cache [ON OFF]	Manages machine caches.	
channel [-1 <channel number="">]</channel>	Displays or switches the console channel.	
chassis	Displays chassis information.	
cksum -b <location> -l <length></length></location>	Computes a 32-bit checksum [POSIX algorithm] for a range of memory.	
clearconfig	Clears the application configuration.	
disable	Disables automatic load of the default application.	
fis {cmds}	Manages flash images. See Chapter 2 of the <u>eCos Reference Manual</u> for { cmds } information.	
flash	Shows flash information.	
go [-w <timeout>] [-c] [-n] [entry]</timeout>	Executes code at a location.	
help <topic></topic>	Displays available RedBoot commands.	
history	Displays command history.	
ip [addr mask gateway]	Displays or sets the IP address configuration.	
load [-r] [-v] [-h <host>] [-p <tcp port="">] [-m <varies>] [-c <channel_number>] [-b <base_address>] <file_name></file_name></base_address></channel_number></varies></tcp></host>	Loads a file from TFTP server or XModem.	
loop 232 422 int port-number	Runs loopback test on port. The DeviceMaster Serial Hub does not support this command.	
mac†	Displays Ethernet MAC address.	
model†	Shows model number.	
password {password}	Sets or deletes the password.	
ping [-v] [-n <count>] [-l <length>] [-t <timeout>] [-r <rate>] [-i <ip_addr>] -h <ip_addr></ip_addr></ip_addr></rate></timeout></length></count>	Network connectivity test.	
reset	Resets the DeviceMaster.	
secureconf [disable enable]	Sets or displays secure config enable.	
securedata [disable enable]	Sets or displays secure data enable.	

RedBoot Commands (Continued)	
sernum [prefix] [serial_number] sernum [serial_number]†	Displays device serial number (if available).
?	Displays short help.
snmp [disable enable]	Sets or displays SNMP enable.
summary	Displays a summary that includes the bootloader version, network address information, MAC address, and security settings.
telnet [disable enable}	Sets or displays telnet server enable. Disables telnet.
teltimeout [seconds]	Shows or sets telnet time-out.
terse	Terse command response mode.
t485 port #1 port #2	Runs port-to-port RS-485 test. This is not available on the DeviceMaster Serial Hub. Port numbering is Port 0 through 15 and you must connect a straight-through cable such as Ethernet patch cord.
timeout {seconds}	Displays or sets Bootloader time-out value.
version	Displays RedBoot version information.
† Read-only items that you cannot change in Redboot.	

External Power Supply Specifications

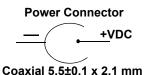
This section discusses information that you may need if you wish to use your own external power supplies.

- <u>1-Port 5VDC Panel Mount Power Supply</u> (below)
- <u>1-Port Panel Mount 5-30VDC Power Supply</u> on Page 140
- <u>DM-2101 and DM-2201: 1-Port DIN Rail Power Supply</u> on Page 140
- DM-2202 and DM-2402: 2-Port (Serial Terminals) Power Supply on Page 141
- <u>DM-2102 and DM-2302: 2-Port DB9 Power Supply (Bottom)</u> on Page 142
- DM-2102 and DM-2302: 2-Port DB9 Power Supply (Top) on Page 143
- <u>DM-2304: 4-Port DIN Rail Models Power Supply</u> on Page 144
- <u>4-Port Panel Mount Power Supply</u> on Page 144
- <u>8-Port Power Supply</u> on Page 145
- <u>16-Port Power Supplies</u> on Page 145

1-Port 5VDC Panel Mount Power Supply

This subsection only provides information for the DeviceMaster 1-port 5VDC panel mount model.

Comtrol Power Supply: 1-Port 5VDC	
Input line voltage Output voltage	47 - 63 Hz 90 - 260VAC 5VDC 2.0A @ 5VDC



The following table provides the DeviceMaster power specifications, if you intend on purchasing your own external power supply.

1-Port 5VDC External Power Supply	
Output voltage† Current† Power	5VDC 420 mA (Min) @ 5VDC 2.1 W
<i>†</i> Any power supply that meets current consumption, voltage, power, and connector pin outs requirements can be used.	

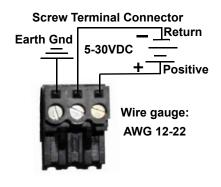
1-Port Panel Mount 5-30VDC Power Supply

This table provides specifications for the optional power supply from Comtrol.

Comtrol Power Supply: 1-Port 5-30VDC	
Input line voltage Output voltage	43-63 Hz 90-260 VAC 24VDC 500 mA @ 24VDC

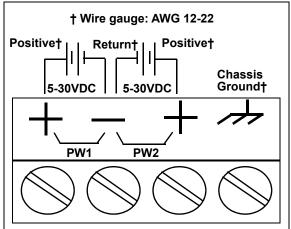
This table provides the specifications, if you intend on using your own power supply.

Comtrol device 1-Port 5-30VDC External Power Supply	
Output voltage†	5-30VDC
Current†	100 mA (Min) @ 24VDC
Power	2.5 W
<i>†</i> Any power supply that meets curr	ent consumption, voltage, power, and
connector pin outs requirements c	an be used.



DM-2101 and DM-2201: 1-Port DIN Rail Power Supply

This table provides the specifications to purchase a power supply for a DeviceMaster DM-2101 and DM-2201 1-port DIN rail.

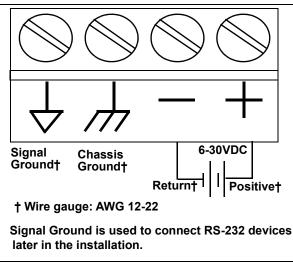


This table provides the specifications, if you intend on using your own power supply.

DeviceMaster DM-2101 and DM-2201 1-Port DIN Rail External Power Supply	
Output voltage† Current† Power	5-30VDC 100 mA (Min) @ 24VDC 2.5 W
<i>†</i> Any power supply that meets current consumption, voltage, power, and connector pin outs requirements can be used.	

DM-2202 and DM-2402: 2-Port (Serial Terminals) Power Supply

This table provides the specifications to purchase a power supply for a DeviceMaster 2-port (DM-2202 and DM-2402) with serial terminals DIN rail.

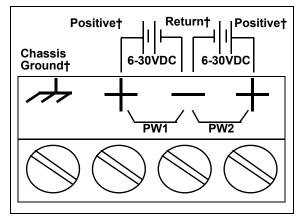


This table provides specifications if you intend on using your own power supply.

Comtrol device 2-Port DIN Rail (Serial Terminals) (DM-2202 and DM-2402) External Power Supply	
Output voltage† Current† Power	6-30VDC 100 mA (Min) @ 24VDC 2.5 W
<i>†</i> Any power supply that meets current consumption, voltage, power, and connector pin outs requirements can be used.	

DM-2102 and DM-2302: 2-Port DB9 Power Supply (Bottom)

This table provides the specifications to purchase a power supply for a DeviceMaster 2-port 1E/2E models (DM-2102 and DM-2302) with DB9 connectors.



† Wire gauge: AWG 12-22

Note: The power supply for these model is on the bottom of the unit. The product serial numbers are before xxxx-030000, where xxxx is the first four digits of the serial number.

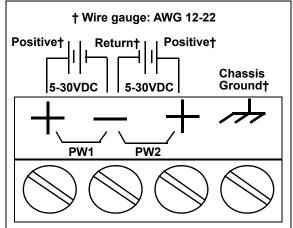
This table provides specifications if you intend on using your own power supply.

2-Port DB9 Models (Power Terminal - Bottom) External Power Supply	
Output voltage† Current† Power	6-30VDC 100 mA (Min) @ 24VDC 2.5 W
<i>†</i> Any power supply that meets current consumption, voltage, power, and connector pin outs requirements can be used.	

DM-2102 and DM-2302: 2-Port DB9 Power Supply (Top)

This table provides the specifications to purchase a power supply for a DeviceMaster DM-2102 and DM-2302 2-port DB9 DIN rail.

Note: The power supply for this model is on the top of the unit. The product serial numbers are above xxxx-030000, where xxxx is the first four digits of the serial number.

