



DeviceMaster

Installation and Configuration Guide



Trademark Notices

Control, NS-Link, and DeviceMaster are trademarks of Control Corporation.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

HyperTerminal is a registered trademark of Hilgraev, 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.

Fourth Edition, June 20, 2012

Copyright © 2001 - 2012. Control Corporation.

All Rights Reserved.

Control Corporation makes no representations or warranties with regard to the contents of this document or to the suitability of the Control 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	10
NS-Link COM Port Driver Installation Overview.....	10
Secure COM Port Redirector Installation Overview	11
NS-Link tty Port Installation Overview	11
TCP/IP Socket Port Installation Overview.....	12
Modbus Server Installation Overview	12
Locating Software and Documentation	12
Connectivity Requirements	14
Developer's Kit	14
Hardware Installation	15
Installation Overview	15
1-Port - Enclosed Installation	16
1-Port - Embedded Installation	18
Building the Serial Ribbon Cable.....	18
Mounting the Embedded	19
Attaching the Network and Serial Cables	20
Connecting the Power and Verifying Installation	20
2-Port (Serial Terminal) 1E/2E Installation	22
2-Port (DB9) 1E/2E Installation	24
4-Port and 8-Port Installation	26
16-Port (DeviceMaster RTS - External Power Supply) Installation	28
16-Port (DeviceMaster PRO) Installation	30
16/32-Port Rack Mount Models (Internal Power Supply) Installation	32
Initial Configuration	35
PortVision Plus Requirements	35
Installing PortVision Plus	35
Configuring the Network Settings	36
Checking the SocketServer Version	38
Uploading SocketServer with PortVision Plus	39
Local Network Segment	39
Using TFTP (Windows)	40
Uploading Modbus Server	47
Device Driver (NS-Link) Installation	49
Overview	49
Before Installing the NS-Link Driver	49
Existing Installations: NS-Link Driver Before V9.02 or SocketServer Before V8.00	49
Linux Installations	50
Windows Installations	51
Supported Operating Systems.....	51
Installation Overview for Windows.....	51
NS-Link for Windows Installation	51

- Configuring the NS-Link Driver for Windows 56**
- Configuring COM Port Properties for Windows 58**

- Secure COM Port Set Up..... 61**
 - Secure COM Port Redirector Overview 61**
 - Configuring Serial Ports and Enabling Security 61**
 - Installing the Secure COM Port Redirector 65**
 - Configuring Secure Redirector COM Ports 68**
 - Adding a Secure Port 68
 - Configuring the Secure COM Port 69

- Socket Port Configuration 71**
 - SocketServer Overview..... 71**
 - Web Page Help System 71
 - SocketServer Architecture 72
 - Accessing Socket Configuration 73**
 - Web Browser 73
 - PortVision Plus 73
 - SocketServer Versions 74**

- DeviceMaster Security..... 75**
 - Understanding Security Methods and Terminology..... 75**
 - PortVision Plus Considerations When Setting Security..... 79**
 - TCP and UDP Socket Ports Used by the DeviceMaster 80**
 - DeviceMaster Security Features 81**
 - Security Modes 81
 - Secure Data Mode and Secure Config Mode Comparison 81
 - DeviceMaster Security Feature Comparison..... 82
 - SSH Server 82
 - SSL Overview 83
 - SSL Authentication 83
 - Server Authentication 83
 - Client Authentication*..... 84
 - Certificates and Keys 84
 - SSL Performance 85
 - SSL Cipher Suites..... 85
 - DeviceMaster Supported Cipher Suites..... 86
 - SSL Resources 86
 - Configure/Enable Security Features 87**
 - PortVision Plus..... 87
 - Web Page - Security Configuration Area..... 88
 - Example 1..... 90
 - Example 2..... 90
 - Example 3..... 91
 - Key and Certificate Management 91
 - Using a Web Browser to Set Security Features 93**
 - Changing Security Configuration 93
 - Changing Keys and Certificates..... 94

Modbus Server Application Overview	95
Recommended Chassis	95
What is Modbus?	96
Modbus/RTU (Supported by Modbus Server)	96
Modbus/TCP (Not supported by Modbus Server).....	96
Modbus Server Functionality	97
Connecting Serial Devices	99
DB9 and RJ45 Connectors	99
DB9 Connectors	99
DB9 Null-Modem Cables (RS-232).....	100
DB9 Null-Modem Cables (RS-422).....	101
DB9 Straight-Through Cables (RS-232/485)	101
DB9 Loopback Plugs.....	101
RJ45 Connectors	102
RJ45 Null-Modem Cables (RS-232).....	102
RJ45 Null-Modem Cables (RS-422).....	102
RJ45 Straight-Through Cables (RS-232/485).....	103
RJ45 Loopback Plugs.....	103
RJ45 RS-485 Test Cable	103
Serial Terminals (4) - 1E	104
Serial Terminal (4) Connectors	104
Serial Terminal (4) Null-Modem Cables (RS-232)	105
Serial Terminal (4) Null-Modem Cables (RS-422)	105
Serial Terminal (4) Straight-Through Cables (RS-232/485).....	105
1E Loopback Signals.....	106
Serial Terminals (8) - 2E	107
Serial Terminal (8) Connectors	107
Serial Terminal (8) Null-Modem Cables (RS-232)	108
Serial Terminal (8) Null-Modem Cables (RS-422)	108
Serial Terminal (8) Straight-Through Cables (RS-232/485).....	108
2E Loopback Signals.....	109
Managing the DeviceMaster	111
Rebooting the DeviceMaster	111
Uploading SocketServer to Multiple DeviceMasters	112
Configuring Multiple DeviceMasters Network Addresses	113
Adding a New Device	114
Remote Using the IP Address.....	114
Local Using the IP Address or MAC Address.....	115
Using Configuration Files	116
Saving a Configuration File	116
Loading a Configuration File	117
Changing the Bootloader Timeout	119
Configure Device Screen (SocketServer v6.05 or Higher)	119
Telnet/SSH Session (SocketServer v6.04 and Below)	120
Managing Bootloader	123
Checking the Bootloader Version.....	123
Uploading Bootloader	123
Checking the NS-Link Version	125
Restoring Factory Defaults (2-Port, Only)	127
Restoring Serial Port Settings	127
NS-Link COM Port.....	127
Socket Port.....	127

RedBoot Procedures.....	129
Accessing RedBoot Overview.....	129
Establishing a Serial Connection	130
Establishing a Telnet Connection	131
Determining the Network Settings	132
Configuring the Network Settings	132
Changing the Bootloader Timeout.....	133
Determining the Bootloader Version.....	133
Resetting the DeviceMaster.....	134
Uploading Firmware.....	134
Serial Method.....	134
Telnet Method (Linux).....	136
Setting Up a TFTP Server in Linux	136
Uploading the Firmware.....	136
Configuring Passwords	138
RedBoot Command Overview.....	139
Hardware Specifications.....	141
Locating DeviceMaster Specifications	141
External Power Supply Specifications	142
1-Port 5VDC Power Supply.....	142
1-Port 5-30VDC Power Supply.....	142
2-Port (Serial Terminals) Power Supply	143
2-Port (DB9) Power Supply.....	143
4-Port Power Supply	144
8-Port Power Supply	144
16-Port Power Supplies	145
DeviceMaster Product Pictures	146
1-Port (DB9) 5VDC.....	146
1-Port (DB9) 5-30VDC.....	147
1-Port Embedded.....	148
2-Port (Single Ethernet Port) with Serial Terminals.....	148
2-Port (Dual Ethernet Ports) with Serial Terminals.....	148
2-Port (Single Ethernet Port) DB9.....	149
2-Port (Dual Ethernet Ports) DB9	149
4-Port (DB9).....	149
8-Port (DB9).....	149
16-Port (RJ45) External Power Supply	150
16-Port (RJ45) Internal Power Supply	150
DeviceMaster PRO 16-Port (RJ45)	150
DeviceMaster Serial Hub 16-Port (DB9).....	150
DeviceMaster RTS 32-Port (RJ45)	150
Notices.....	151
Radio Frequency Interference (RFI) (FCC 15.105)	151
Labeling Requirements (FCC 15.19).....	151
Modifications (FCC 15.21).....	151
Serial Cables (FCC 15.27)	151
Underwriters Laboratory	151
Important Safety Information	151

Troubleshooting and Technical Support	153
Troubleshooting Checklist	153
General Troubleshooting	155
Testing Ports Using Port Monitor (PMon2)	157
Overview	157
Testing Control COM Ports	157
Testing Ports Using Test Terminal	160
Overview	160
Opening Ports	160
Sending and Receiving Test Data (RS-232/422/485: 4-Wire)	161
Loopback Test (RS-232)	162
Sending and Receiving Data (RS-485: 2-Wire)	163
Socket Mode Serial Port Testing	166
Daisy-Chaining DeviceMaster 2E/4/8/16-Port Units	171
DeviceMaster LEDs	172
Port LEDs	172
Network and Device LEDs.....	172
Removing DeviceMaster Security Features	174
Serial Connection Method	174
Returning the DeviceMaster to Factory Defaults	176
Clearing the Flash	177
Clearing EEPROM.....	177
Telnet Access	177
Serial Port Access	178
Web Server Access	178
Technical Support	179

Introduction

This section discusses the following topics:

- [Supported DeviceMaster Models](#) on Page 9
- [DeviceMaster Port Usage](#) (below)
- [Installation Overview](#) on Page 10
 - [NS-Link COM Port Driver Installation Overview](#) on Page 10
 - [Secure COM Port Redirector Installation Overview](#) on Page 11
 - [NS-Link tty Port Installation Overview](#) on Page 11
 - [TCP/IP Socket Port Installation Overview](#) on Page 12
 - [Modbus Server Installation Overview](#) on Page 12
- [Locating Software and Documentation](#) on Page 12
- [Connectivity Requirements](#) on Page 14
- [Developer's Kit](#) on Page 14

Supported DeviceMaster Models

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

- DeviceMaster PRO
- DeviceMaster RTS
- DeviceMaster Serial Hub

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

DeviceMaster Port Usage

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

- *COM port* when the NS-Link driver for Windows is installed
- *Secure COM ports* when the secure port redirector 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
- *Modbus Server ports* when the Modbus Server firmware is uploaded and configured

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. Refer to [Hardware Installation](#) on Page 15 for detailed installation procedures for your DeviceMaster model.

2. Install PortVision Plus.

Control recommends connecting the DeviceMaster to a PC or laptop running Windows and that you install PortVision Plus for easy IP address configuration and firmware updates. See [PortVision Plus Requirements](#) on Page 35 and refer to [Installing PortVision Plus](#) on Page 35 to install PortVision Plus.

3. Program the IP address.

See [Configuring the Network Settings](#) on Page 36 for detailed configuration procedures.

4. If necessary, update [SocketServer](#).

Note: *Technical Supports recommends that you update to the latest version of SocketServer before installing an NS-Link device driver, the secure COM port redirector, or configuring socket ports. This step is not required if you planning on uploading Modbus Server onto the DeviceMaster. If you have existing installations with NS-Link, you may want to review [Existing Installations: NS-Link Driver Before V9.02 or SocketServer Before V8.00](#) on Page 49 for additional information about NS-Link changes.*

a. Check the SocketServer version. Refer to [Checking the SocketServer Version](#) on Page 38 to determine the version on the DeviceMaster. You can use the CD or the ftp site ftp://ftp.comtrol.com/dev_mstr/rts/software/socketserver/ to locate the latest version of SocketServer.

b. If necessary, update SocketServer. See [Uploading SocketServer with PortVision Plus](#) on Page 39 if you need to update SocketServer.

5. Go to the appropriate overview or overviews for your environment:

- NS-Link COM ports - [NS-Link COM Port Driver Installation Overview](#) on Page 10

Note: *If you require secure COM ports, you can also install the secure COM port redirector (Page 61) with or without the NS-Link device driver.*

- Secure COM ports - [Secure COM Port Redirector Installation Overview](#) on Page 11
- NS-Link tty ports - [NS-Link tty Port Installation Overview](#) on Page 11
- TCP/IP socket ports - [TCP/IP Socket Port Installation Overview](#) on Page 12
- Modbus Server ports - [Modbus Server Installation Overview](#) on Page 12

NS-Link COM Port Driver 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 Windows operating systems.

Note: *If you require secure COM ports, you can also install the secure COM port redirector (Page 61) with or without the NS-Link device driver.*

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

See [Windows Installations](#) on Page 51 for an installation overview of the NS-Link driver for Windows operating systems.

For detailed installation and configuration information, see the *DeviceMaster Device Driver (NS-Link) User Guide* on the CD or download the latest from the ftp site at: ftp://ftp.comtrol.com/dev_mstr/rts/drivers/win7/sw_doc/.

Note: Although the ftp link displays win7 in the path, the driver supports Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

3. Configure the COM ports using the Comtrol Drivers Management Console. See [Configuring the NS-Link Driver for Windows](#) on Page 56, which provides an overview of COM port configuration.
4. Configure device properties, you can refer to [Configuring COM Port Properties for Windows](#) on Page 58.
5. Optionally, you may need to configure one or more ports for socket mode. See [Socket Port Configuration](#) on Page 71 for information about configuring socket ports using the Server Configuration web page.
6. Connect the serial devices to the DeviceMaster. Refer to [Connecting Serial Devices](#) on Page 99 for cabling and connector information.

Secure COM Port Redirector Installation Overview

Use the following steps, which are discussed in detail in the subsequent sections, to install and configure the secure COM port redirector for the DeviceMaster.

1. After connecting the DeviceMaster, programming the IP address, and uploading the latest version of SocketServer, you are ready to configure SocketServer and install the secure port redirector.
2. Configure the serial port characteristics and enable the security feature in the SocketServer. Refer to [Configuring Serial Ports and Enabling Security](#) on Page 61 for detailed set-up procedures.
3. Install the secure port redirector. Refer to [Installing the Secure COM Port Redirector](#) on Page 65 for installation procedures.

You can use the CD or the ftp site ftp://ftp.comtrol.com/dev_mstr/rts/redirector/windows/ to locate the secure COM port redirector.

4. Configure the secure COM port redirector. You can refer to [Configuring Secure Redirector COM Ports](#) on Page 68 to complete the set up of the secure COM port redirector.
5. Connect the serial devices to the DeviceMaster. Refer to [Connecting Serial Devices](#) on Page 99 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.
2. Locate and unpack the driver assembly. You can use the CD or the ftp site ftp://ftp.comtrol.com/dev_mstr/rts/drivers/linux/ to locate the latest version of NS-Link Linux device driver.

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 [Socket Port Configuration](#) on Page 71 for information about configuring socket ports using the *Server Configuration* web page.
4. Connect the serial devices to the DeviceMaster. Refer to [Connecting Serial Devices](#) on Page 99 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 Plus 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 [Socket Port Configuration](#) on Page 71 for information for configuration procedures.

3. Connect the serial devices to the DeviceMaster. Refer to [Connecting Serial Devices](#) on Page 99 for cabling and connector information.

Modbus Server Installation Overview

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

Note: Only load the Modbus Server firmware if you want exclusively Modbus Server ports on the DeviceMaster.

1. After connecting the DeviceMaster and programming the IP address, you are ready to upload and configure Modbus Server firmware. For information about Modbus Server, see [Modbus Server Application Overview](#) on Page 95.

2. Upload Modbus Server using PortVision Plus.



You can use the CD or the web site to locate the latest version of Modbus Server at: <http://www.comtrol.com/content/downloads/>. See [Uploading Modbus Server](#) on Page 47 to upload Modbus Server.












3. Use the *Modbus Server User Guide* to configure the DeviceMaster port, which is available on the CD or you can download the latest version from the ftp site: ftp://ftp.comtrol.com/dev_mstr/rts/software/modbus_server/docs/modbus_server_user_guide.pdf to configure the DeviceMaster ports.
4. Connect the serial devices to the DeviceMaster. Refer to [Connecting Serial Devices](#) on Page 99 for cabling and connector information.

Locating Software and Documentation

You can access the appropriate software assembly, PortVision Plus, and the *DeviceMaster* documentation from the CD shipped with the DeviceMaster and use the CD to locate the latest files. Optionally, you can download the latest files using the following links, which opens the Comtrol ftp subdirectory that contains the latest file.

If you are not sure what files are required for your installation, each [Installation Overview](#) subsection also provides links to the required files in this *Guide*.

Software		Description	File	Document
Configuration Application	PortVision Plus	Install on a Windows host to configure the IP address and upload SocketServer on the DeviceMaster. PortVision Plus supports: <ul style="list-style-type: none"> • Windows 7 • Windows Server 2008 • Windows Vista • Windows Server 2003 • Windows XP 		 (This Guide)

Software		Description	File	Document
SocketServer	SocketServer	<p>This is the firmware that comes pre-installed on your DeviceMaster platform.</p> <p>You may need to upload the latest version of SocketServer before installing and configuring drivers or configuring sockets or the secure COM port redirector.</p>		 <i>(This Guide)</i>
Device Driver	Linux	Install if you want tty ports.		Readme file compressed in the driver assembly
	Windows 7 Windows Server 2008 Windows Vista Windows Server 2003 Windows XP	<p>Install if you want COM ports.</p> <p>You can also install and configure the Secure COM port redirector if you require secure COM ports.</p>		 <i>DeviceMaster Device Driver (NS-Link) User Guide</i>
Secure COM Port Redirector	Windows 7 Windows Server 2008 Windows Vista Windows Server 2003 Windows XP Windows 2000	Install and configure the Secure COM port redirector if you require secure COM ports.		 <i>(This Guide)</i>
Bootloader	Bootloader	<p>The operating system that runs on the DeviceMaster hardware during the power on phase, which then loads SocketServer.</p> <p>Only update the Bootloader on your DeviceMaster, if advised by Technical Support</p>		 <i>(This Guide)</i>
Modbus Server	Modbus Server	The Modbus Server firmware was designed to provide enhanced connectivity for OPC servers and applications that require Modbus/RTU communication from Ethernet TCP/IP or COM ports directly to serial ports.		 <i>Modbus Server User 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	Hub, switch, router, or NIC	10/100 ETHERNET
DeviceMaster RTS Embedded	Hub, switch, router, or NIC	RJ45 port (not labeled)
DeviceMaster RTS 2-port 1E	NIC	10/100
	Hub, switch, or router	
DeviceMaster RTS 2-port 2E	NIC	10/100 1E/2E
	Hub, switch, or router	
DeviceMaster RTS 4/8/16-port (external power supply)	NIC	DOWN
	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
	Hub, switch, or router	UP
DeviceMaster Serial Hub 8-port	NIC	DOWN
	Hub, switch, or router	UP
DeviceMaster Serial Hub 16-port	Hub, switch, router, or NIC	10/100 NETWORK

Developer's Kit

In addition to the standard capabilities of the DeviceMaster they are also a fully-programmable, embedded computing, platform.

If you are interested in writing your own applications for the DeviceMaster or would like information on how to obtain the Control DeviceMaster Developer's Kit, see <http://www.comtrol.com/pub/en/DeviceMaster-SDK-Support> or please contact your Control sales representative.

Note: *The DeviceMaster PRO is shipped with the Developer's Kit. The DeviceMaster RTS supports the Developer's Kit. The DeviceMaster Serial Hub is not supported in the Developer's Kit.*

Hardware Installation

Installation Overview

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

DeviceMaster PRO

DB9 serial ports with dual Ethernet†† ports	8†	4-Port and 8-Port Installation on Page 26
RJ45 serial ports with dual Ethernet†† ports	16	16-Port (DeviceMaster PRO) Installation on Page 30

Default Network Settings

IP address:
192.168.250.250
Subnet mask:
255.255.0.0
Gateway address:
192.168.250.1

DeviceMaster RTS

DB9 serial port with a single Ethernet port	1	1-Port - Enclosed Installation on Page 16
Embedded system	1	1-Port - Embedded Installation on Page 18
Screw terminal serial ports	2‡	2-Port (Serial Terminal) 1E/2E Installation on Page 22
DB9 serial ports	2‡	2-Port (DB9) 1E/2E Installation on Page 24
DB9 serial ports with dual Ethernet†† ports	4† or 8†	4-Port and 8-Port Installation on Page 26
RJ45 serial ports with dual Ethernet†† ports	16	16-Port (DeviceMaster RTS - External Power Supply) Installation on Page 28
RJ45 serial ports with a single Ethernet port	16 or 32	16/32-Port Rack Mount Models (Internal Power Supply) Installation on Page 32

DeviceMaster Serial Hub

DB9 serial ports with dual Ethernet†† ports	8	4-Port and 8-Port Installation on Page 26
DB9 serial ports with a single Ethernet port	16	16/32-Port Rack Mount Models (Internal Power Supply) Installation on Page 32

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

†† One of the Ethernet ports on the DeviceMaster is a built-in downstream port for daisy-chaining DeviceMaster systems or other network-ready devices.

‡ Either Ethernet port on the DeviceMaster RTS 2-port 2E model can be used for daisy-chaining DeviceMaster systems or other network-ready devices.

1-Port - Enclosed Installation

Use the following procedure to install the DeviceMaster 1-Port

1. Record the MAC address and serial number of the DeviceMaster on the customer service label provided.

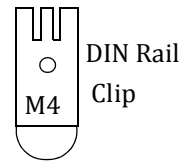
You may need the MAC address during driver configuration. The MAC address (starts with **00 C0 4E**) and serial number are located on a label on the DeviceMaster.

Note: Do not connect multiple units until you have changed the default IP address, see [Initial Configuration](#) on Page 35.

2. Place the 1-Port on a stable surface and skip to [Step 3](#) 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.)



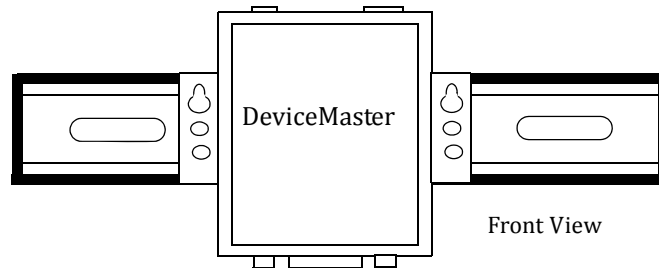
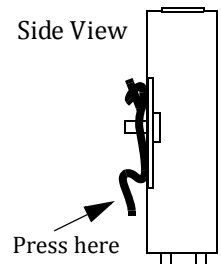
- c. Slide the DIN rail clip behind the DeviceMaster and line it up with one of the screw holes on the DeviceMaster.

- d. Insert the **M4** screw into the hole and tighten with a Phillips screwdriver.

- e. Repeat [Steps b](#) 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.



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

If you plan on using the NS-Link device driver, make sure that you do not connect RS-422/485 devices until the appropriate port interface type has been configured in the driver. The NS-Link default port setting is RS-232.

4. 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 [Step 5](#) to verify that the DeviceMaster is functioning properly.



Caution



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.

If you purchased the Control power supply (separately), the wires are identified below:

- Red = 5-30VDC positive
- White = 5-30VDC return
- Black = earth ground

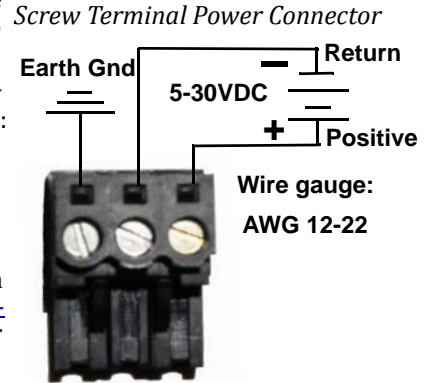
If you did not purchase a power supply from Control for the DeviceMaster, see [1-Port 5-30VDC Power Supply](#) on Page 142 for power requirements.

- 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 [Step 5](#) to verify that the DeviceMaster is functioning properly.

5. 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 Enclosed LED Descriptions	
Status	The amber Status LED on the device is lit, indicating you have power and it has completed the boot cycle. Note: <i>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.</i>
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 additional LED information, go to the Status LED table on Page 154.	

6. Go to [Initial Configuration](#) on Page 35 for default network settings and how to configure the DeviceMaster for use.

1-Port - Embedded Installation

Installing the DeviceMaster 1-Port Embedded system follows these basic steps:

- Building the serial ribbon cable (below).
- [Mounting the Embedded](#) on Page 19 and installing light pipes.
- [Attaching the Network and Serial Cables](#) on Page 20.
- [Connecting the Power and Verifying Installation](#) on Page 20.

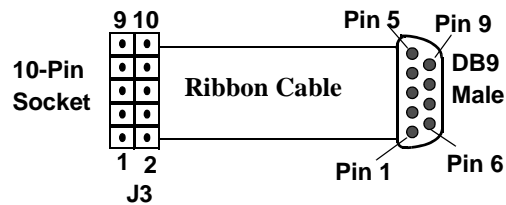


Caution

Observe proper ESD techniques when handling the DeviceMaster.

Building the Serial Ribbon Cable

Use the following information to build a DB9 serial ribbon cable to connect to the DeviceMaster 1-Port Embedded IDC10 connector (**J3**).



J3 Header	RS-232	RS-422	RS-485
1	CD	Not used	Not used
2	DSR	Not used	Not used
3	RxD	RxD-	Not used
4	RTS	TxD+	TRX+
5	TxD	TxD-	TRX-
6	CTS	RxD+	Not used
7	DTR	Not used	Not used
8	RI	Not used	Not used
9	GND	Not used	Not used
10	Not connected		

Mounting the Embedded



Caution

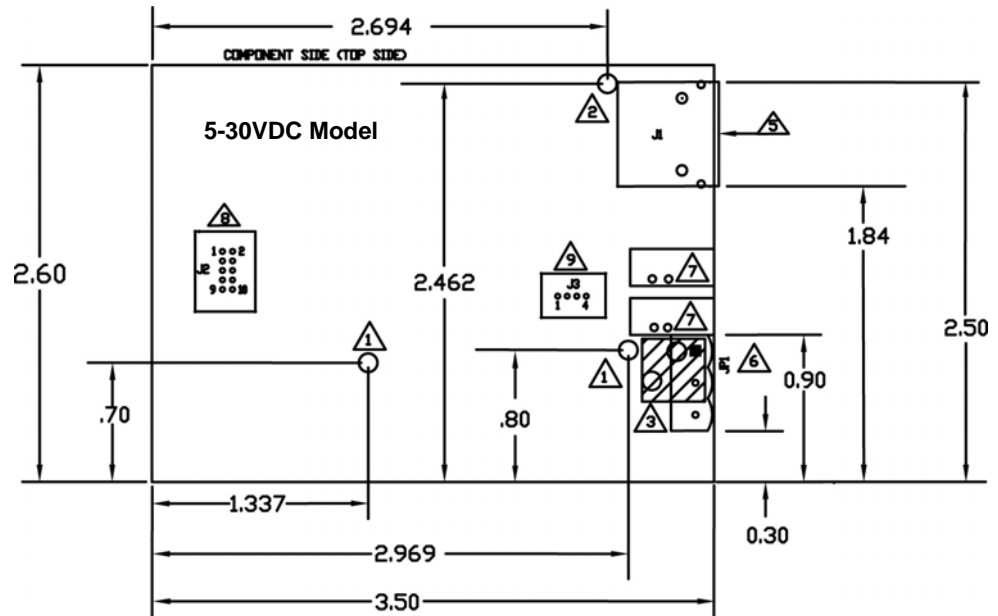
Use the following procedure to mount the DeviceMaster 1-Port Embedded with the 5-30VDC power supply.

Observe proper ESD techniques when handling the DeviceMaster.

- Carefully remove the DeviceMaster from the anti-static bag, following standard electrostatic device handling procedures.

Note: Write down the MAC address located on a label on the bottom (solder side) center of the DeviceMaster because you may need it during configuration.

- Mount the DeviceMaster for your environment using 1/4" stand-offs to separate the DeviceMaster from the base.



- 1 Non-plated/non-grounded mounting holes 0.116" diameter (+/-0.003").
- 2 Plated/chassis grounded mounting hole 0.116" diameter (+/-0.003").
- 3 WARNING: Holes in hatched area are not mounting holes.
- 4 Maximum component height above board is 0.55".
- 5 Ethernet connection J2: J2 overhangs board edge by 0.14" and the height is 0.55".
- 6 Power connector; the mating connector is Weidmuller P/N: 152651.
- 7 LED light pipe mounting holes. The LED light pipes are not provided.
- 8 Serial port connector J3: 0.1" pin spacing, 0.025" square pin diameter, and 0.230" pin height.
- 9 Debug port connector J4: 0.1" pin spacing, 0.025" square pin diameter, and 0.230" pin height.



Caution

- Use one of the following methods to ground the DeviceMaster.
 - Through the **power supply** by connecting the ground wire on the power cable using plastic or metal stand-offs.
 - Through the **chassis**, using metal stand-offs. If plastic stand-offs are used to mount the board, then you must ground the DeviceMaster using the power cable.

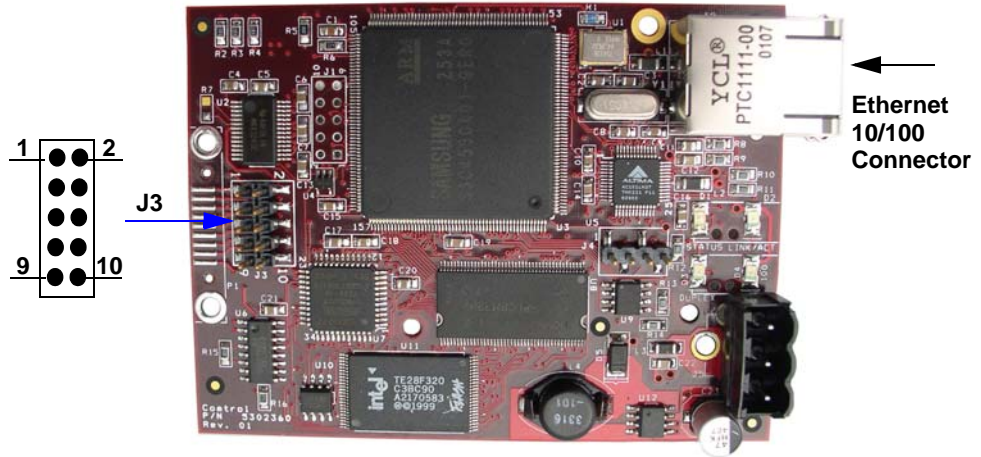
Note: The maximum diameter of the metal stand-offs should be 0.175" with a 4-40 machine screw. Metal stand-offs are not provided with the DeviceMaster.
- Optionally, attach the light pipes. The following light pipes have been tested and found to function; Bivar, Inc. (P/N:LP-230) and Ledtronics, Inc. (P/N:LTP003-OCW-001).

After mounting the DeviceMaster, you are ready to connect the cables.

Attaching the Network and Serial Cables

Use the following procedure to attach the serial ribbon and Ethernet cables. For a larger illustration of the system, see [1-Port Embedded](#) on Page 148.