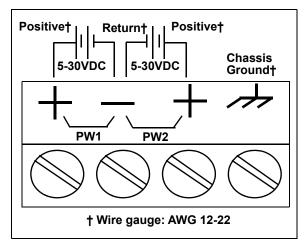


This table provides specifications if you intend on using your own power supply.

DM-2102 and DM-2302: 2-Port DIN Rail External Power Supply		
Output voltage† Current† Power	5-30VDC 100 mA (Min) @ 24VDC 2.5 W	
<i>†</i> Any power supply that meets current consumption, voltage, power, and connector pin outs requirements can be used.		

DM-2304: 4-Port DIN Rail Models Power Supply

This table provides the specifications to purchase a power supply for a DeviceMaster DM-2304 4-port (DIN rail).



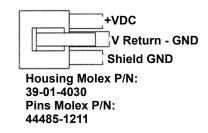
This table provides specifications if you intend on using your own power supply.

DM-2304: 4-Port DIN Rail External Power Supply		
Output voltage† Current† Power	5-30VDC 100 mA (Min) @ 24VDC 2.5 W	
<i>†</i> Any power supply that meets current consumption, voltage, power, and connector pin outs requirements can be used.		

4-Port Panel Mount Power Supply

This table provides the specifications for the power supply shipped with the DeviceMaster 4-port.

Comtrol Power Supply: 4-Port		
Output voltage	47 - 63 Hz 90 - 260 VAC 24VDC 500 mA @ 24VDC	



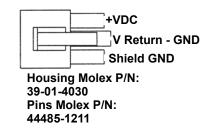
This table provides the specifications, if you intend on using your own power supply.

External Power Supply: 4-Port	
Output voltage† Current† Power	9-30VDC 200 mA (Min) @ 24VDC 4.8 W
<i>†</i> Any power supply that meets current consumption, voltage, power, and connector pin outs requirements can be used.	

8-Port Power Supply

The following table provides the specifications for the Comtrol-supplied power supply for the DeviceMaster 8-port.

Comtrol Power S	Supply: 8-Port
Output voltage	47 - 63 Hz 90 - 260 VAC 24VDC 500 mA @ 24VDC



+VDC

The following table provides the specifications, if you intend on purchasing your own power supply.

External Power Supply: 8-Port					
Output voltage† Current† Power	9-30VDC 290 mA (Min) @ 24VDC 6.96 W				
† Any power supply that meets power, and connector pin out.	current consumption, voltage, s requirements can be used.				

16-Port Power Supplies

The following table provides the specifications for the Comtrol-supplied power supply for the DeviceMaster 16-port models.

Comtrol Pov	ver Supply: 16-Port Models	V Return - GND
Input line frequency Input line voltage Output voltage Output current	47 - 63 Hz 90 - 260 VAC 24VDC 500 mA @ 24VDC	Housing Molex P/N: 39-01-4030 Pins Molex P/N: 44485-1211
Note: The DeviceMaste a single Etherner	r RTS 16-port and 32-port models with t port have internal power supplies.	44403-1211

Note: The DeviceMaster Serial Hub and DeviceMaster PRO, and DeviceMaster RTS (16-port and 32-port models with a single Ethernet port) have an internal power supplies.

The following tables provide the specifications, if you intend on purchasing your own power supply for your DeviceMaster RTS.

External Power Supply: 16-Port DeviceMaster RTS						
Input line frequency	N/A					
Input line voltage	N/A					
Output voltage†	9-30VDC					
Output current†	490 mA (Min) @ 24VDC					
Power	11.76W					
† Any power supply that connector pin outs requ	meets current consumption, voltage, power, and urements can be used.					

Troubleshooting and Technical Support

This section contains troubleshooting information for your DeviceMaster. You may want to review the following subsections before calling Technical Support because they will request that you perform many of the procedures or verifications before they will be able to help you diagnose a problem.

- <u>Troubleshooting Checklist</u> on Page 147
- <u>General Troubleshooting</u> on Page 149
- <u>Testing Ports Using Port Monitor (PMon2)</u> on Page 151
- <u>Testing Ports Using Test Terminal</u> on Page 154
- <u>Socket Mode Serial Port Testing</u> on Page 160
- Daisy-Chaining DeviceMaster 4/8/16-Port Units on Page 166
- <u>DeviceMaster LEDs</u> on Page 167
- <u>Removing DeviceMaster Security Features</u> on Page 169
- <u>Returning the DeviceMaster to Factory Defaults</u> on Page 171

If you cannot diagnose the problem, you can contact <u>*Technical Support*</u> on Page 174.

Troubleshooting Checklist

The following checklist may help you diagnose your problem:

- Verify that you are using the correct types of cables on the correct connectors and that all cables are connected securely.
 - *Note:* Most customer problems reported to Comtrol Technical Support are eventually traced to cabling or network problems.

Model	Connected to	Ethernet Cable	Connector Name
1-Port (Panel Mount)	Ethernet hub or NIC	Standard	10/100 ETHERNET
1-Port (DIN Rail)	Ethernet hub or NIC	Standard	10/100
2-Port - 1E (Single Ethernet Port)	Ethernet hub or NIC	Standard	10/100
2-Port - 2E (Dual Ethernet Ports)	Ethernet hub or NIC	Standard	10/100 - E1/E2
4-Port (DIN Rail)	Ethernet hub or NIC	Standard	10/100 - E1/E2
4/8-Port	NIC	Standard	DOWN
4/0-1 010	Ethernet hub	Standard	UP
16-Port (external power supply)	NIC	Standard	DOWN
10-1 of t (external power supply)	Ethernet hub	Standard	UP
16/32-Port (internal power supply)	Ethernet hub or NIC	Standard	10/100 NETWORK

- Verify that the network IP address, subnet mask, and gateway is correct and appropriate for the network. Make sure that the IP address programmed into the DeviceMaster matches the unique reserved IP configured address assigned by the system administrator.
 - If IP addressing is being used, the system should be able to ping the DeviceMaster.
 - If using DHCP, the host system needs to provide the subnet mask and gateway.
- Verify that the Ethernet hub and any other network devices between the system and the DeviceMaster are powered up and operating.
- Verify that the hardware MAC address in the NS-Link device driver matches the address on the DeviceMaster.
- If using a driver for Windows, verify that you are addressing the port correctly. In many applications, device names above COM9 require the prefix \\.\ in order to be recognized. For example, to reference COM20, use \\.\COM20 as the file or port name.
- If using a driver for Windows, you can use one of the Comtrol tools.
 - Advanced tab in the DeviceMaster Drivers Management Console which helps identify problems.
 - PortVision DX contains two applications that can be used to test or monitor the DeviceMaster:
 - *Test Terminal* program, which can be used to troubleshoot communications on a port-by-port basis. See <u>*Testing Ports Using Test Terminal*</u> on Page 154 for testing procedures.
 - *Port Monitor* program, which checks for errors, modem control, and status signals. In addition, it provides you with raw byte input and output counts. See <u>*Testing Ports Using Port Monitor (PMon2)*</u> on Page 151 for procedures.
 - Enable the Verbose Event Log feature on the Device General tab and then reboot the system.
- Reboot the system, then reset the power on the DeviceMaster and watch the **PWR** or **Status** (Page 167) light activity.

PWR or Status LED	Description
5 sec. off, 3 flashes, 5 sec. off, 3 flashes	RedBoot [™] checksum failure.
5 sec. off, 4 flashes, 5 sec. off, 4 flashes	SREC load failure.

Note: If the device has a power switch, turn the device's power switch off and on, while watching the LED diagnostics. If the DeviceMaster does not have a power switch, disconnect and reconnect the power cord.

- Remove and reinstall the DeviceMaster NS-Link device driver.
- If you have a spare DeviceMaster, try replacing the device.

General Troubleshooting

This table illustrates some general troubleshooting tips.

Note: Make sure that you have reviewed the <u>Troubleshooting Checklist</u> on Page 147.