1. Attach the ribbon cable built in [Building the Serial Ribbon Cable](#) on Page 18 to the header labeled **J3**.



2. Connect a standard Ethernet cable from the RJ45 port on the DeviceMaster to your Ethernet hub.

The default serial port setting on the DeviceMaster is RS-232. Do not connect the serial device until you have configured the serial port settings. You must configure network settings and upload firmware before configuring the serial port settings.



Use the next subsection to wire the power terminal connector and verify the hardware installation.

Connecting the Power and Verifying Installation

Use the following procedure to wire the power terminal connector and connect the DeviceMaster to a power source.

Observe proper ESD techniques when connecting and disconnecting the DeviceMaster.

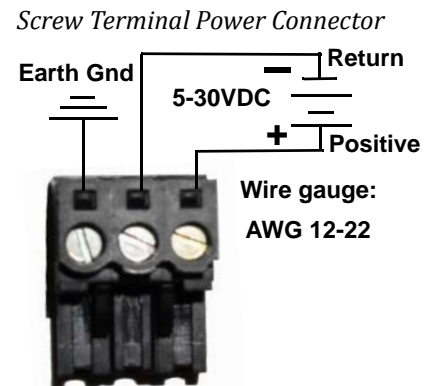
1. Insert the earth ground wire into the earth ground screw terminal.
2. Insert the DC positive wire into the positive screw terminal and the DC return wire into the return screw terminal.

If you purchased the Control power supply (separately), the wires are identified below:

- Red = 5-30VDC positive
- White = 5-30VDC return
- Black = earth ground

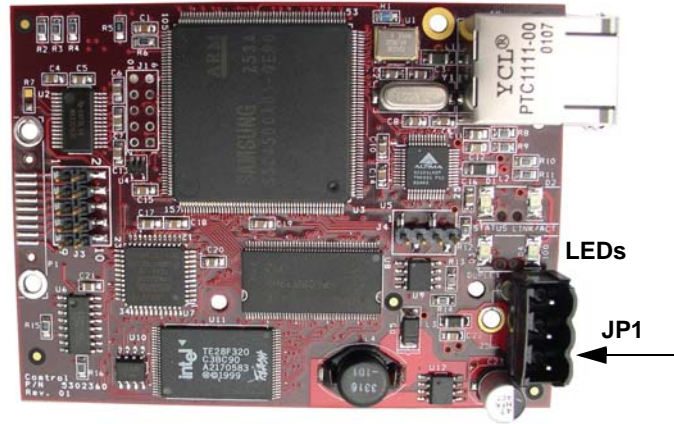
If you did not purchase a power supply from Control for the DeviceMaster, see [1-Port 5-30VDC Power Supply](#) on Page 142 for power requirements.

3. Use a small flat head screw to lock the wires into place.
4. Verify that each wire has been tightened securely.



5. Plug the screw terminal power connector into the DeviceMaster.
6. Connect the power supply to a power source.
7. Plug the screw terminal power connector into **JP1** on the DeviceMaster by aligning the scalloped sides.

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.



8. Apply power to the DeviceMaster.
9. Verify the **Status** LED has completed the boot cycle and network connection for the DeviceMaster is functioning properly using the table below.

The LEDs are located between the RJ45 connector and the power terminal block.

1-Port Embedded LED Descriptions	
Status	<p>When lit, the amber Status LED (D1) on the DeviceMaster indicates the devices is fully powered and has completed the boot cycle.</p> <p>Note: The Status LED flashes for approximately 15 seconds while booting. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.</p>
Link/Act	<p>When lit, the red Link/Act LED (D2) indicates a working Ethernet connection.</p>
Duplex	<p>When lit, the red Duplex (D3) LED indicates full-duplex activity.</p>
100	<p>When lit, the red 100 (D4) LED indicates a working 100 MB Ethernet connection (100 MB network, only). If the LED is not lit, it indicates a 10 MB Ethernet connection.</p>
<p>Note: For additional LED information, go to the Status LED table on Page 154.</p>	

10. Go to [Initial Configuration](#) on Page 35 for default network settings and how to configure the DeviceMaster for use.

2-Port (Serial Terminal) 1E/2E Installation

Use the following procedure to install DeviceMaster 2-port models with serial terminal connectors. See [2-Port \(DB9\) 1E/2E Installation](#) on Page 24 if the DeviceMaster has DB9 serial connectors.

- Record the MAC address and serial number of the DeviceMaster unit on the customer service label provided.

You may need the MAC address during driver configuration. The MAC address (starts with **00 C0 4E**) and serial number are located on a label on the DeviceMaster.

- Attach the DeviceMaster 2-Port to the DIN rail adapter.
- 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.



- Insert the earth ground wire into the chassis ground screw terminal. The chassis ground connection is made only if the DIN rail is NOT connected to signal ground.
- Insert the DC positive wire into the + screw terminal and the DC return wire into the - screw terminal.

If you purchased the Control power supply (separately), the wires are identified below:

- Red = 5-30VDC positive
- White = 5-30VDC return
- Black = chassis ground

If you did not purchase a power supply from Control for the DeviceMaster, see [2-Port \(Serial Terminals\) Power Supply](#) on Page 143 for power requirements.

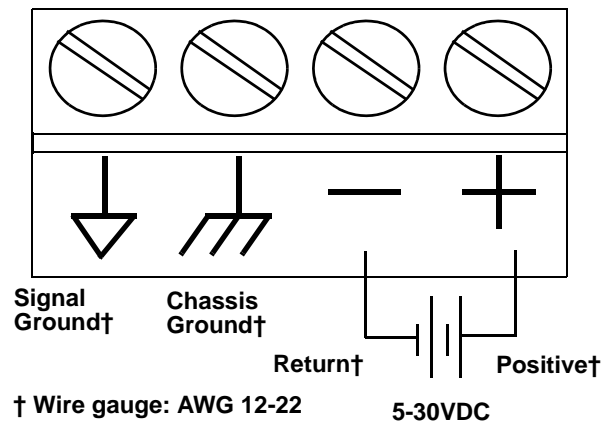
- Use a small flat head screw driver to lock the wires into place.
- Verify that each wire has been tightened securely.
- Connect the power supply to a power source.

Note: Do not connect multiple units until you have changed the default IP address, see [Initial Configuration](#) on Page 35.

- Use the appropriate method for network attachment of your DeviceMaster 2-port:
 DeviceMaster **1E**: Connect the **10/100 port** to the same Ethernet network segment as the host PC using a standard network cable.

DeviceMaster **2E**: Connect the DeviceMaster 2E using one of these methods:

- Ethernet hub, switch (10/100Base-T), Server NIC (10/100Base-T)**: Connect a **10/100** port to the same Ethernet network segment as the host PC using a standard Ethernet cable.
- Daisy-chaining DeviceMaster units**: Connect the port labeled **E1** (or **E2**) on the first DeviceMaster to the port labeled **E1** (or **E2**) on the second DeviceMaster or other device using a standard Ethernet cable. Refer to [Daisy-Chaining](#).



Signal Ground is used to connect RS-232 devices later in the installation.



[DeviceMaster 2E/4/8/16-Port Units](#) on Page 171 for more detailed information.

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

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

2-Port Serial Terminal LED Descriptions	
STATUS	The STATUS LED on the device is lit, indicating you have power and it has completed the boot cycle. <i>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.</i>
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.
<i>Note: For additional LED information, go to the Status LED table on Page 154.</i>	

- Go to [Initial Configuration](#) on Page 35 for default network settings and how to configure the DeviceMaster for use.

2-Port (DB9) 1E/2E Installation

Use the following procedure to install DeviceMaster 2-port models with DB9 connectors.

1. Record the MAC address and serial number of the DeviceMaster unit on the customer service label provided.

You may need the MAC address during driver configuration. The MAC address (starts with **00 C0 4E**) and serial number are located on a label on the DeviceMaster.

2. Attach the DeviceMaster 2-Port to the DIN rail adapter.
3. 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. 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.

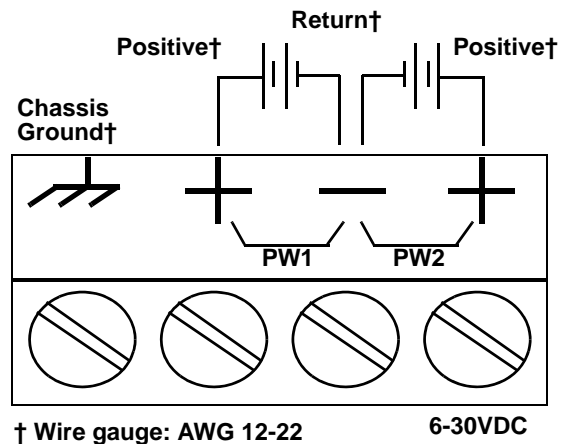
A second redundant power supply can be connected to the unit by inserting the DC positive wire into the other + screw terminal and the DC return wire into the - screw terminal.

The DeviceMaster will continue to operate if one of the two connected power supplies should fail.

If you purchased the Control power supply (separately), the wires are identified below:

- Red = 6-30VDC positive
- White = 6-30VDC return
- Black = chassis ground

If you did not purchase a power supply from Control for the DeviceMaster, see [2-Port \(DB9\) Power Supply](#) on Page 143 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 the power supply to a power source.

Note: *Do not connect multiple units until you have changed the default IP address, see [Initial Configuration](#) on Page 35.*

4. Use the appropriate method for network attachment of your DeviceMaster 2-port:
- DeviceMaster **1E**: Connect the **10/100 port** to the same Ethernet network segment as the host PC using a standard network cable.

DeviceMaster **2E**: Connect the DeviceMaster 2E using one of these methods:

- **Ethernet hub, switch (10/100Base-T), Server NIC (10/100Base-T)**: Connect a **10/100** port to the same Ethernet network segment as the host PC using a standard Ethernet cable.
- **Daisy-chaining DeviceMaster units**: Connect the port labeled **E1** (or **E2**) on the first DeviceMaster to the port labeled **E1** (or **E2**) on the second DeviceMaster or other device using a standard Ethernet cable. Refer to [Daisy-Chaining DeviceMaster 2E/4/8/16-Port Units](#) on Page 171 for more detailed information.

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



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

2-Port DB9 LED Descriptions	
STATUS	The STATUS LED on the device is lit, indicating you have power and it has completed the boot cycle. <i>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.</i>
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.
<i>Note: For additional LED information, go to the Status LED table on Page 154.</i>	

6. Go to [Initial Configuration](#) on Page 35 for default network settings and how 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. Record the MAC address and serial number of the DeviceMaster unit on the customer service label provided.

You may need the MAC address during driver configuration. The MAC address (starts with **00 C0 4E**) and serial number are located on a label on the DeviceMaster.

Note: *Do not connect multiple units until you have changed the default IP address, see [Initial Configuration](#) on Page 35.*

2. 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 RTS



Larger Picture, [Page 150](#)



Larger Picture, [Page 150](#)

*DeviceMaster PRO and
DeviceMaster Serial Hub*



Larger Picture, [Page 150](#)



Caution

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 [download the document](#) to mount the DeviceMaster on the shelf.*

3. Connect the DeviceMaster 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 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 [Daisy-Chaining DeviceMaster 2E/4/8/16-Port Units](#) on Page 171 for more detailed information.

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

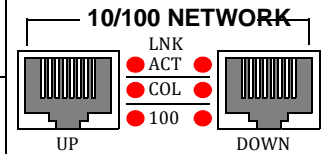


Caution

4. 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 your own power supply, see [4-Port Power Supply](#) on Page 144.

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

4-Port and 8-Port LED Descriptions	
PWR	LED on the front panel of the DeviceMaster is lit, indicating you have power and it has completed the boot cycle. 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.
<p>Note: For additional LED information, go to the Status LED table on Page 154.</p>	



6. Go to [Initial Configuration](#) on Page 35 for default network settings and how to configure the DeviceMaster for use.

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. Record the MAC address and serial number of the DeviceMaster unit on the customer service label provided.

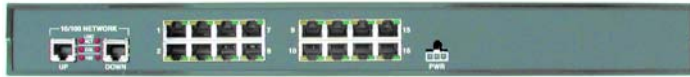
You may need the MAC address during driver configuration. The serial number and MAC address (starts with **00 C0 4E**) are located on a label on the DeviceMaster.

Note: Do not connect multiple units until you have changed the default IP address, see [Initial Configuration](#) on Page 35.

2. Place the DeviceMaster RTS 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.



Larger picture, [Page 150](#)

- c. Attach the L bracket into your rack.

Follow these guidelines when mounting the DeviceMaster RTS 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.**

3. Connect the DeviceMaster RTS 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 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 appropriate port interface type has been configured. The default port setting is RS-232.

4. 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 [External Power Supply Specifications](#) on Page 142 if you want to provide your own power supply.



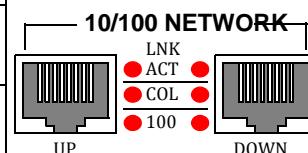
Caution



Caution

5. 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	
Red LED	Red LED on the front panel of the DeviceMaster is lit, indicating you have power and it has completed the boot cycle. Note: <i>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.</i>
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.
<p>Note: For additional LED information, go to the Status LED table on Page 154.</p>	



6. Go to [Initial Configuration](#) on Page 35 for default network settings and how to configure the DeviceMaster for use.

16-Port (DeviceMaster PRO) Installation

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

1. Record the MAC address and serial number of the DeviceMaster unit on the customer service label provided.

You may need the MAC address during driver configuration. The serial number and MAC address are located on a label on the device. The MAC address starts with **00 C0 4E**.

2. 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 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 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.**

3. 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 [Initial Configuration](#) on Page 35.

If you plan on using the NS-Link device driver, make sure that you do not connect RS-422/485 devices until the appropriate port interface type has been configured in the driver. The NS-Link default port setting is RS-232.

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



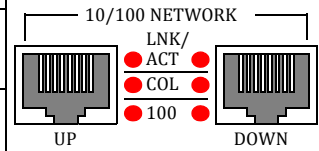
Caution



Caution

6. 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)	<p>Red LED on the front panel of the DeviceMaster PRO is lit, indicating you have power and it has completed the boot cycle.</p> <p>Note: <i>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.</i></p>
LNK/ACT	<p>The red LNK/ACT LED is lit, indicating that you have a working Ethernet connection.</p>
COL	<p>If the red COL LED is lit, there is a network collision.</p>
100	<p>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.</p>
<p>Note: For additional LED information, go to the Status LED table on Page 154.</p>	



7. Go to [Initial Configuration](#) on Page 35 for default network settings and how to configure the DeviceMaster for use.

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. Record the MAC address and serial number of the DeviceMaster unit on the customer service label provided.

You may need the MAC address during driver configuration. The serial number and MAC address (starts with **00 C0 4E**) are located on a label on the DeviceMaster.

Note: Do not connect multiple units until you have changed the default IP address, see [Initial Configuration](#) on Page 35.

2. 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.

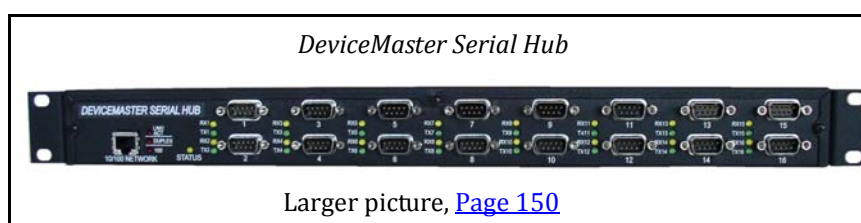
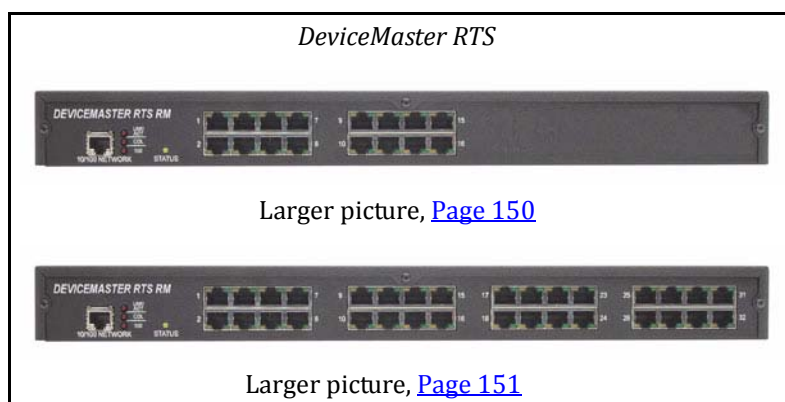
Follow these guidelines when mounting the DeviceMaster in a rack.

- **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.**



Caution

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



If you plan on using the NS-Link device driver, make sure that you do not connect RS-422/485 devices until the appropriate port interface type has been configured in the driver. The NS-Link default port setting is RS-232.

- 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.
- 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	
Status	<p>The amber Status LED on the device is lit, indicating you have power and it has completed the boot cycle.</p> <p>Note: <i>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 Status LED table on Page 154.</i></p>
LNK/ACT	<p>The red LNK/ACT LED is lit, indicating that you have a working Ethernet connection.</p>
Duplex	<p>If the red Duplex LED is lit, it indicates full-duplex activity.</p>
100	<p>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.</p>
<p>Note: <i>The port LED activity may be inconsistent until the port has been opened. After a port is opened, LED activity works as documented.</i></p>	

- Go to [Initial Configuration](#) on Page 35 for default network settings and how to configure the DeviceMaster for use.

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 Plus* for initial configuration.

This section shows you how to:

- Install PortVision Plus
- Configure the network address ([Page 36](#))
- Check the SocketServer version on the DeviceMaster ([Page 38](#))
- If necessary, download the latest version SocketServer and upload it into the DeviceMaster ([Page 39](#))
- Modbus Server, only load Modbus Server if you want a Modbus Server-only environment ([Page 47](#))

If you do not want to install PortVision Plus, see [RedBoot Procedures](#) on Page 129 for alternate methods to configure the network or upload the latest firmware.

PortVision Plus Requirements

Use PortVision Plus to identify, configure, update, and manage the DeviceMaster on the following operating systems:

- Windows 7
- Windows Server 2008
- Windows Vista
- Windows Server 2003
- Windows XP

PortVision Plus requires that you connect the DeviceMaster to the same network segment as the Windows host system during the configuration process.

If you have a previous version of PortVision Plus on your system, use the *Control Panel* to remove PortVision Plus before installing the latest version.

Note: A legacy version of PortVision Plus that supports [Windows 2000](#) is available.

See [PortVision Plus Considerations When Setting Security](#), Page 79 for more information.

Installing PortVision Plus

During initial configuration, PortVision Plus automatically detects and identifies DeviceMaster units, if they are in the same network segment by using the **Scan Network** button in PortVision Plus.

Use the *Software and Documentation* CD that came with the DeviceMaster to check for the latest version of PortVision Plus or use the link below to download the latest version.

1. Execute the **PVplus[version].msi** file and follow the installation wizard using one of the following methods:
 - **CD Installation:** Use the CD menu system to check the version on the CD against the latest released version.
 - **Download the latest version:** ftp://ftp.comtrol.com/dev_mstr/portvision_plus.

2. Click **Launch** and **Finish** in the last installation screen.
3. Click **Scan** so that PortVision Plus locates the DeviceMaster.

Note: *PortVision Plus locates all DeviceMaster models, including: the DeviceMaster 500, DeviceMaster PRO, DeviceMaster RTS, DeviceMaster Serial Hub, and DeviceMaster UP connect to the local Ethernet segment. If the DeviceMaster is not on the local segment and it has been programmed with an IP address, it will be necessary to manually add the DeviceMaster to PortVision Plus.*

4. Go to [Step 4](#) in the next section, *Configuring the Network Settings*, to program the DeviceMaster network settings.

If you need additional information about PortVision Plus, 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.

Default Network Settings

IP address:
192.168.250.250

Subnet mask:
255.255.0.0

Gateway address:
192.168.250.1

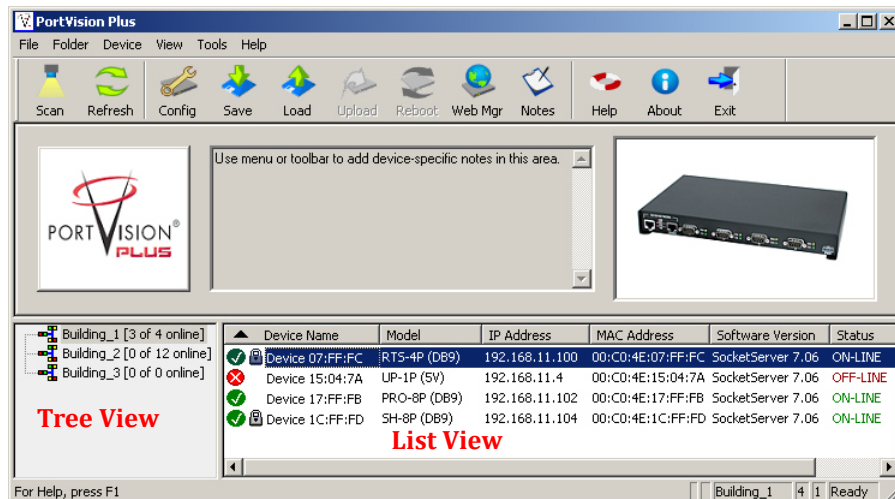
Note: *Technical Support advises configuring one new DeviceMaster at a time to avoid device driver configuration problems. If you want to configure multiple DeviceMasters using the **Assign IP to Multiple Devices** option, see [Configuring Multiple DeviceMasters Network Addresses](#) on Page 113.*

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 [Adding a New Device](#) on Page 114.

1. If you have not done so, install PortVision Plus ([Installing PortVision Plus](#) on Page 35).
2. Start PortVision Plus using the **PortVision Plus** desktop shortcut or from the **Start** button, click **Programs > Control > PortVision Plus > PortVision Plus**.
3. If this is the first time you have opened PortVision Plus, click **Scan** and then **Yes** to locate DeviceMasters on the network.

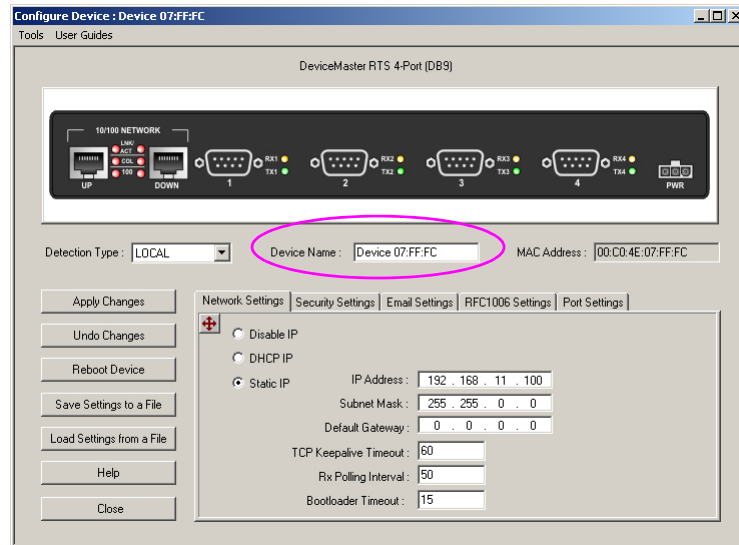
Note: *PortVision Plus will locate all Control DeviceMaster models, including: DeviceMaster 500, DeviceMaster PRO, DeviceMaster RTS, DeviceMaster Serial Hub and DeviceMaster UP.*

4. Highlight the DeviceMaster for which you want to program network information and open the **Configure Device** screen using one of these methods.
 - Double-click the DeviceMaster in the *List View* pane.
 - Click **Config**.
 - Right-click the DeviceMaster in the *List View* pane and click **Configure Device**.




Note: See the PortVision Plus Help system for detailed information.

- Optionally, rename the DeviceMaster in the **Device Name** field.



- 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 Plus Help system. Access the Help system using the Help button or go directly to the help for a specific property page by clicking the Context menu button ().

- Click **Apply Changes** to update the network information on the DeviceMaster.
- Optionally, click **Save Settings to a File** to create a configuration file that you can use to configure other DeviceMasters.

If you are deploying multiple DeviceMasters that share common values, you can save the configuration file and load that configuration onto other DeviceMasters.

You can refer to [Using Configuration Files](#) on Page 116 for more information.

- Click **Close** to exit the *Configure Device* window.
- Go to [Checking the SocketServer Version](#) on Page 38 to check the SocketServer version. You should update SocketServer firmware before any further configuration, unless you are planning on installing Modbus Server.

Checking the SocketServer Version

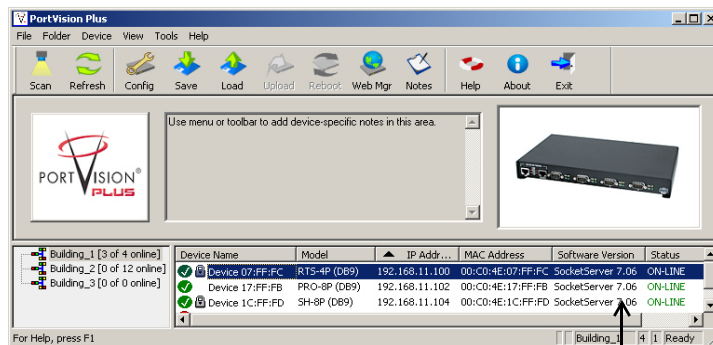
[SocketServer](#) refers to the web page that is integrated in the firmware that comes pre-installed on your DeviceMaster platform, which provides an interface to TCP/IP socket mode configuration and services. If you install an NS-Link device driver, an NS-Link version of SocketServer loads on the DeviceMaster.

Control recommends verifying that your DeviceMaster contains the latest SocketServer version before any further configuration to avoid installation problems.

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

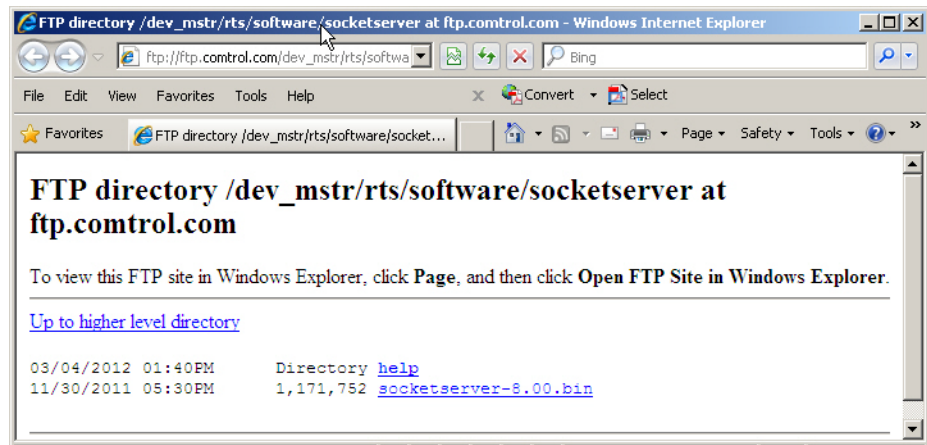
Use the following procedure to check the SocketServer version on the DeviceMaster.

1. If necessary, start PortVision Plus and scan the network.
2. Check the SocketServer version number of the *Software Version* for the DeviceMaster.



Version number

3. Check the Control web site to see if a later version is available at: ftp://ftp.control.com/dev_mstr/rts/software/socketserver.



Note: *The DeviceMaster PRO, DeviceMaster RTS, DeviceMaster Serial Hub, and DeviceMaster 500 all use the same firmware, although the path above points 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 [Uploading SocketServer with PortVision Plus](#) on Page 39.

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

Uploading SocketServer with PortVision Plus

Use this section to upload a new version of [SocketServer](#) on the DeviceMaster using PortVision Plus. Technical Support recommends updating SocketServer before any further configuration to avoid configuration problems. Use one of the two methods to upload SocketServer using PortVision Plus.

- Local network segment
- [Using TFTP \(Windows\)](#) on Page 40

Local Network Segment

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

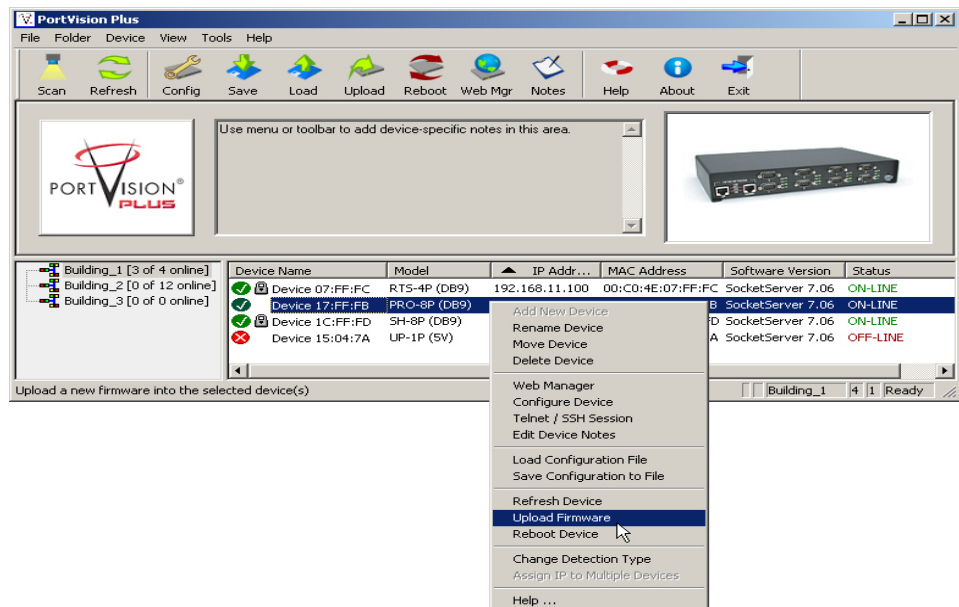
If the DeviceMaster is on the other side of several switches, a router, or wireless, go to [Using TFTP \(Windows\)](#) on Page 40, which provides more reliable uploads.

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

ftp://ftp.comtrol.com/dev_mstr/rts/software/socketserver.

Note: The Software and Documentation CD provides links to the latest files.

2. If necessary, open **PortVision Plus > Start/Programs > Control > PortVision Plus > PortVision Plus**.
3. Right-click the DeviceMaster or DeviceMasters for which you want to update, click **Upload Firmware**, browse to the SocketServer **.bin** file, and then click **Open**.



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 device. The device will reboot 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 Plus updates the *List View* pane and displays the new SocketServer version.
6. Click **Refresh**.
7. If the upload fails, reset the Bootloader timeout to 45 seconds and then repeat [Steps 3](#) through 6. For procedures, see [Changing the Bootloader Timeout](#) on Page 119.