General Condition	Explanation/Action					
	Indicates that the bootloader has not downloaded to the DeviceMaster.					
	1. If applicable, remove the NS-Link driver.					
PWR or Status LED	2. Make sure that you have downloaded the most current driver: <u>http://</u> <u>downloads.comtrol.com/dev_mstr/rts/drivers/</u> .					
flashing	3. Install the latest driver and configure the DeviceMaster using the MAC address. Make sure that you reboot the system. See <u>Device Driver (NS-Link) Installation</u> on Page 47 for procedures.					
	Note: If the PWR or Status LED is still flashing, contact Technical Support.					
PWR or Status LED not lit	Indicates that power has not been applied or there is a hardware failure. Contact Technical Support.					
Can ping the Comtrol	The NS-Link driver uses Port 4606 (11FE h) to communicate with the DeviceMaster.					
device, but cannot open the ports from a remote location. (You must have previously programmed the IP address, subnet mask, and IP gateway.)	When using a <i>sniffer</i> to track NS-Link packets, filtering for Port 4606 will easily track the packet. The packet should also contain the MAC address of the device and the originating PC so that it can be determined if the packet is able to travel the full distance one way or not.					
	If the 4606 packet is found on one side of a firewall or router, using sniffer, a not on the other side, then that port needs to be opened up to allow the 4606 pass.					
	This will most often be seen with firewalls, but is also seen in some routers.					
Cannot ping the device through Ethernet hub	Isolate the DeviceMaster from the network. Connect the device directly to the NIC in the host system.					
	The default DeviceMaster IP address is often not accessible due to the subnet masking from another network unless 192.168 is used in the network.					
Cannot ping or connect to	In most cases, it will be necessary to program in an address that conforms your network. See <u>Configuring the Network Settings</u> on Page 38 to use PortVision DX to program the IP address.					
the DeviceMaster	If you do not use PortVision DX (or the NS-Link driver for Windows) to program the IP address, you can use RedBoot.					
	If you use RedBoot, you only have 15 seconds to disable the Bootloader with RedBoot to get into the setup utility. See <u><i>RedBoot Procedures</i></u> on Page 131 for the RedBoot method of programming an IP address.					

General Condition	Explanation/Action
	The problem is caused by a L2 bridging feature called Spanning Tree Algorithm (STA) in the switch. This feature is enabled by default in some switches. This features causes time-out problems on certain L2 protocols, such as our MAC mode.
	<i>Resolution</i> : There will be no firmware fix for this problem. Only one of the following fixes is required for resolution.
	1. Disable STA in the switch.
	2. Enable STA fast forwarding on the port.
	3. Change the STA Forward Delay and Message Age to minimum time values.
	4. On the device, set the time-out value to 0 (to disable loading of SocketServer) or 120. The command from the redboot prompt is "Timeout 120" without the quotes.
DeviceMaster continuously	<i>Problem Details</i> : STA by default blocks packets for 30 seconds after an ethernet port auto negotiates. Blocking of these packets causes the NS-Link driver load process to fail.
reboots when connected to	The normal NS-Link driver load process is:
some Ethernet switches with the NS-Link driver	1. If NS-Link determines that it needs to load a device, it resets the device. It does this to get the device into RedBoot mode. Only RedBoot accepts load binary commands, which are needed to load the NS-Link binary into the DeviceMaster.
	2. After a 6 second delay, NS-Link sends an ID query to the device. This query is to verify that the device is in RedBoot and can accept load binary commands.
	3. The device sends an ID query response.
	4. NS-Link loads the device.
	If the device is not loaded after timeout seconds (default 15), it loads SocketServer.
	The above process fails when STA is running because the switch blocks packets for 30 seconds after the DeviceMaster reboots. Therefore, the ID query is not received by the DeviceMaster and after 15 seconds the device loads SocketServer. After 30 seconds, NS-Link finally can do an ID query, which reveals that the device is not in RedBoot. NS-Link therefore reboots the device, and the process repeats.
DeviceMaster continuously reboots when connected to some Ethernet switches or routers	Invalid IP information may also cause the switch or router to check for a gateway address. Lack of a gateway address is a common cause.

Testing Ports Using Port Monitor (PMon2)

You can use this subsection to test the DeviceMaster driver installation. If you need to install the device driver, locate the <u>latest</u> driver and driver installation documentation.

Overview

This procedure will check whether the DeviceMaster can:

- Communicate through the Comtrol device driver
- Determine if a port is open with an application

Testing Comtrol COM Ports

If necessary, *Installing PortVision DX* on Page 35 to install PortVision DX, which contains Port Monitor.

- 1. Start PortVision DX from the Start menu, select Comtrol > PortVision DX or click the desktop shortcut.
- 2. Select Tools > Applications > Port Monitor (PMon2).

Scan Refresh	Refresh All Scan Network	Ipload Reboot Webpage Notes	telp Abo	ut Exit
Scan Refresh Scan Network Check for Updates IP O R T VI Options Scan Network Check for Updates Pload Reboot Webpage Notes Help St Floor [8 / 8] Customize Test Terminal (WCom2) Port Monitor (PMon2)				
	Applications +	Customize		
	Options	Test Terminal (WCom2)		
lame : First Floor		Port Monitor (PMon2) HyperTerminal Drivers		

3. Click Add Ports using the icon or Tools > Add Ports,

🗅 🖨 🖬	a	%		1 8									
Port Name	Status	CTS	DSR	CD	RTS	DTR	Actual Throughput	TxTotal	RxTotal	Total Errors	OverrunErrors	FramingErrors	ParityErro

4. Click Driver, click RPSHSI/NSLINK.

Add Ports	X
C Ports	ОК
COM1 COM2 COM3 COM4 COM5 COM6 COM7 COM8 COM9 COM10	Cancel
C Range For example: 3-15,21,45,5	1-56,74
 Driver 	
ROCKETPORT INFIN	ITY / EXPRESS
DEVICEMASTER / N	SLINK
ROCKETPORT / ROC	KETMODEM

5. If the DeviceMaster is communicating with the device driver for Windows, Port Monitor should display CLOSED status. If a port is open for an application, it displays as OPEN, and displays Actual Throughput, TxTotal and RxTotal statistics.

File Tools	View	Help												
D 🚅 🔒				(?										
Port Name	Status	CTS	DSR	CD	RTS	DTR	Actual Throughput	TxTotal	RxTotal	Total Errors	FramingErrors	ParityErrors	OverrunErrorsRaw	
COM4	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	T
COM5	OPEN	ON	ON	ON	ON	ON	115800	9105348	9101707	0	0	0	0	
COM6	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	
COM9	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	
COM10	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	
COM11	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	
COM12	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	
COM18	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	
COM25	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	
COM26	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	
COM100	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	
COM101	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	

Normally, there should be no data errors recorded or they should be very small. To find out what the actual errors are, scroll to the right. You will see three columns: **Overrun Errors**, **Framing Errors**, and **Parity Errors**.

If the errors are:

- **Overrun Errors** represent receive buffer overflow errors. If this is the case, you will have to configure either software or hardware handshaking to control the flow of data. The most common errors are **Overrun** errors.
- Framing Errors indicate that there is an synchronization error between the beginning of a data frame and the end of the data frame. A frame usually consists of a start bit, 8 data bits, and a stop bit or two. The framing error occurs if the stop bit is not detected or it occurs in the wrong time frame. Most causes for framing errors are electrical noise on the data lines, or differences in the data clocks of the DeviceMaster and the connected device.
- **Parity Errors** occur when parity is used and the parity bit is not what is expected. This can also be caused by noise on the data lines.