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

- [Device Driver \(NS-Link\) Installation](#) on Page 49

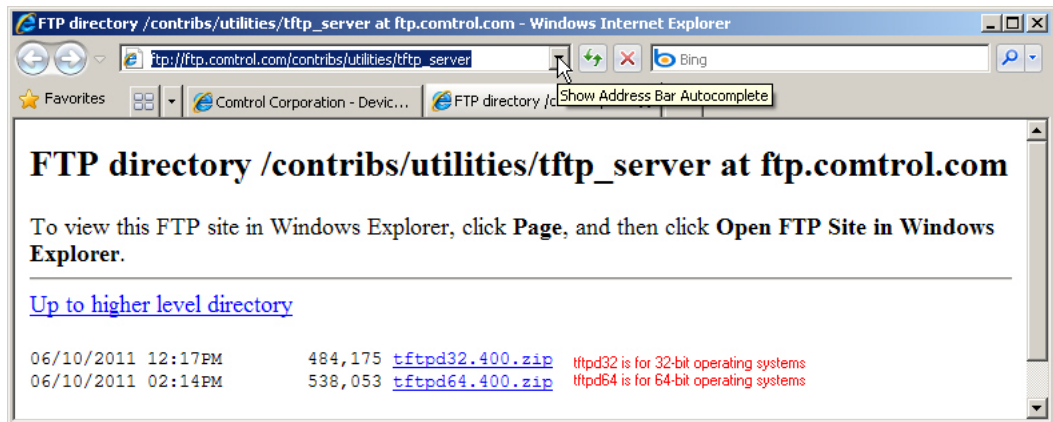
- [Secure COM Port Set Up](#) on Page 61
- [Socket Port Configuration](#) on Page 71

Using TFTP (Windows)

Use this procedure to update SocketServer with PortVision Plus using a TFTP server. If you have a TFTP server installed, skip to [Step 2](#).

1. If you do not have a TFTP server, you can download the appropriate one for your Windows operating system from the Control ftp site:

ftp://ftp.control.com/contribs/utilities/tftp_server



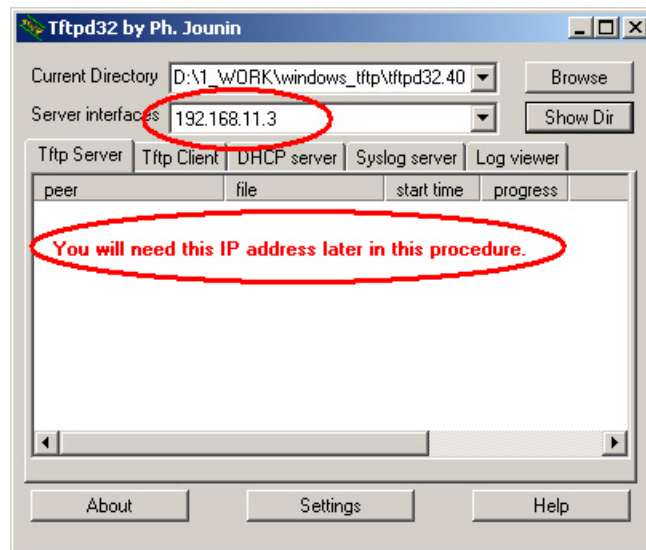
- a. Unzip the tftp server that you downloaded to your host system in a location that you can easily find.
- b. Execute the **tftpd32.exe** (or **tftpd64.exe**) file.
- c. Click **Run**.



- d. If necessary, click **Unblock**, if you receive this popup.

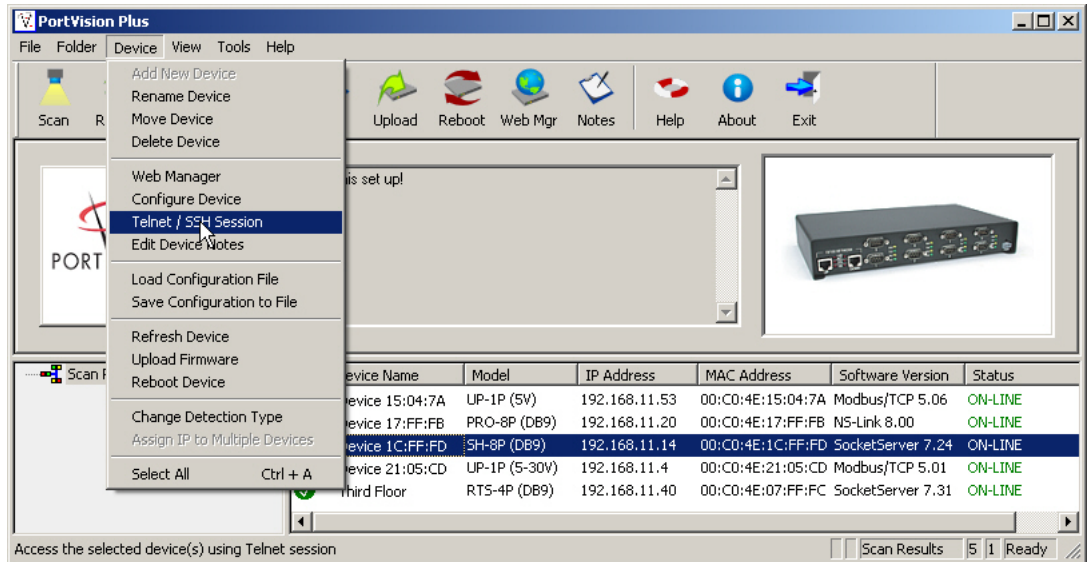


The **Tftpd** application opens:

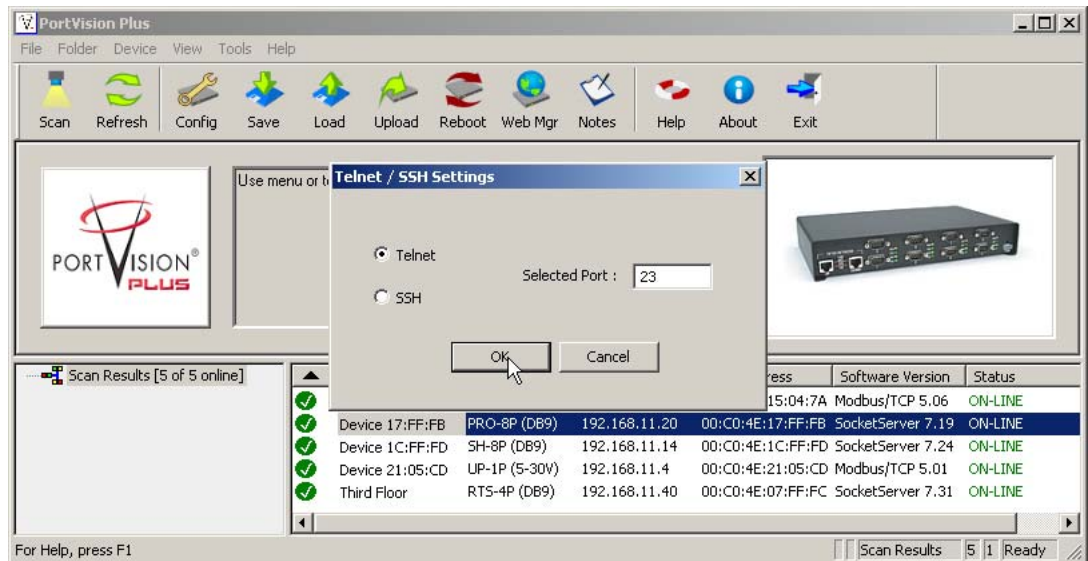


2. Make sure that you have downloaded the latest SocketServer version from: ftp://ftp.control.com/dev_mstr/rts/software/socketserver.
You may want to place SocketServer in the same directory that you placed the **Tftpd** server.
3. Rename the **SocketServer.bin** file to **1.bin**, which will make the following steps easier.
4. If necessary, open PortVision Plus: **Start >Program > Control > PortVision Plus > PortVision Plus**.

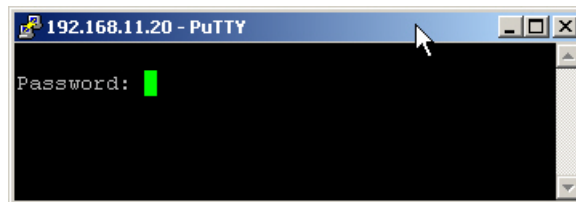
- Highlight the DeviceMaster for which you want to upload the latest SocketServer, and click **Telnet/SSH Session** from the **Device** menu.



- Click **Telnet**, leave Port 23 as the *Selected Port* and click **Ok**

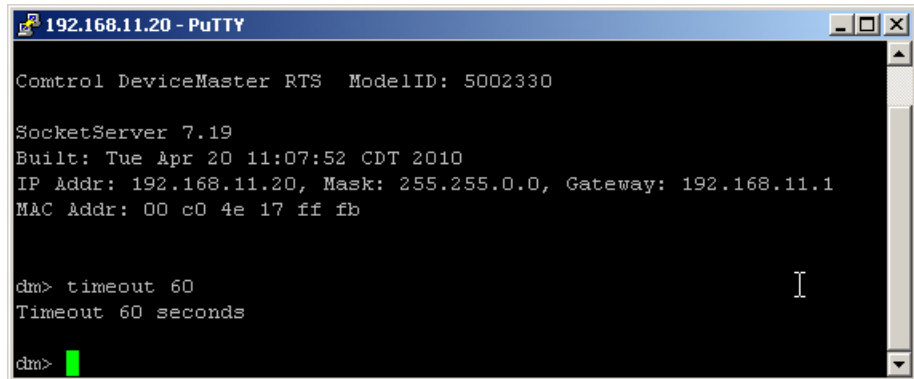


- If you have not set up a password, press **Enter** when the PuTTY screen appears or type the password and then press **Enter**.



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. To check this, return to PortVision Plus, double-click the DeviceMaster, and click the *Security Settings* tab. Click **Enable Telnet/ssh**, **Apply Changes**, and **Close**. Repeat [Step 6](#).

- At the **dm>** prompt, enter **timeout 60** and press **Enter**.



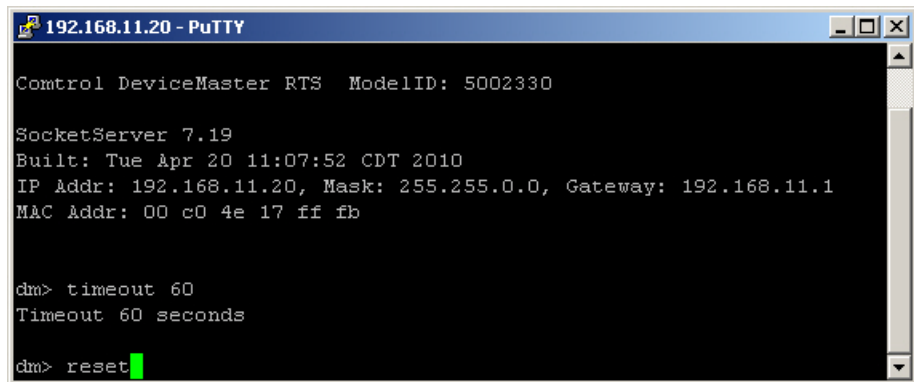
```
192.168.11.20 - PuTTY
Control DeviceMaster RTS ModelID: 5002330

SocketServer 7.19
Built: Tue Apr 20 11:07:52 CDT 2010
IP Addr: 192.168.11.20, Mask: 255.255.0.0, Gateway: 192.168.11.1
MAC Addr: 00 c0 4e 17 ff fb

dm> timeout 60
Timeout 60 seconds

dm>
```

- At the **dm>** prompt, enter **reset** and press **Enter**.



```
192.168.11.20 - PuTTY
Control DeviceMaster RTS ModelID: 5002330

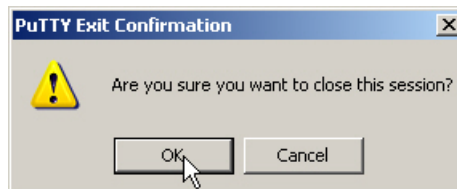
SocketServer 7.19
Built: Tue Apr 20 11:07:52 CDT 2010
IP Addr: 192.168.11.20, Mask: 255.255.0.0, Gateway: 192.168.11.1
MAC Addr: 00 c0 4e 17 ff fb

dm> timeout 60
Timeout 60 seconds

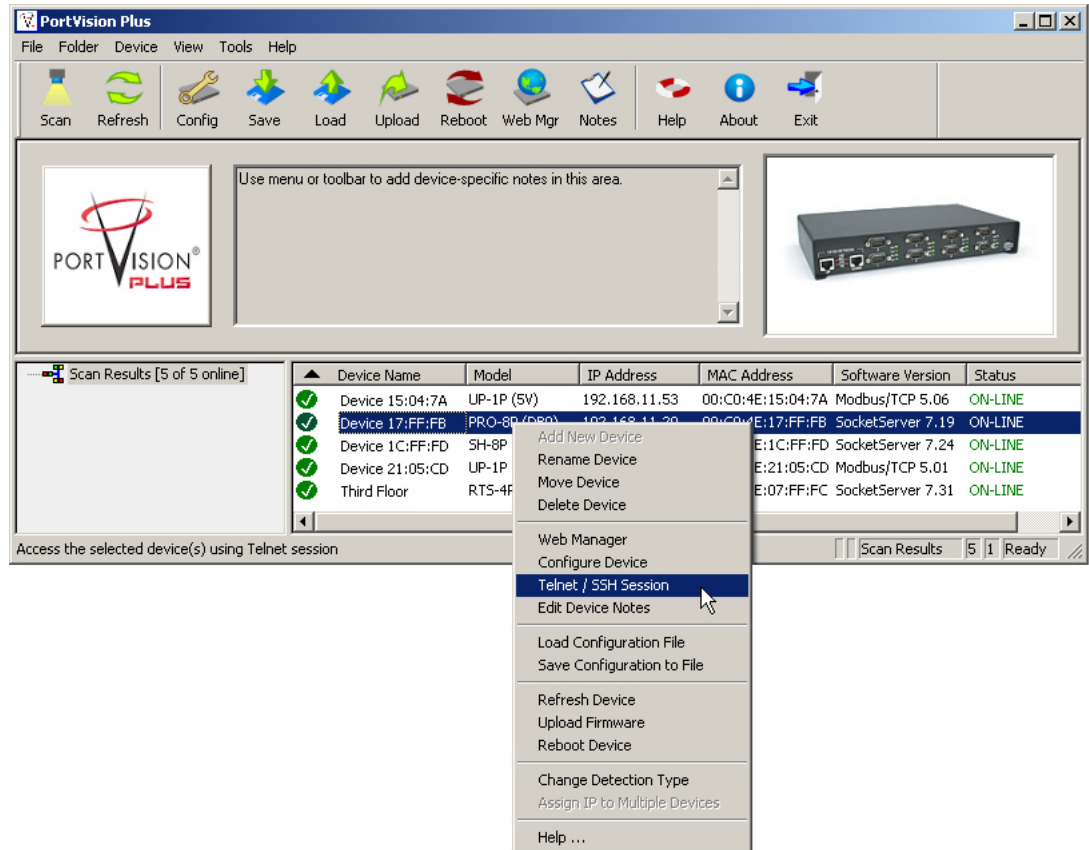
dm> reset
```

The DeviceMaster will reboot.

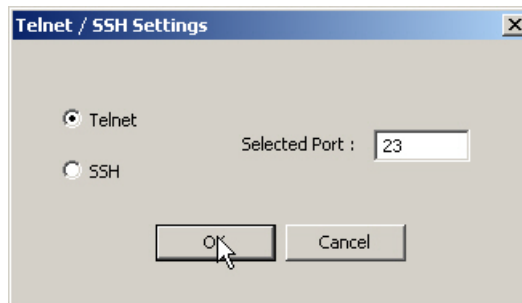
- Close the PuTTY session.