6. You can view additional statistics to Port Monitor by adding columns. Click Tools and Add Columns.

File Too	ols View Help												
D	Add Ports		?	-									
Port	Remove Ports		5	RTS	DTR	Actual Throughput	TxTotal	RxTotal	Total Errors	FramingErrors	ParityErrors	OverrunErrorsRaw	Г
СОМ			F	OFF	OFF	0	10	0	0	0	0	0	
СОМ	Add Columns	4		ON	ON	116397	10564800	10561149	0	0	0	0	
COM	Remove Columns	i hi	5	OFF	OFF	0	0	0	0	0	0	0	
COM			-	OFF	OFF	0	10	0	0	0	0	0	
сом	Reset Values		-	OFF	OFF	0	10	0	0	0	0	0	
сом	Default Columns		-	OFF	OFF	0	0	0	0	0	0	0	
СОМ	berdan conditions		-	OFF	OFF	0	0	0	0	0	0	0	
сом	Settings		F	OFF	OFF	0	0	0	0	0	0	0	
COMZ	CLUSED OFF	VIT	- Urf	OFF	OFF	0	0	0	0	0	0	0	
COM26	CLOSED OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	
COM100	CLOSED OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	
COM101	CLOSED OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	

7. Highlight or shift-click to add multiple statistics and click Ok.

DTR	*
Actual Throughput ExTotal	
RxTotal Total Errors	-
) verrunErrors	
FramingErrors	
ParityErrors	
itatus Flags TxPackets	_
BxPackets	
rxTotalRaw	
3xTotalRaw	*

Note: See the Port Monitor help system if you need an explanation of a column.

8. Scroll to the right to view the new columns.

		iew H	· ·											_
🗅 🗃 I	84	S COM	*		(💡									
Status	CTS	DSR	CD	RTS	DTR	Actual Throughput	TxTotal	RxTotal	Total Errors	FramingErrors	ParityErrors	OverrunErrorsRaw	TxPackets	
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0	
OPEN	ON	ON	ON	ON	ON				0	0	0	0		
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0	
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0	
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0	
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0	
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0	
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0	
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0	
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0	
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0	
4							-							b.

- 9. If you want to capture this session, you can save a current session as a report. To do this, select one of the following save options:
 - File > Save As
 - File > Save if the report already exists in an older format
 - Save Active Session 📕 button

Reports can be opened, viewed and re-used when needed. To open and view a report:

- a. Select File > Open or the Open Existing Session 🖻 button. The Open Session dialog appears.
- b. Locate the session (table), you want to open and click the **Open** button.

Optionally, if you want to continue monitoring for an existing session, you need to activate the *Polling Interval*.

- Select Tools > Settings to access the PMon2 Settings dialog
- Change the **Polling Interval** field to a value other than zero (0)

10. Leave Port Monitor open so that you can review events when using *Test Terminal* to test a port or ports.

Testing Ports Using Test Terminal

You can use the following procedure to test COM ports. If you need to install the DeviceMaster device driver, locate the <u>latest</u> driver and driver installation documentation.

The following procedures require a loopback plug to be placed on the port or ports that you want to test. A loopback plug was shipped with your product. If you need to build a replacement or additional loopback plugs, refer to <u>*Connecting Serial Devices*</u> on Page 87.

Overview

Test Terminal (WCom2) allows you to open a port, send characters and commands to the port, and toggle the control signals. This application can be used to troubleshoot communications on a port-by-port basis.

- Send and Receive Test Data: This sends data out the transmit line to the loopback plug, which has the transmit and receive pins connected thus sending the data back through the Rx line to Test Terminal, which then displays the received data in the terminal window for that port. This test is only testing the Tx and Rx signal lines and nothing else. This test works in either RS-232 or RS-422 modes as both modes have transmit and receive capability. A failure in this test will essentially prevent the port from working in any manner.
- Loopback Test: This tests all of the modem control signals such as RTS, DTR, CTS, DSR, CD, and RI along with the Tx and Rx signals. When a signal is made HI in one line the corresponding signal line indicates this. The Loopback Test changes the state of the lines and looks for the corresponding state change. If it successfully recognizes all of these changes, the port passes.

A failure on this test is not necessarily critical as it will depend on what is connected and how many signal lines are in use. For example, if you are using RS-232 in 3-wire mode (Transmit, Receive and Ground) a failure will cause no discernible issue since the other signals are not being used. If the port is configured for use as either RS-422 or RS-485 this test will fail and is expected to fail since RS-422 and RS-485 do not have the modem control signals that are present in RS-232 for which this test is designed.

Opening Ports

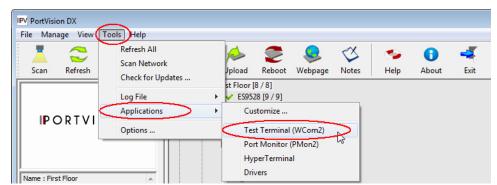
The following procedure shows how to use **Test Terminal** to send and receive test data to the serial ports. If necessary, use <u>Installing PortVision DX</u> on Page 35, which contains Test Terminal.

1. Stop all applications that may be accessing the ports such as RRAS or any faxing, or production software. See the appropriate help systems or manuals for instructions on stopping these services or applications.

If another application is controlling the port, then **Test Terminal** will be unable to open the port and an error message will be shown.

2. Start Test Terminal (WCom2). If necessary, start PortVision DX from the Start menu, select Comtrol > PortVision DX or click the desktop shortcut.

3. Select Tools > Applications > Test Terminal (WCom2).



4. Select **File > Open Port**, the appropriate port (or ports) from the *Open Ports* drop list and **Ok**.

Note: If you left Port Monitor open from the previous subsection, you should show that the port is open.

Go to the appropriate procedure to send and receive test data.

- <u>Sending and Receiving Test Data (RS-232/422/485: 4-Wire)</u> (below)
- <u>Sending and Receiving Data (RS-485: 2-Wire)</u> on Page 156

Sending and Receiving Test Data (RS-232/422/485: 4-Wire)

You can use this procedure to send and receive test data through the RS-232/422/485 (4-wire, full-duplex) port or ports that you want to test.

- 1. If you have not done so, perform <u>Steps 1</u> through <u>2</u> on Page 154.
- Install the loopback plug onto the port (or ports) that you want to test. See <u>Connecting Serial Devices</u> on Page 87, if you need to build loopback plugs.
- 3. Select Port > Send and Receive Test Data.

You should see the alphabet scrolling across the port. If so, then the port installed properly and is operational.

Note: If you left Port Monitor running, it should show data sent and received and show the average data throughput on the port.

- 4. Select **Port** > **Send and Receive Test Data** to stop the scrolling data.
- 5. You can go to the next procedure to run the *Loopback Test* on Page 156 if this is an RS-232 port.

If this test successfully completed, then the port is operational as expected.

Note: Do NOT forget to restart the communications application.

🖫 WCom2 - Test Terminal	
File Port Settings View Window Help	
🛛 🗗 🚟 🚟 😹 🖉 📖 🚥 💷 🛛 🦓	
COM5	
ABCDEFGHIJKLMNOPORSTU ABCDEFGHIJKLMNOPORSTUV ABCDEFGHIJKLMNOPORSTUVW ABCDEFGHIJKLMNOPORSTUVWX ABCDEFGHIJKLMNOPORSTUVWXY ABCDEFGHIJKLMNOPORSTUVWXYZ A ACDEFGHIJKLMNOPORSTUVWXYZ A BCDE ABC ABC ABC ABC	
Ready	NUM //

 Select Ports 	ОК
COM1 COM2 COM3	Cancel
COM4 COM5	Settings
COM6 COM7 COM8 COM9 COM10	-
C Select Range	

Loopback Test (RS-232)

The Loopback Test tests the modem control (hardware handshaking) signals. It only has meaning in RS-232 mode on serial connector interfaces with full RS-232 signals. If performed under the following conditions, the test will always fail because full modem control signals are not present:

- RS-422
- RS-485
- RJ11 connectors

Use the following steps to run the Loopback Test.

- 1. If necessary, start Test Terminal (Page 154, <u>Steps 1</u> through <u>2</u>).
- 2. Click **Port > Loopback Test**.

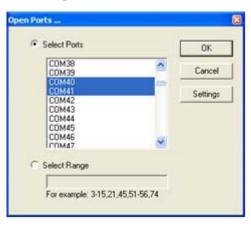
This is a pass fail test and will take a second or two to complete. Repeat for each port that needs testing.

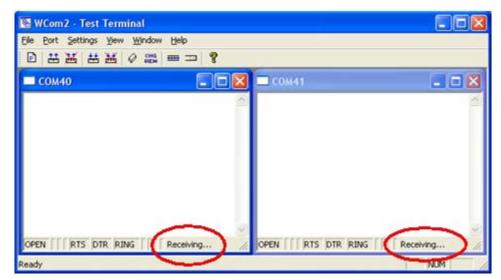
If the Loopback Test and the Send and Receive Test Data tests successfully complete, then the port is operational as expected.

Sending and Receiving Data (RS-485: 2-Wire)

This procedure shows how to use Test Terminal (WCom2) to test two RS-485 (2-Wire, Half-Duplex) ports.

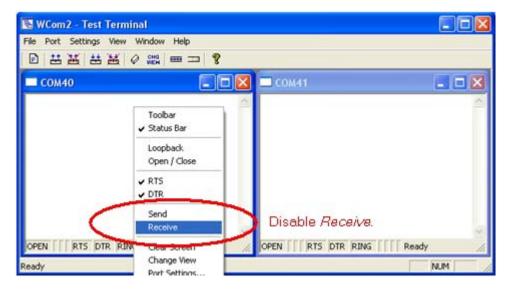
- 1. In PortVision DX, click Tools >Applications >Test Terminal (WCom2) to start Test Terminal.
- 2. Open two ports RS-485 ports. This example uses COM40 and COM41.





Test Terminal will open two windows, note that both ports show Receiving on the status bar.

3. Right-click in both COM windows and remove the check mark for Receive.



Both COM ports show *Ready* on the status bar.

📴 WCom2 - Test Terminal	
Eile Port Settings View Window Help	
□ # # # # Ø # = □ ?	
Сом40	🗆 COM41 📃 🗖 🔀
	A
OPEN TS DTR RING Ready	OPEN TTS DTR RING Ready
Ready	NUM

- 4. Right-click in ONE window and select the **Receive** option from the pop up.
- 5. Right-click the OPPOSITE window and click Send.

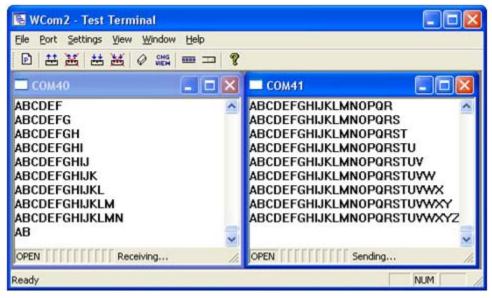
🗟 WCom2 - Test Terminal	
Eile Port Settings View Window Help	
◎ # # # # ⊘ \$\$ == ⊃ %	
🗖 СОМ40	🗖 COM41 📃 🗖 🗙
OPEN [[[[[[]]	ABCDEFGHIJKLM ABCDEFGHIJKLMN ABCDEFGHIJKLMNO ABCDEFGHIJKLMNOPQ ABCDEFGHIJKLMNOPQR ABCDEFGHIJKLMNOPQRS ABCDEFGHIJKLMNOPQRST ABCDEFGHIJKLMNOPQRSTU ABCDEFGHIJ COPEN Receiving
Ready	NUM

The *Status* line shows *Sending* or *Receiving*. In this case, COM40 is sending data and COM41 is receiving the data which is visually confirmed by the data scrolling across the COM41 window.

Note: If you do not see the data being received it MAY be necessary to also disable the RTS and DTR options from the right-click pop-up menu in each COM port.

6. Right-click and remove the check mark on the Sending COM port.

7. Right-click and remove the check mark on the *Receiving* COM port.



Neither COM port is sending or receiving data but shows *Ready* on the *Status* bar.

8. Reverse the sending/receiving windows one at a time. Set the **Receive** option first, then in the opposite window, select the **Send** option.

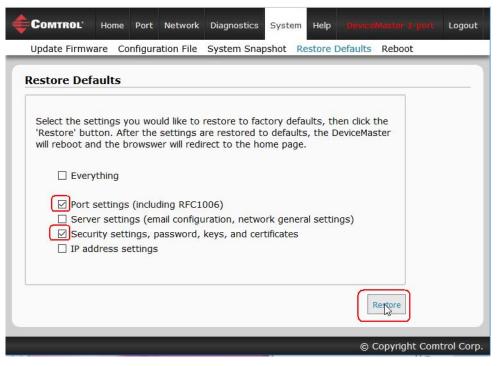
The Status line shows Sending or Receiving in the reverse windows.

Data is now scrolling in the COM40 window. COM41 is static as it is not receiving data but transmitting data.

Socket Mode Serial Port Testing

This procedure illustrates using Putty, which is available in PortVision DX. Optionally, you can use any other Winsock compatible application.

- **Note:** The following procedure starts with resetting DeviceMaster to factory default values. You may want to save the DeviceMaster socket configuration using <u>PortVision DX Saving a SocketServer Configuration</u> <u>File</u> on Page 107.
- 1. If necessary, install PortVision DX using *Installing PortVision DX* on Page 35 and scan the network to locate the DeviceMaster that you want to test.
- 2. Right-click the DeviceMaster and click Webpage.
- 3. Click System | Restore Defaults.
- 4. Click the **Port settings** and **Security settings**, **password**, **keys**, **and certificates** options, and then the **Restore** button.





5. If necessary, re-open the web pages and click the port that you want to test.

6. Under the *TCP Connection Configuration* section, click the **Enable** option, and leave all other settings on this page at their default values.

Serial	TCP Connection Enabled:	UDP Connection
Port Name: Port Mode: RS-232 V Baud Rate: 9600 V Parity: none V Data Bits: 8 V Stop Bits: 1 V Flow Control: none V Advanced DTR Mode: off V RTS Mode: off V RTS Mode: off V Pre/Post RTS Hold Time: 0/0 ms Detect End of Line: disabled V End of Line Characters: 0 0 (dec) Serial Rx Buffer Timeout: 0 ms Rx FIFO Disable: □ Send Buffered Data After Close: □	Listen: On Port: 8000 Connect to IP Address: Target Port: 0 Source Port: 0 Connect: Always Data DDSR CD Disconnect: Idle No DSR No CD Idle Timeout: 300 s Telnet Protocol Enable (RFC2217): □	Enable serial to Ethernet: Enable Ethernet to serial: Allow Ethernet data from any IP address: Serial data to last host that sent UDP data: Target IP Address 0 0

Note: The Port number as it is needed later in this procedure. In this example, the port number is 8000.

7. Click the Save button.

8. Verify that the port has been enabled.

t Overview			
	Port 1		
Port Name:			
NS-Link Connections			
00:40:f4:a8:c3:e7			
Socket Connections			
Local:	[]:0		
Remote:	[]:0		
Rx Count:	0		
Tx Count:	0		
Port Configuration (serial)			
Port Mode:	RS-232		
Baud Rate:	9600		
Parity:	none		
Data Bits:	8		
Stop Bits:	1		
Flow Control:	none		
DTR Mode:	off		
RTS Mode:	off		
Pre/Post RTS hold time:	0/0		
End of line character(s):	none		
Serial RX buffer timeout:	0		
Send buffered data after close:	no		
Rx FIFO Disable:	no		
Port Configuration (network)			
TCP Enabled:	yes		
Listen Enabled:	yes		
Listen on port:	8000		
Connect to IP Address:	[]:0		
From Source Port:	0		
Connect On:	never		
Disconnect When:	never		
Idle Timeout:	300		

- 9. Leave the web page open.
- 10. Attach the loopback plug that was shipped with the DeviceMaster to the serial port of the DeviceMaster. See <u>Connecting Serial Devices</u> on Page 87 if you need to build a loopback plug.