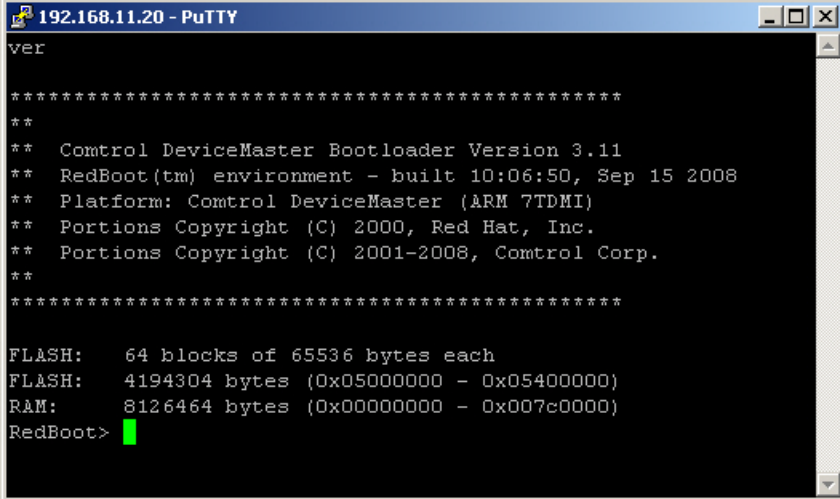
11. In PortVision Plus, right-click the DeviceMaster for which you want to upload the latest SocketServer, and select **Telnet/SSH Session**.



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



13. Make sure that the Bootloader version number displays with the **RedBoot>** prompt.



```

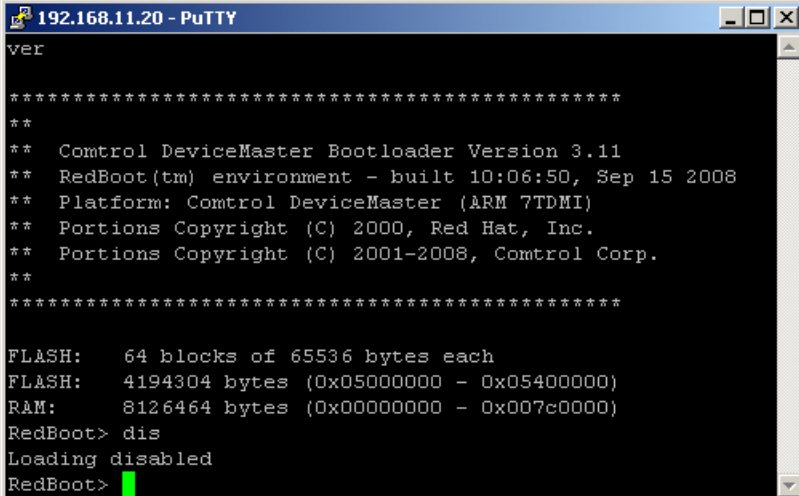
192.168.11.20 - PuTTY
ver
*****
**
** Control DeviceMaster Bootloader Version 3.11
** RedBoot(tm) environment - built 10:06:50, Sep 15 2008
** Platform: Control DeviceMaster (ARM 7TDMI)
** Portions Copyright (C) 2000, Red Hat, Inc.
** Portions Copyright (C) 2001-2008, Control Corp.
**
*****

FLASH: 64 blocks of 65536 bytes each
FLASH: 4194304 bytes (0x05000000 - 0x05400000)
RAM: 8126464 bytes (0x00000000 - 0x007c0000)
RedBoot>

```

If the **RedBoot>** prompt does not appear, reboot the DeviceMaster and try again. You must be at the **RedBoot>** prompt for the following steps. Repeat [Steps 6](#) through 12.

14. At the **RedBoot>** prompt, enter **dis** and press **Enter**.



```

192.168.11.20 - PuTTY
ver
*****
**
** Control DeviceMaster Bootloader Version 3.11
** RedBoot(tm) environment - built 10:06:50, Sep 15 2008
** Platform: Control DeviceMaster (ARM 7TDMI)
** Portions Copyright (C) 2000, Red Hat, Inc.
** Portions Copyright (C) 2001-2008, Control Corp.
**
*****

FLASH: 64 blocks of 65536 bytes each
FLASH: 4194304 bytes (0x05000000 - 0x05400000)
RAM: 8126464 bytes (0x00000000 - 0x007c0000)
RedBoot> dis
Loading disabled
RedBoot>

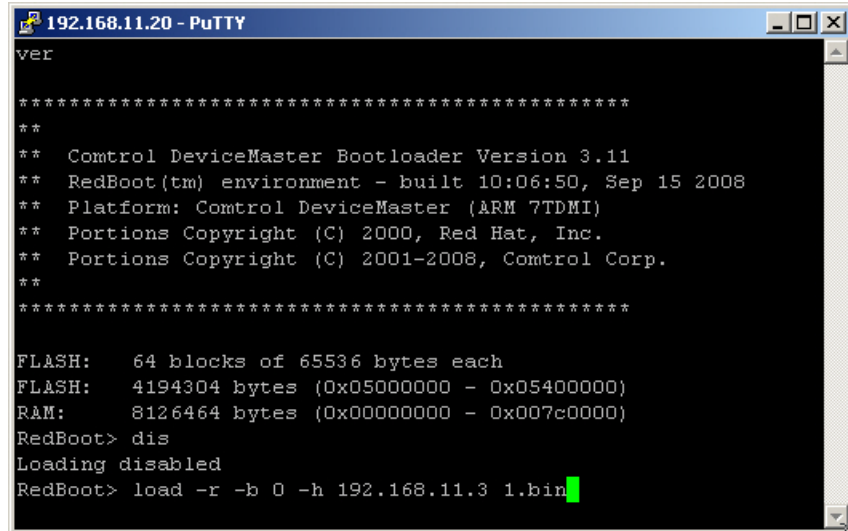
```

Note: Make sure that loading is disabled before performing the next step.

15. Enter the following command:

```
load -r -b 0 -h <tftp-Server_IP_Address> <Downloaded_File_Name>
```

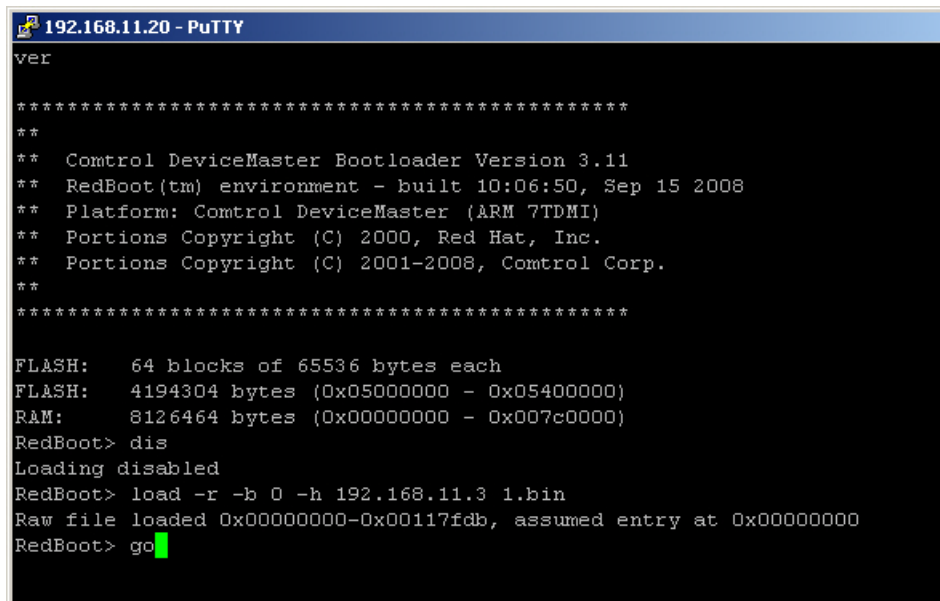
Note: Zero is the character between the `-b` and `-h`. The `tftp-Server_IP_Address` can be viewed in the application (Page 41) and if you renamed the file as suggested, the file name is `1.bin`.



```
192.168.11.20 - PuTTY
ver
*****
**
** Control DeviceMaster Bootloader Version 3.11
** RedBoot(tm) environment - built 10:06:50, Sep 15 2008
** Platform: Control DeviceMaster (ARM 7TDMI)
** Portions Copyright (C) 2000, Red Hat, Inc.
** Portions Copyright (C) 2001-2008, Comtrol Corp.
**
*****

FLASH: 64 blocks of 65536 bytes each
FLASH: 4194304 bytes (0x05000000 - 0x05400000)
RAM: 8126464 bytes (0x00000000 - 0x007c0000)
RedBoot> dis
Loading disabled
RedBoot> load -r -b 0 -h 192.168.11.3 1.bin
```

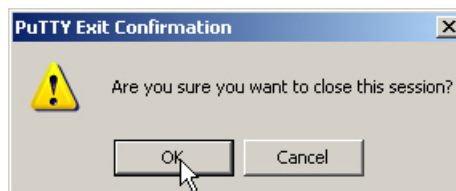
16. At the **RedBoot>** prompt, type **go** after the *raw* file string appears.



```
192.168.11.20 - PuTTY
ver
*****
**
** Control DeviceMaster Bootloader Version 3.11
** RedBoot(tm) environment - built 10:06:50, Sep 15 2008
** Platform: Control DeviceMaster (ARM 7TDMI)
** Portions Copyright (C) 2000, Red Hat, Inc.
** Portions Copyright (C) 2001-2008, Comtrol Corp.
**
*****

FLASH: 64 blocks of 65536 bytes each
FLASH: 4194304 bytes (0x05000000 - 0x05400000)
RAM: 8126464 bytes (0x00000000 - 0x007c0000)
RedBoot> dis
Loading disabled
RedBoot> load -r -b 0 -h 192.168.11.3 1.bin
Raw file loaded 0x00000000-0x00117fdb, assumed entry at 0x00000000
RedBoot> go
```

17. Close the PuTTY window and click **Ok**.



18. In PortVision Plus, highlight the DeviceMaster that you updated and click **Refresh**. You may need to click **Refresh** several times before you will see the latest SocketServer listed under the *Software Version*.

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

- [Device Driver \(NS-Link\) Installation](#) on Page 49
- [Secure COM Port Set Up](#) on Page 61
- [Socket Port Configuration](#) on Page 71

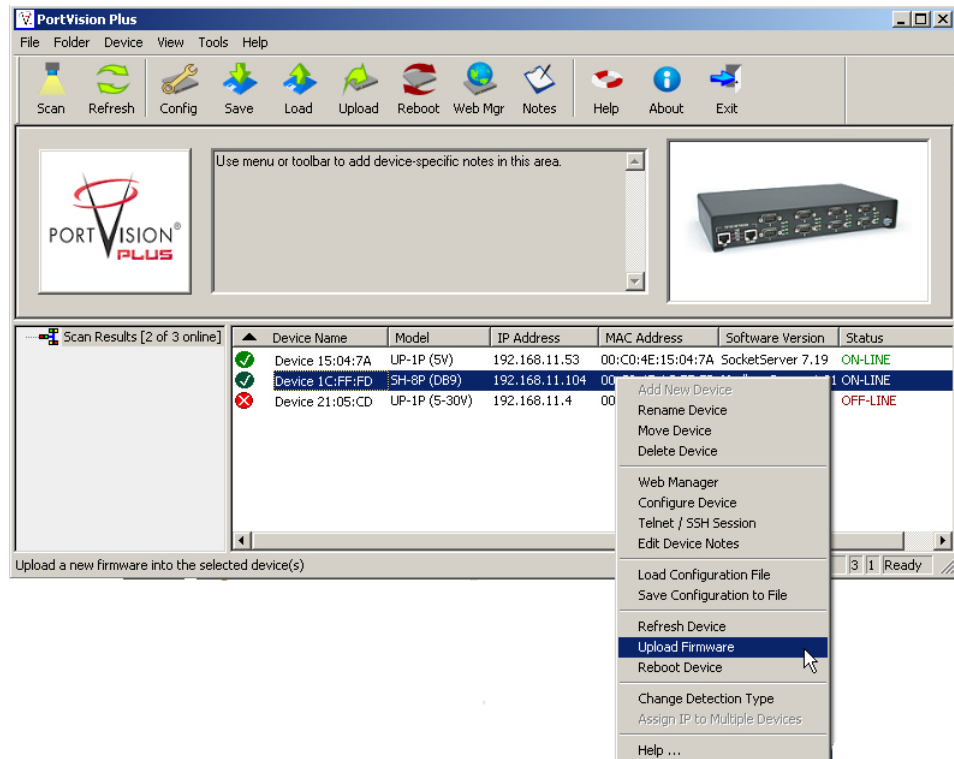
Uploading Modbus Server

Use this section to upload Modbus Server firmware on the DeviceMaster using PortVision Plus.

Note: Only load the Modbus Server firmware if you want exclusively Modbus Server ports on the DeviceMaster. For more information about Modbus Server, see [Modbus Server Application Overview](#) on Page 95.

1. Make sure that you have located or downloaded the [latest Modbus Server](#) firmware.
2. Execute the **Modbus_Server.msi** file and follow the file wizard.
3. Right-click the DeviceMaster for which you want to update, click **Upload Firmware**, browse to the Modbus Server **.bin** file, and then click **Open**.

The Modbus Server **.bin** was placed in the **Control/Modbus_Server** directory on your system until you changed the file location in the installation wizard.



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 device. The device will reboot 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 Plus updates the *List View* pane and displays the Modbus Server version.

Use the [DeviceMaster Modbus Server User Guide](#) to configure the DeviceMaster ports.

Device Driver (NS-Link) Installation

This section discusses the following topics:

- [Linux Installations](#) on Page 50
- [Windows Installations](#) on Page 51

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 15).
- The network information has been configured in the DeviceMaster ([Configuring the Network Settings](#) on Page 36).
- Checked to see if the latest version of SocketServer resides on the DeviceMaster ([Checking the SocketServer Version](#) on Page 38 using PortVision Plus or you can open your browser, enter the DeviceMaster IP address to view the version on the *Server Configuration* page).
- If necessary, uploaded the latest version of SocketServer ([Uploading SocketServer with PortVision Plus](#) on Page 39 or you can use RedBoot, [Uploading Firmware](#) on Page 134).

Note: *Technical Supports recommends that you update to the latest version of SocketServer before installing an 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 71).

Existing Installations: NS-Link Driver Before V9.02 or SocketServer Before V8.00

If you are familiar with the NS-Link device driver, you will be pleasantly surprised to find that NS-Link driver configuration is now handled in an easy to use *Management Console*. In addition, if you are comfortable with using the *Device Manager* configuration method, you can still configure the driver without changing your installation routine.

Previous to the NS-Link driver v9.02 and SocketServer v8.00, there were two versions of firmware that ran on the DeviceMaster, SocketServer and NS-Link.

With the release of v9.02 of the NS-Link driver, SocketServer and NS-Link have been incorporated into a single binary (.bin) file that may be named one of the following depending on the location from which it was loaded:

- nslink-8.xx.bin
- socketserver-8.xx.bin

where the version number of the .bin file is 8.00 or higher.

By default, once loaded, SocketServer shows in both the web page and PortVision Plus until the NS-Link device driver begins communication with this particular DeviceMaster.

Once a driver establishes communications, the firmware indicates that it is NS-Link. The driver does not need to upload firmware to the DeviceMaster or reboot the DeviceMaster.

If SocketServer does not change to NS-Link in the web page and PortVision Plus, then the NS-Link device driver loaded in the PC/laptop is NOT communicating with the DeviceMaster.