IPV PortVision DX							
File Manage View Tools Help							
1 2 🖉 🤞	s 👍 🎓	🥭 💄	\propto	- 5	0 🚽		
Scan Refresh All Properties Save	e Load Upload	Reboot Webpage	Notes	Help	About Exi	t	
IP ORTVISION		6 XT [9 / 10] S7506 [1 / 3] S7510 S7510-XT [1 / 1] # ✓ Axis P5534 Camera	1				
Name : First Floor	R P	S7528 S8508 S8508F-M S8509-XT roperties dit Notes					
Use menu or toolbar to add notes in A this area.		Vebpage					
	 Device Name 	Configuration	▶ 1	P Address	MAC Address	Software Version	Status
	DM UP16 T	racker	+ 1	92.168.11.60	00:C0:4E:40:00:5D	Modbus Router 6.05	ON-LINE
	ES9528-XT		1	92.168.11.105	00:C0:4E:36:00:02	v1.4a (b1.1.0.4)	ON-LINE
	IOLIMI-4-EI	ename		92.168.11.198		EtherNet/IP 1.2.0	ON-LINE
		love		92.168.11.55		Modbus Router 6.05	ON-LINE
0000 0000	Modbus S D	elete		92.168.11.54		Modbus Server 4.04	ON-LINE
20 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Modbus/T			92.168.11.53	00:C0:4E:15:04:7A		ON-LINE
· · · · · · · · · · · · · · · · · · ·		lelp		92.168.11.20	00:C0:4E:17:FF:FB	NS-Link 9.18 SocketServer 9.35	ON-LINE ON-LINE
Use menu or toolbar to add notes in 🔺 📗	RTS 2-Port RTS-1P Printer#10	RTS-1P (5-30V)		92.168.11.52		SocketServer 9.35	ON-LINE ON-LINE
	RTS4 Spare COM P			92.168.11.40		SocketServer 9.18	ON-LINE
		COM P SH-8P (DB9)		92.168.11.14	00:C0:4E:1C:FF:FD		ON-LINE
							on Line
<u>'</u>	•						•
Access the selected device(s) using Telnet ses	sion					Fi	rst Floor 11 1 Ready

11. Right-click the DeviceMaster in the Device List pane and click Telnet / SSH Session.

12. Enter the socket number of the port that you are testing $(\underline{\text{Step 6}})$ and click **Ok**.

Telnet / SSH Settings	—
☞ Telnet ○ SSH	Selected Port : 8000
Ok	Cancel

PuTTY loads.



13. Type 123.

🧬 192.168.11.23 - PuTTY	
112233	*
	· · · · · · · · · · · · · · · · · · ·

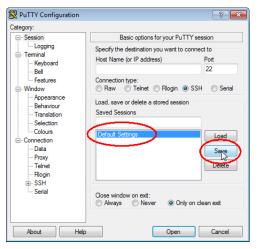
- If 112233 displays, you need to disable local echo. Use the following steps to disable local echo.
- a. Go to c: \Program Files (x86)\Comtrol\PortVision DX.
- b. Execute **PUTTY.EXE** to open the application.

Category:			
Session	Basic options for your PuTTY session		
Logging Terminal Keyboard Bell Features Window	Specify the destination you want to connect to Host Name (or IP address) Port I 22 Connection type: Riogin @ SSH Serial		
 — Appearance — Behaviour — Translation — Selection — Colours — Connection — Data — Proxy — Telnet — Riogin ⊕ SSH — Serial 	Load, save or delete a stored session Saved Sessions		
	Default Settings Load Save Delete		
	Close window on exit:		
About	elp Open Cancel		

c. Click **Terminal** and click **Force off** for the *Local echo* option.

🕵 PuTTY Configuration	? 💌
Category:	
Session	Options controlling the terminal emulation
Learing Terminal Koyboard - Bell - Features - Window - Appearance - Behavour - Translation - Selection - Colours	Set various terminal options Auto wrap mode initially on CC Origin Mode initially on Implicit CR in every LF Implicit LF in every CR Use background colour to erase screen Enable blinking text Answerback to ^E: PuTTY
□ - Connection □ - Data - Proxy - Teinet - Riogin ⊕ SSH	Line discipline options Local echo: Auto Force on Auto Force off Auto Force off Force off Force off
I Serial	Remote-controlled printing Printer to send ANSI printer output to: None (printing disabled)
About Help	Open Cancel

d. Return to the Session menu, highlight Default Settings and then click Save.



e. Click Cancel to close PuTTY.

- f. Close the telnet (PuTTY) session that you opened from PortVision DX.
- g. Re-open the telnet session by right-clicking the DeviceMaster, and select the Telnet / SSH Session option.
- h. Enter the Socket Port number and then click Ok.

Telnet / SSH Settings	X
	Selected Port : 8000
	OK Cancel

i. Enter 123, single digits should appear.

சூ 192.168.11.23 - PuTTY	
123	*
	~

- 14. Remove the loopback plug and type abc. No characters should display because the return path is open.
- 15. Re-attach the loopback plug, type **abc**, and the characters should appear.



- 16. If you want to test additional ports, simply repeat this procedure on that port or ports.
- 17. Remove the loopback plug from the serial port and attach your serial device.You may need to set the serial parameters as necessary to match your attached equipment.

Daisy-Chaining DeviceMaster 4/8/16-Port Units

The DeviceMaster 4/8/16-port (panel mount) models with external power supplies follow the IEEE specifications for standard Ethernet 10/100BASE-TX topologies.

Note: If the serial number of your product is above xxxx-030000, the **UP** and **DOWN** Ethernet ports are interchangeable.

When using the **UP** and **DOWN** ports, the DeviceMaster 4/8/16 is classified as a switch. When using the **UP** port only, it is a simple end node device.

The maximum number of daisy-chained DeviceMaster 4/8/16 units, and the maximum distance between units is based on the Ethernet standards and will be determined by your own environment and the conformity of your network to these standards.

Comtrol has tested with seven DeviceMaster 4/8/16 units daisy-chained together using 10 foot CAT5 cables, but this is not the theoretical limit. You may experience a performance hit on the devices at the end of the chain, so it is recommended that you overload and test for performance in your environment. The OS and the application may also limit the total number of ports that may be installed.

Following are some quick guidelines and URLs of additional information. Note that standards and URLs do occasionally change.

- Ethernet 10BASE-T Rules
 - The maximum number of repeater hops is four.
 - You can use Category 3 or 5 twisted-pair 10BASE-T cables.
 - The maximum length of each cable is 100m (328ft).

Note: Category 3 or 5 twisted pair cables look the same as telephone cables but they are not the same. The network will not work if telephone cables are used to connect the equipment.

- Fast Ethernet 100BASE-TX rules
 - The maximum number of repeater hops is two (for a Class II hub). A Class II hub can be connected directly to one other Class II Fast Ethernet hub. A Class I hub cannot be connected directly to another Fast Ethernet hub.
 - You must use Category 5 twisted-pair 100BASE-TX cables.
 - The maximum length of each twisted-pair cable is 100m (328ft).
 - The total length of twisted-pair cabling (across directly connected hubs) must not exceed 205m (672ft).

Note: Category 5 twisted pair cables look the same as telephone cables but they are not the same. The network will not work if telephone cables are used to connect the equipment.

- IEEE 802.3 specification: A network using repeaters between communicating stations (PCs) is subject to the 5-4-3 rule of repeater placement on the network:
 - Five segments connected on the network.
 - Four repeaters.
 - Three segments of the 5 segments can have stations connected. The other two segments must be interrepeater link segments with no stations connected.

Additional information may be found by searching the web.

DeviceMaster LEDs

The DeviceMaster has network and port LEDs to indicate status. This subsection discusses:

- <u>TX/RX LEDs</u>
- <u>Network and Device LEDs</u> on Page 167

TX/RX LEDs

This subsection discusses RX and TX LEDs on the following products:

- DB9: Comtrol device 4-port (panel mount) and 8-port models and the DeviceMaster Serial Hub 16-port.
- RJ45: DeviceMaster RTS 16-port and 32-port models and the DeviceMaster PRO 16-port.

Note: DeviceMaster DIN rail models do not have TX/RX LEDs.

The RX (yellow) and TX (green) LEDs function accordingly when the cable is attached properly to a serial device.

- After power cycling the DeviceMaster, the RX/TX LEDs are off.
- The LEDs do not function as described until the port has been opened by an application. You can use Test Terminal to open a port or ports if you want to test a port or ports (<u>Testing Ports Using Test Terminal</u> on Page 154).
 - If the port is configured for RS-232/422 mode:
 - RX LEDs (yellow) are lit
 - TX LEDs (green) are lit when as the data exits the port
 - If the port is configured for RS-485 mode:
 - RX LEDs (yellow) are lit while receiving
 - TX LEDs (green) are lit during active data transmission

Network and Device LEDs

The LEDs indicate that the default DeviceMaster application, SocketServer is running or after driver installation, that the NS-Link driver loads. If you have loaded PortVision DX, you can check the DeviceMaster status on-line.

Ports	Model	Network LEDs	
		• The Status LED on the front of the unit is lit, which indicates that it has power and has completed the boot cycle.	
1 Panel	DeviceMaster RTS	Note: The Status LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.	
Mount	1016	• The red Link Act LED is lit, which indicates a working Ethernet connection.	
		• If the red Duplex LED is lit, it indicates full-duplex activity.	
		• If the red 100 LED is lit, it indicates a working 100 MB Ethernet connection (100 MB network, only).	

Ports	Model	Network LEDs (Continued)
		• The Status LED on the front of the unit is lit, which indicates that it has power and has completed the boot cycle.
1 DIN Rail	DM-2101 DM-2201	Note: The Status LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.
		• If the LINK (green) LED is lit, it indicates a working Ethernet connection.
		• If the ACT (yellow) LED flashes, it indicates network activity.
		• The STATUS LED on the device is lit, indicating you have power and it has completed the boot cycle.
2 DIN Rail	DM-2102 DM-2202 DM-2302	Note: The STATUS <i>LED</i> flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.
	DM-2402	• If the LINK (green) LED is lit, it indicates a working Ethernet connection.
		• If the ACT (yellow) LED flashes, it indicates network activity.
	DM-2304	• The STATUS LED on the device is lit, indicating you have power and it has completed the boot cycle.
4 DIN Rail		Note: The STATUS LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.
		• If the LINK (green) LED is lit, it indicates a working Ethernet connection.
		• If the ACT (yellow) LED flashes, it indicates network activity.
4 Panel	DeviceMaster PRO (8)	• The PWR LED on the front of the unit is lit, which indicates it has power and has completed the boot cycle.
Mount 8	DeviceMaster RTS†	Note: The PWR LED flashes while booting and it takes approximately 15 seconds for the bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.
C		• The red LNK/ACT LED is lit, which indicates a working Ethernet connection.
16	DeviceMaster Serial Hub (8)	• If the red 100 LED is lit, it indicates a working 100 MB Ethernet connection (100 MB network, only).
	DeviceMaster PRO (16) DeviceMaster	• The Status LED on the front of the unit is lit, which indicates it has power and has completed the boot cycle.
16		Note: The Status LED flashes while booting and it takes approximately 15 seconds for the bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.
	RTS†† DeviceMaster Serial Hub (16)	• The red LNK/ACT LED is lit, which indicates a working Ethernet connection.
32		• If the red Duplex LED is lit, it indicates full-duplex activity.
		• If the red 100 LED is lit, it indicates a working 100 MB Ethernet connection (100 MB network, only).
† Exteri	nal power supply.	
†† Intern	al power supply.	

Removing DeviceMaster Security Features

When presented with a DeviceMaster that has had all security options set and the user is unaware of what the settings are, the restoring of a DeviceMaster can be very difficult.

It may be necessary to use the DeviceMaster debug dongle provided with the *Software Developers Kit* (SDK) or return the DeviceMaster to Comtrol after obtaining an return material authorization (RMA) so that Comtrol can re-flash the DeviceMaster with default values.

One of the following two conditions must be true, so that you can remove the security settings from the DeviceMaster.

- Serial connection using Port 1 to access RedBoot:
 - Bootloader timeout set to value greater than 10 seconds (default is 15 seconds).
 - A known good null modem cable.
 - A COM port on PC/Laptop.
- Bootloader Command Console using an Ethernet connection
 - No password or a known password.
 - A known or discoverable IP address.
 - A utility such as *Angry IP Scanner* from <u>www.angryip.org</u> may be used to discover IP addresses. If the IP range is unknown, a full scan from 0.0.0.1 to 255.255.255.255 may take a long time.
 - An Ethernet cable.
 - A PC/Laptop with a telnet application installed such as PuTTY included in PortVision DX.

Serial Connection Method

Use the following procedure to set up serial connection with a terminal server program (for example, Test Terminal (WCom2), HyperTerminal or Minicom) and the DeviceMaster.

Note: Optionally, you can use Test Terminal, which is included in PortVision DX under the Tools >Applications > Test Terminal menu.

1. Connect a null-modem cable from an available COM port on your PC to Port 1 on the DeviceMaster.

Note: See <u>Connecting Serial Devices</u> on Page 73 to build a null-modem cable.

2. Configure the terminal server program to the following values:

- Bits per second = 57600
- Data bits = 8
- Parity = None
- Stop bits = 1
- Flow control = None
- 3. Reset the DeviceMaster.

Note: Depending on the model, disconnect and reconnect the power cable (external power supply and no power switch) or turn the power switch on and then off (internal power supply).

4. Immediately type #!DM and press Enter in the terminal program.

#!DM RedBoot>dis Loading disabled 5. At the **RedBoot>** prompt, type **dis**, and press **Enter**.

Note: If you do not disable the loading feature of the Bootloader within the time-out period (default is fifteen seconds), an application will be loaded from flash and started. If this happens, repeat Steps 3 through 5. The **#!DM** command is the only case-sensitive command and must be in uppercase.

- 6. Enter password and press Enter, which clears the existing password.
- 7. Enter auth none and press Enter, which removes the authentication level.
- 8. If you do not know the IP address, enter ip and press Enter.
- 9. Enter **timeout 15** and press **Enter**, which sets a reasonable timeout value.

Note: If the Bootloader timeout has been set too low to allow console port access, and the IP address cannot be discovered, then the DeviceMaster must be returned to Comtrol for re-flashing.

10. Connect the DeviceMaster directly to the PC/laptop running PortVision DX.

Note: If necessary, see <u>Installing PortVision DX</u> on Page 35.

- 11. Open PortVision DX.
- 12. Scan the network so that PortVision DX discovers the DeviceMaster.
- 13. Right-click the DeviceMaster and then click Telnet/SSH Session.

RedBoot> dis Loading disabled RedBoot> password Cleared RedBoot> auth none Auth: none RedBoot> IP

IP: 192.168.11.40 Mask: 255.255.255.0 Gateway: 192.168.11.1

RedBoot> timeout 15 Timeout 15 seconds RedBoot>

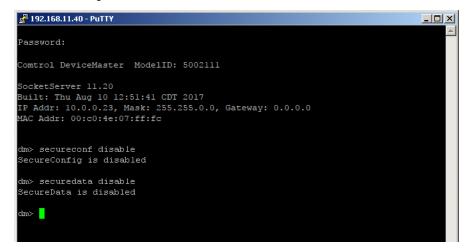
File Manage View Tools Help
Scan Refresh All Properties Save Load Upload Rebot Webpage Notes Help About Exit
IP ORTVISION First Floor [11 / 11] IP ORTVISION First Floor [11 / 11] IName : First Floor First Floor [11 / 11] IName : First Floor First Floor [11 / 11] IName : First Floor First Floor [11 / 11] IName : First Floor First Floor [11 / 11] INAME : First Floor First Floor [11 / 11] INAME : First Floor First Floor [11 / 11] INAME : First Floor First Floor [11 / 11] INAME : First Floor First Floor [11 / 11] INAME : First Floor First Floor [11 / 11]
Use menu or toobar to add notes in this area.
Device Name Configuration IP Address MAC Address Software Version Status V DM UP16 Tracker 1921681100 Oncode42600020 V14.e Ibi1.04) ON-UNE Use menu or toobar to add notes in the scree. W Modburs 5 Delete 19216811.03 Oncode42600020 Oncode42600020 Oncode42600020 On-UNE Use menu or toobar to add notes in the scree. Modburs 5 Delete 19216811.13 Oncode426100025 SockdeEvery 9.35 ON-UNE V Modburs 5 RTS-1P Fonter#10 RTS-1P Fonter#10 RTS-1P Fonter#10 RTS-1P Fonter#10 Oncode42100025 Oncode42100025 Oncode42100025 V Modburs 5 Delete 19216811.30 Oncode4210FRFB Nocode4210FFFB Nocode4210FFFB Nocode4210FFFB Nocode4210FFFB SockdeEvery 9.35 ON-UNE V RTS-1P Fonter#10 RTS-1P (FS) 19216811.14 Oncode4210FFFB SockdeEvery 9.35 ON-UNE V RTS-1P Fonter#10 RTS-1P (FS) 19216811.14 Oncode4210FFFB SockdeEvery 9.35 ON-UNE <t< td=""></t<>
Access the selected device(s) using Telnet session First Floor 11 1 Ready

14. Click Telnet, leave Port 23 as the Selected Port and click Ok

Telnet / SSH Settings
ⓒ Telnet Selected Port : 8000
OK Cancel

15. Press Enter at the Password prompt.

- 16. Enter secureconf disable and press Enter.
- 17. Enter securedata disable and press Enter.