Note: Control recommends uploading the latest version of SocketServer before configuring the driver.

Linux Installations

You can locate the latest device driver for Linux using one of these methods:

- **Download the latest device driver:** ftp://ftp.comtrol.com/dev_mstr/rts/drivers/linux.

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

- **Software and Documentation CD:** You can use the CD to check the driver version on the CD against the latest released version. Open the `/html/default.htm` file to use the menu system, which provides you with links to download all software and documents.

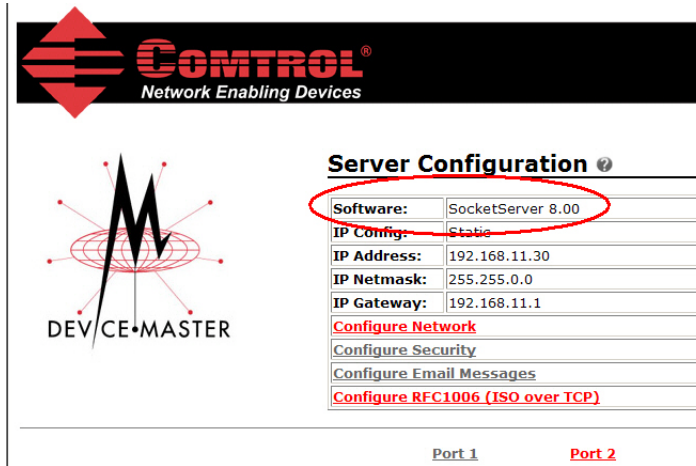
Refer to the **README** file packaged with the Linux driver for driver installation and configuration procedures.

Before you install the Linux NS-Link device driver:

1. Make sure that you have programmed an appropriate network address into the DeviceMaster. If you do not want to install PortVision Plus, you can use RedBoot, which is discussed in [Configuring the Network Settings](#) on Page 132.
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 Plus (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.



- b. Check the ftp site for the latest version: ftp://ftp.comtrol.com/dev_mstr/rts/software/SocketServer.
- c. If necessary, download the latest version and use RedBoot to upload the latest version of SocketServer, which is discussed in [Uploading Firmware](#) on Page 134.

Note: Technical Supports recommends that you update to the latest version of SocketServer before installing an NS-Link device driver. You can use PortVision Plus to check and upload the latest version (Page 38) or optionally use RedBoot (Page 134).

Windows Installations

This subsection provides an installation overview for the NS-Link device driver for Windows. For detailed installation and configuration information, see the *DeviceMaster Device Driver (NS-Link) User Guide for Windows*, which is available on the *Software and Documentation* CD or you can download the latest at: ftp://ftp.comtrol.com/dev_mstr/rts/drivers/win7/sw_doc/.

Note: Although the ftp link displays win7 in the path, the driver supports Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

Supported Operating Systems

The NS-Link device driver for Windows supports:

- Windows 7
- Windows Server 2008
- Windows Vista
- Windows Server 2003
- Window XP

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

If you require secure COM ports, you can also [install the secure COM port redirector](#) (Page 61) with or without the NS-Link device driver.

Note: Administrative privileges are required to install device drivers on Windows Vista, Windows Server 2008, and Windows 7 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 Control Drivers Management Console using the *Installation Wizard*.
- Configure the COM ports using the Control Drivers Management Console.
- Configure device properties using the Control 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 on the *Software and Documentation* CD if you do not have internet access or download the latest driver from:

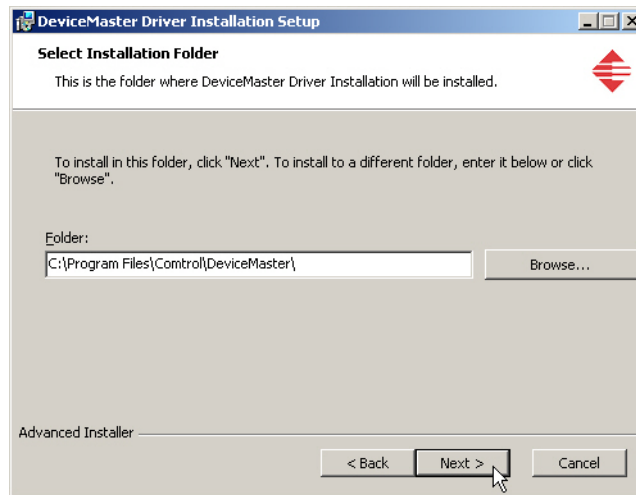
ftp://ftp.comtrol.com/dev_mstr/rts/drivers/win7.

Note: Although the ftp link displays win7 in the path, the driver supports Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

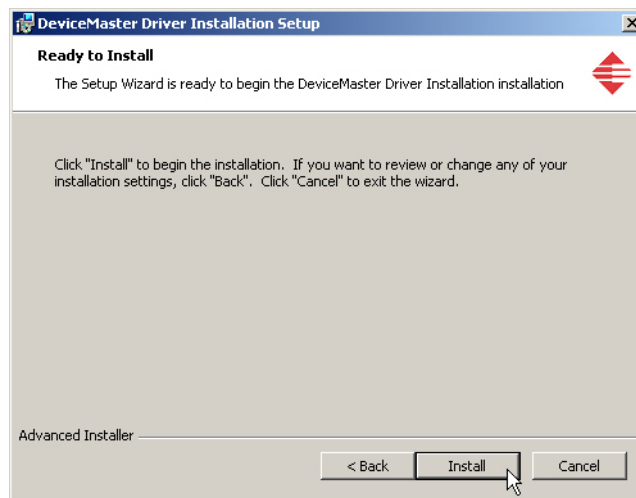
2. Execute the driver assembly **DeviceMaster_Windows_x.xx.exe** file and click **Next** to start the installation.



3. Click **Next** to install in the default location.



4. Click **Install**



5. 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: **Programs > Control > DeviceMaster > Driver Installation Wizard**.

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



7. Click **Next** to start the driver installation.



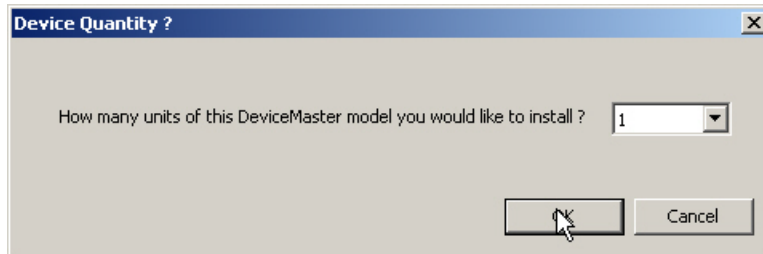
8. Click **Install** and **Next**



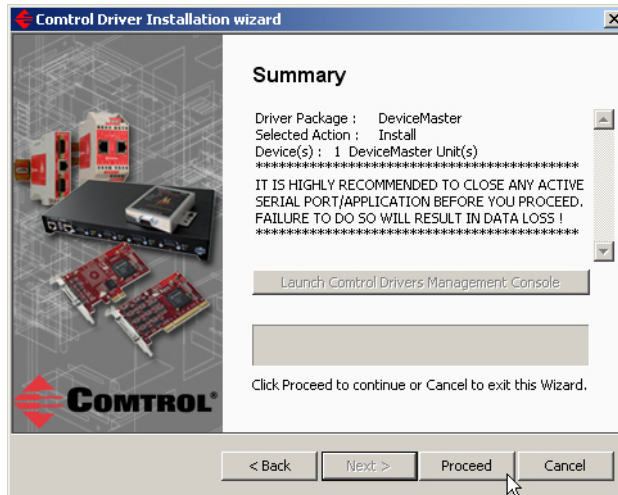
9. Select the DeviceMaster model that you are installing from the list.



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



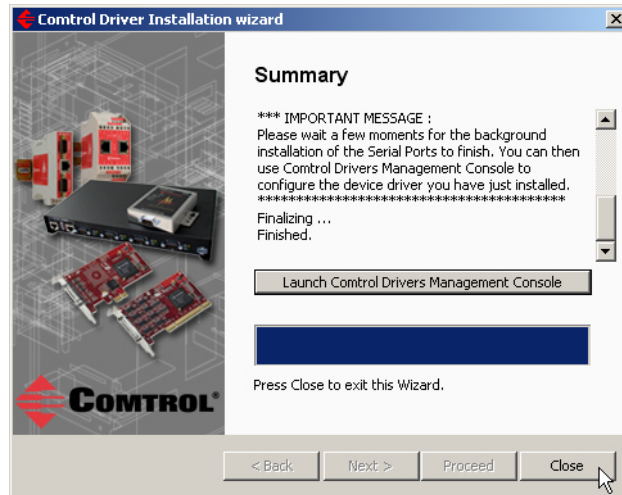
11. Repeat Steps 9 and 10 for each DeviceMaster that you are installing and click **Next**.
12. Click **Proceed**.



You may see the following popup for each port



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



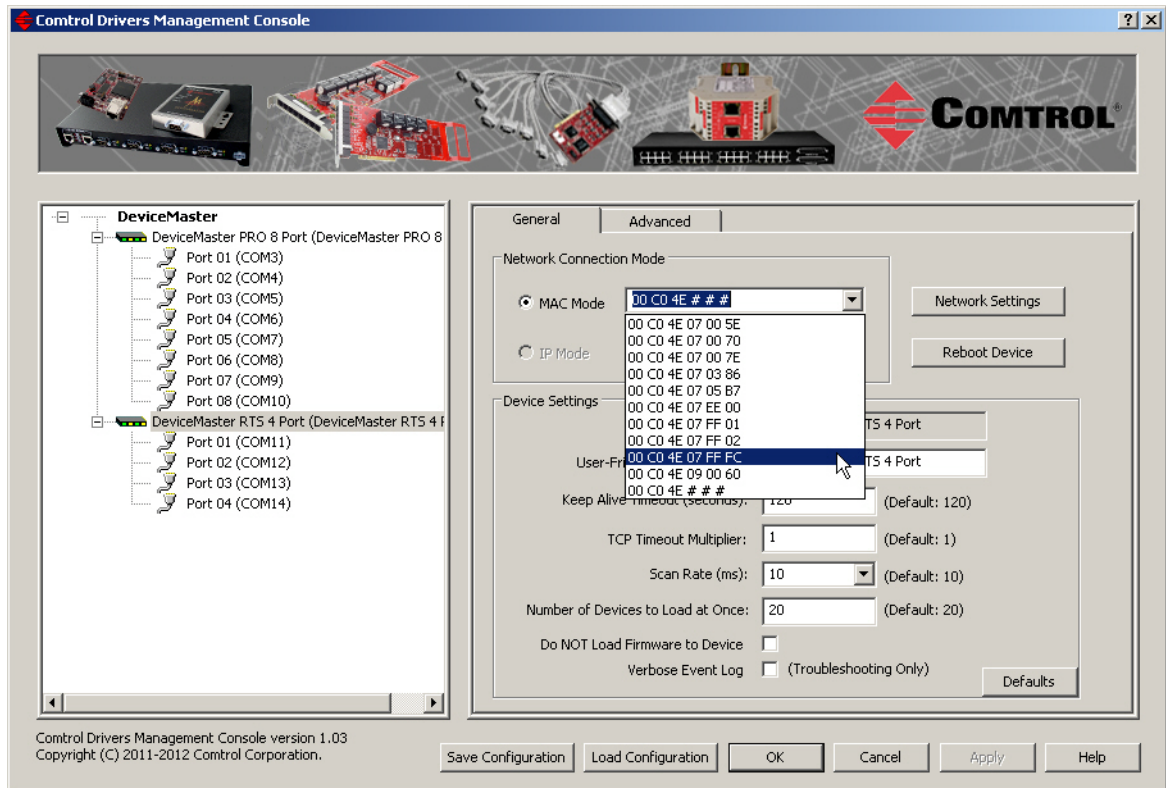
14. Go to the next subsection for NS-Link driver configuration procedures.

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 *Software and Documentation CD* or you can download the latest at: [ftp://ftp.comtrol.com/dev_mstr/rts/drivers/win7/sw_doc/](http://ftp.comtrol.com/dev_mstr/rts/drivers/win7/sw_doc/).

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 Control Drivers Management Console using the desktop shortcut or **Start > Programs > Control > DeviceMaster**.
2. Highlight the *Device Name* of the DeviceMaster that you want to configure.



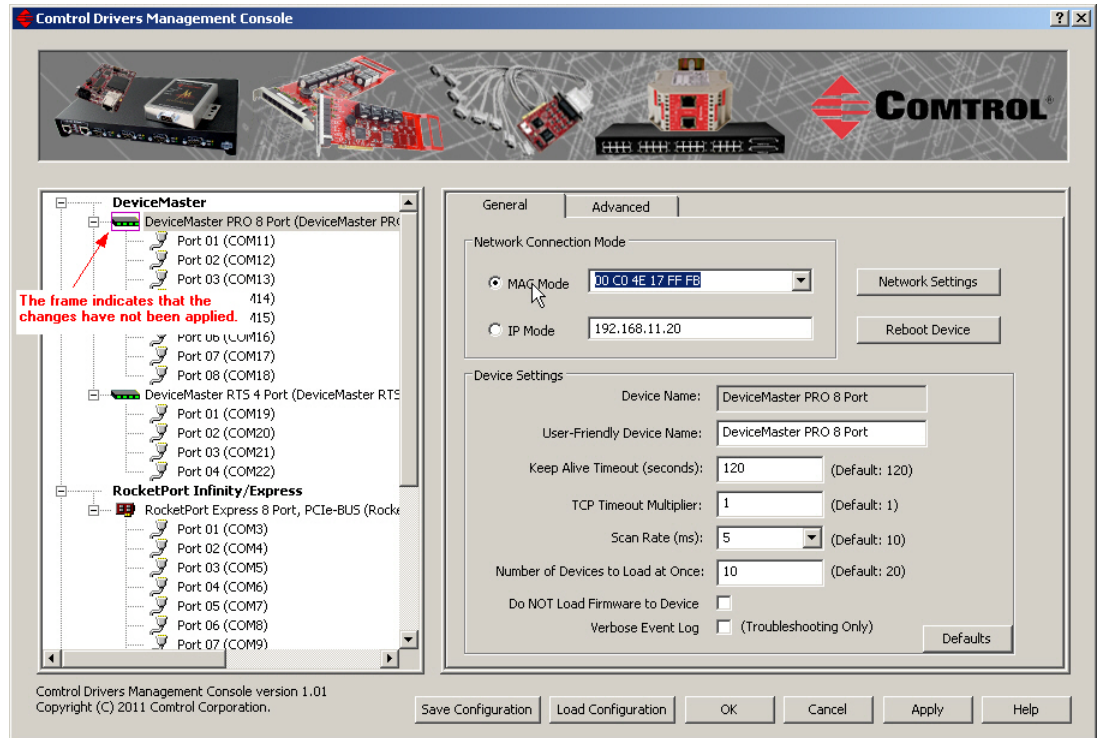
3. Select the MAC address from the drop-down list or enter the address from the MAC address label on the DeviceMaster. If you programmed the IP address using PortVision Plus, the IP address displays in the **IP Mode** text box after you select the MAC address.

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 Plus.

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 model DeviceMaster 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 Control 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.



5. 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

If you want use **IP mode** and the IP address is configured for your network, click the **IP Mode** radio button and click **Apply**.

Click the **Network Settings** button and click **Modify** to make any network settings changes.