Returning the DeviceMaster to Factory Defaults

The DeviceMaster uses two types of memory, volatile and non-volatile. The volatile memory is in the form of DRAM and SRAM. They are used for program execution and buffers. Clearing the volatile memory, as its name suggests, requires powering off the DeviceMaster.

The non-volatile memory is in the form of flash and EEPROM memories.

The flash memory is used for non-volatile program storage. Leaving the factory, there are two programs stored in the flash:

• Bootloader binary (bootloader.bin)

The bootloader binary is loaded into DRAM for execution, when the device is turned on. After a period of time, the bootloader loads the default application,

• Default application binary (SocketServer.bin)

SocketServer.bin or in some instances, a customer written custom application, into DRAM and it starts execution. It continues until the unit is powered off.

The only access you have to the binaries is if they decide to load a newer version. If this is done, the newer version overwrites that piece of flash. No user data is ever entered here.

Parameter Name	Default Value	User Configurable	Web or Telnet	Console Port	Port
Authentication	None	Yes	No	No	Yes
IP Address	192.168.250.250	Yes	Yes	Yes	Yes
IP Mask	255.255.0.0	Yes	Yes	Yes	Yes
IP Gateway	192.168.250.1	Yes	Yes	Yes	Yes
Password	Blank	Yes	Yes	No	Yes
Telnet	Enable	Yes	Yes	Yes	Yes
Telnet Timeout	300 sec.	Yes	Yes	Yes	Yes
Bootloader Timeout	15 sec.	Yes	Yes	Yes	Yes
SNMP	Enable	Yes	Yes	Yes	Yes
SSL†	Disable	Yes	Yes	Yes	Yes
† SSL is a security feature available with SocketServer v7.00 and later.					

The EEPROM memory is programmed with a number of default values. The values that you can modified are shown in the following table.

Clearing the Flash

The flash only has program binaries. There is no user data stored in the flash. If it is necessary to erase the binaries, the default application (**SocketServer.bin**) can be erased using the **fis init** command from the DeviceMaster using a serial connection, that is Port 1 through a null-modem cable and a COM port.

See <u>Establishing a Serial Connection</u> on Page 132 (<u>Steps 1</u> through 6) to access RedBoot and enter fis init -f at the RedBoot prompt.

There is no easy way to remove the bootloader binary. Removal of the bootloader binary would leave the DeviceMaster inoperable and require that it be returned to the factory to be reprogrammed.

Clearing EEPROM

The user configurable values in the EEPROM, can be accessed and set in three different ways. All of the values can be set using a serial connection (Port 1 with a null-modem cable connected to a COM port). Most of the values can be accessed by using the Web Server (SocketServer or NS-Link equivalent) or telnet. Refer to the appropriate procedure for your situation:

- <u>Telnet Access</u>
- Serial Port Access on Page 173
- <u>Web Server Access</u> on Page 173

Telnet Access

Use this procedure to access the DeviceMaster configuration through telnet,

- Note: To reset authentication, see <u>Serial Port Access</u> on Page 173 or use the <u>RedBoot Command Overview</u> on Page 137.
- 1. Open a telnet session, enter the DeviceMaster IP address. If using Windows, open a **Command** window and type **telnet** [*ip_address*].

Note: Press the Enter key if you have not programmed a password or use the password previously configured. The DeviceMaster does not come pre-programmed with a password.

2. To return the IP address to the default value, type **ip 192.168.250.250 255.255.0.0 192.168.250.1** and press **Enter**.

- 3. To reset the password, type **password** and press Enter.
- 4. To reset the telnet timeout value, type teltimeout 300 and press Enter.
- 5. To reset the bootloader timeout value, type timeout 15 and press Enter.
- 6. To enable SNMP, type **snmp enable** and press **Enter**.
- 7. To disable SSL, type **ssl disable** and press **Enter**. The SSL command is only available on DeviceMaster products running SocketServer 7.0 and later.

Serial Port Access

To use the serial method to access the DeviceMaster configuration, use <u>*Establishing a Serial Connection*</u> on Page 132. Once the connection is established, use the following commands to reset the factory default values.

- 1. To reset the authentication, type auth none and press Enter.
- 2. To return the IP address to the default value, type **ip 192.168.250.250 255.255.0.0 192.168.250.1** and press **Enter**.
- 3. To reset the password, type **password** and press **Enter**.
- 4. To reset the telnet timeout value, type teltimeout 300 and press Enter.
- 5. To reset the bootloader timeout value, type timeout 15 and press Enter.
- 6. To enable SNMP, type **snmp enable** and press **Enter**.
- 7. To disable SSL, type **ssl disable** and press **Enter**. The SSL command is only available on DeviceMaster products running SocketServer 7.0 and later.

Web Server Access

You can optionally use SocketServer (or the NS-Link equivalent) to access the DeviceMaster configuration and reset many values to their default values.

Some of the values require resetting the DeviceMaster to take effect. After changing the IP addresses and resetting the DeviceMaster, it will not reconnect automatically. You will need to use the new IP address to reconnect.

Note: The authentication method and the password cannot be changed using SocketServer.

To reset authentication, see <u>Serial Port Access</u> on Page 173 or use the <u>RedBoot Command Overview</u> on Page 137.

To reset the password, see <u>Configuring Passwords</u> on Page 136 or <u>Telnet Access</u> on Page 172.

- 1. Open your web browser and enter the IP address of the DeviceMaster.
- 2. Click Network |Security:
 - a. Verify that the Enable Secure Data Mode option is not checked.
 - b. Verify that the **Enable Secure Config Mode** option is not checked.
 - c. Verify that the Enable Telnet/SSH option is checked.
 - d. Verify that the **Enable Monitoring Secure Data via Telnet** option is not checked.
 - e. Verify that the Enable SNMP option is checked.
 - f. Click Save.
 - g. Click OK when reminded it is necessary to reboot to take effect.
- 3. Click the **Email** tab:
 - a. Verify that the SMTP Server IP Address is set to: 0.0.0.0.
 - b. Verify that all remaining options are clear.
 - c. Click Save.
 - d. Click OK.

Security Configuration

1

- 4. Return to the Server Status (home) page and click Reboot.
- 5. Click Set configuration for all ports to factory default settings.
- 6. Click Yes: Reboot.
- 7. Click the **Network** tab and make the following changes:
 - a. Click the Use static configuration below check box and enter the following values:
 - Set the IP Address to 192.168.250.250.
 - Set the Netmask to 255.255.0.0.
 - Set the Gateway to 192.168.250.1.
 - Set the Bootloader Timeout to 15.
 - b. Click Save.
 - c. Click **OK** when reminded it is necessary to reboot to take effect.

The DeviceMaster reboots. When it starts running, everything will have been returned to factory default values. If you choose to verify the values, the IP address has been reset to 192.168.250.250.

Technical Support

If you are using an NS-Link driver for a Windows system, you should review the troubleshooting section in the *DeviceMaster Device Driver (NS-Link) User Guide for Windows* (Page 11) before contacting Technical Support.

It contains troubleshooting procedures that you should perform before contacting Technical Support since they will request that you perform, some or all of the procedures before they will be able to help you diagnose your problem. If you need technical support use one of the following methods.

	Comtrol Contact Information
Downloads (FTP)	ftp://ftp.comtrol.com/html/default.htm
Downloads (HTTP)	http://downloads.comtrol.com/html/default.htm
Web site	http://www.comtrol.com
Phone	(763) 957-6000