6. Configure 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, change the **Number of Devices to Load at Once**.
- f. If necessary, click **Do NOT Attempt to Load Firmware in Device**.
- g. Optionally, click **Verbose Event Log** if you want to log additional DeviceMaster information into the event log.
- h. After making your changes, click **Apply** if you have additional configuration procedures or click **Ok** if you have completed configuring your DeviceMaster.

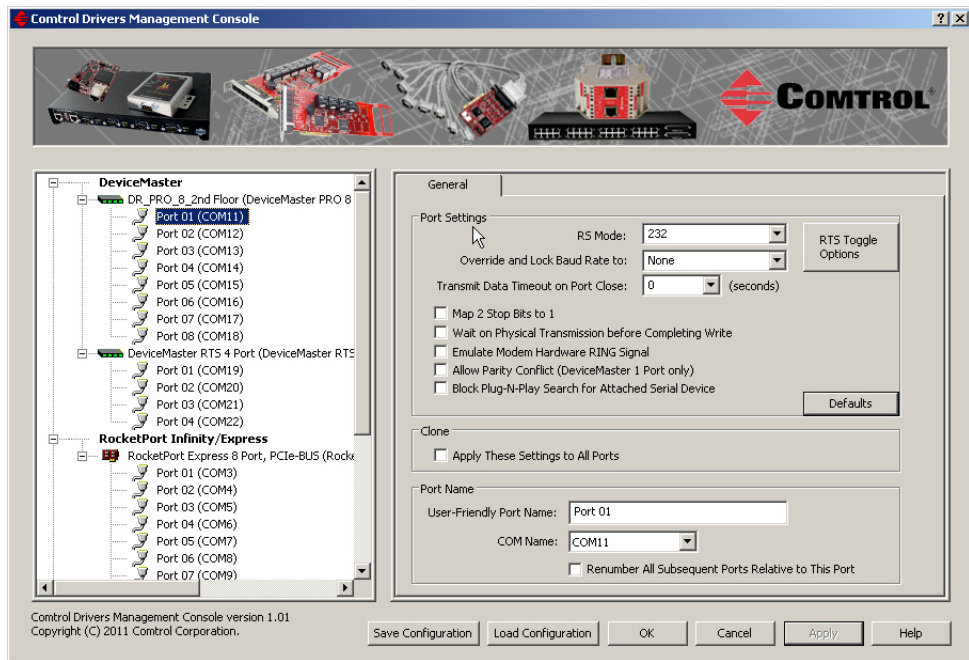
Note: You can refer to the help system if you need information about any of the options or features.

7. Optionally, you can click the **Advanced** tab and verify that the *Device Status* message indicates that the DeviceMaster is active and *Ok*.
8. 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 [DeviceMaster Device Driver \(NS-Link\) User Guide](#) (also available on the CD) or the NS-Link **Help** system for detailed configuration information.

1. Highlight the first port you want to configure.

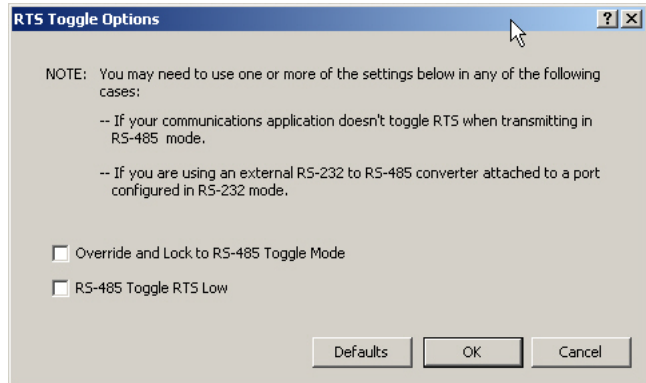


2. Complete the screen appropriately for the serial device that you plan on connecting to the port and click **Ok**.

- 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 FTS 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 [Steps 1](#) through 6.
8. Refer to [Connecting Serial Devices](#) on Page 99 to attach your serial device.
9. Optionally, you may need to configure one or more ports for socket mode ([Socket Port Configuration](#) on Page 71).

Secure COM Port Set Up

Before configuring security and installing the secure COM port redirector, the following conditions must be met:

- The DeviceMaster is connected to the network and powered on ([Hardware Installation on Page 15](#)).
- The network information has been configured in the DeviceMaster ([Configuring the Network Settings on Page 36](#)) for your network.
- If this is the initial secure port redirector installation, verify that the DeviceMaster contains the latest SocketServer ([Checking the SocketServer Version on Page 38](#)).

Secure COM Port Redirector Overview

If you require secure COM ports, you will need to do the following to set up secure COM ports on the DeviceMaster.

- Configure the serial port characteristics and enable the security feature in the SocketServer or NS-Link web page using the next subsection.
- Install the secure COM port redirector (Page 65).
- Add and configure the DeviceMaster serial port with the secure port redirector (Page 68).

If your site does not require security and you want to configure COM ports, you should install the [NS-Link device driver](#).

Configuring Serial Ports and Enabling Security

The first step to setting up a secure connection on the DeviceMaster is to use SocketServer or the NS-Link web page to enable the appropriate port or ports and configure DeviceMaster security.

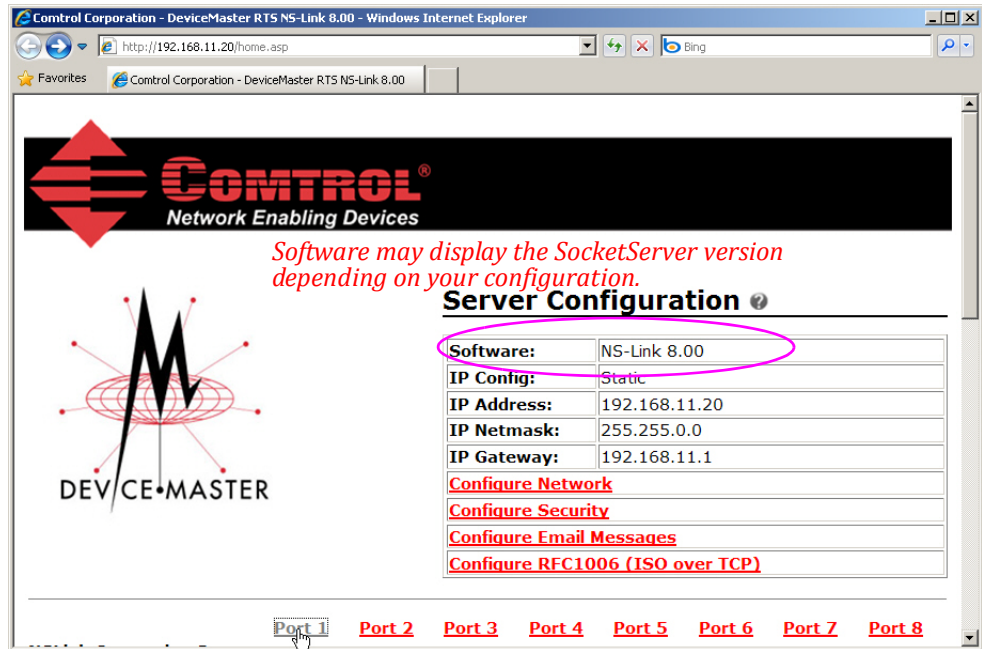
Note: *Make sure that the DeviceMaster contains the latest version of SocketServer or NS-Link before setting up security on the DeviceMaster.*

Refer to [Checking the SocketServer Version on Page 38](#) using PortVision Plus or [Checking the NS-Link Version on Page 125](#) using RedBoot, if you need to check for the latest version.

For additional information about DeviceMaster security, you can refer to [Socket Port Configuration on Page 71](#).

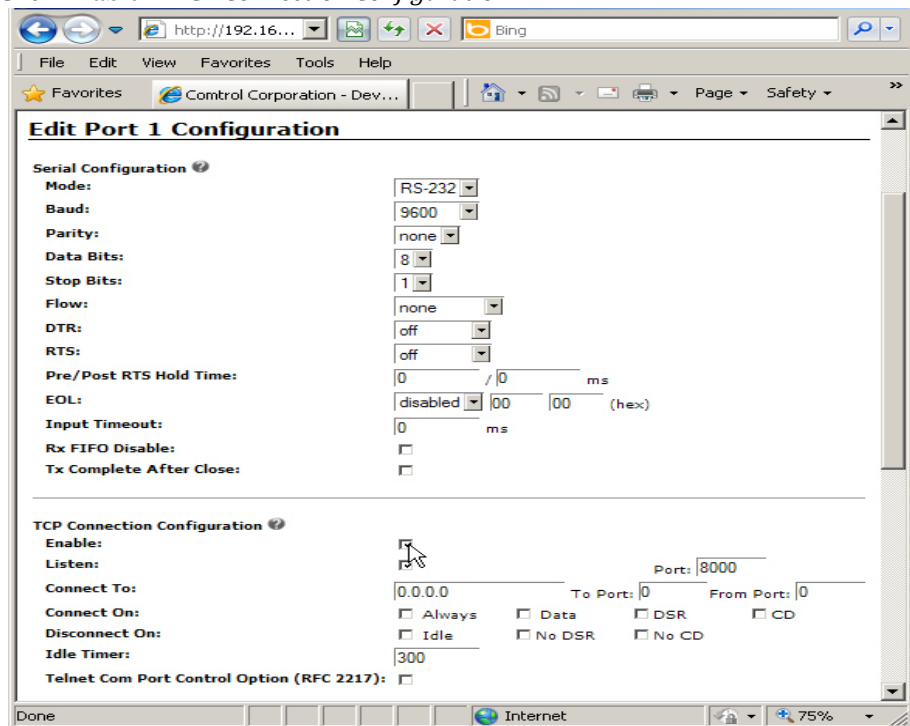
1. Open the DeviceMaster *Server Configuration* page using one of these methods:
 - Web browser, open a web browser and enter the IP address of the DeviceMaster that you want to configure.
 - PortVision Plus, right-click the DeviceMaster that you want to configure and click **Web Manager**.

- Click the port for which you want to configure.



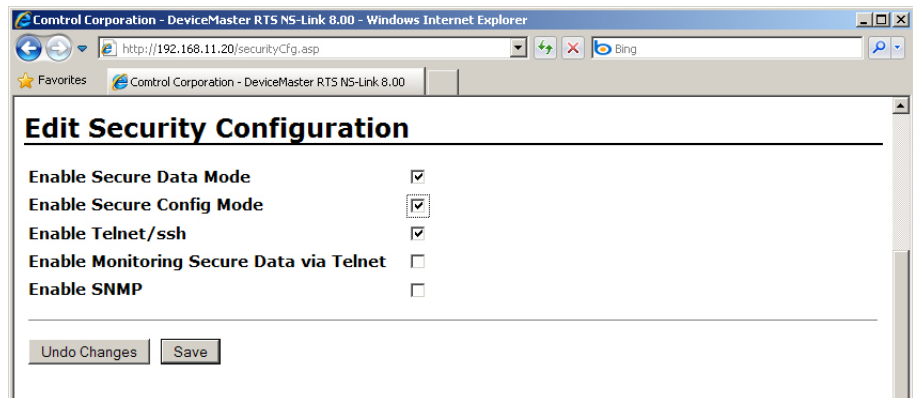
Note: Click the ? in a configuration area for field specific information or the Help button at the bottom of the page to view page level help.

- If connecting an RS-422 or RS-485 serial device to this port, select the appropriate setting from the *Mode* drop list.
- If necessary, set additional *Serial Configuration* parameters to match your serial device.
- Click **Enable** in *TCP Connection Configuration*.



6. Optionally, click **Clone** if you want to set up all of the DeviceMaster serial ports with the same serial characteristics.

***Note:** You will need the DeviceMaster IP address and the TCP port number to if you want to configure the secure COM port redirector.*
7. Click **Save**.
8. Click **Ok** at the *Configuration Updated* page.
9. Click **Configure Security**.
10. Click **Enable Secure Data Mode** so that TCP connections that carry data to/from the serial ports are encrypted using SSL or TLS security protocols. If this is enabled the following DeviceMaster features are disabled:
 - The Control proprietary MAC mode Ethernet driver protocol used in NS-Link and both UDP and MAC mode serial data transport
 - The e-mail feature in SocketServer
 - The RFC1006 features in SocketServer
11. Click **Enable Secure Config Mode** if you want to provide this level of security, which disables the following features:
 - 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. Encrypted access to the web server via port 443 (https:// URLs) is still allowed.
 - Administrative commands that change configuration or operating state which are received using the Control proprietary TCP driver protocol on TCP port 4606 are ignored.
 - Administrative commands that change configuration or operating state that are received using the Control MAC mode proprietary Ethernet protocol number 0x11FE are ignored.
12. You can leave **Enable Telnet/ssh** enabled (default) so that the DeviceMaster can communicate in Telnet.



13. If required, click **Set** to configure *RSA key pair* used by SSL and SSH servers.

This 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.

 - a. Click **Browse** to locate the server RSA key
 - b. Highlight the file, click **Open**, and then click **Upload**.
 - c. If you do not need upload any other files, go to [Step 17](#).

14. If required, click **Set** to configure 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.

- a. Click **Browse** to locate the RSA server certificate.
 - b. Highlight the file, click **Open**, and then click **Upload**.
 - c. If you do not need upload any other files, go to [Step 17](#).
15. If required, click **Set** to enter the *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.

16. If required, click **Set** to upload the *Client Authentication Certificate*.

If a CA certificate is uploaded, the DeviceMaster only allows SSL/TLS connections from client applications that provide to the DeviceMaster an identity certificate that has been signed by the CA certificate that was uploaded to the DeviceMaster.

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.

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.

- a. Click **Browse** to locate the *Client Authentication Certificate*.
 - b. Highlight the file, click **Open**, and then click **Upload**.
17. After completing the key and certification management, click **Save**.
 18. Click **Continue** if you have further configuration on this DeviceMaster or click **Reboot** for security to be enabled on the DeviceMaster.

Note: *Security is not enabled until the DeviceMaster has been rebooted.*

19. To configure another port as a secure COM port, update the *Serial Configuration* ([Step 2](#)).
20. If you want to configure a secure COM port, you are ready to install the secure port redirector using the next subsection, *Installing the Secure COM Port Redirector*.
21. Close the web page.

Installing the Secure COM Port Redirector

You can refer to the help system in the secure COM port redirector or use the following procedure to install the secure port redirector for Windows.

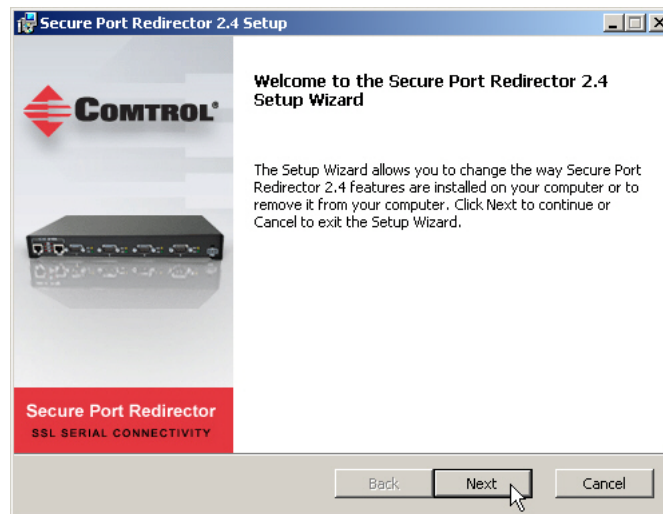
1. Locate the secure COM port redirector on the CD or download the latest version at: ftp://ftp.comtrol.com/dev_mstr/rts/redirector/windows.

Note: Although the ftp link displays rts in the path, the secure port redirector supports the DeviceMaster models discussed in this User Guide.

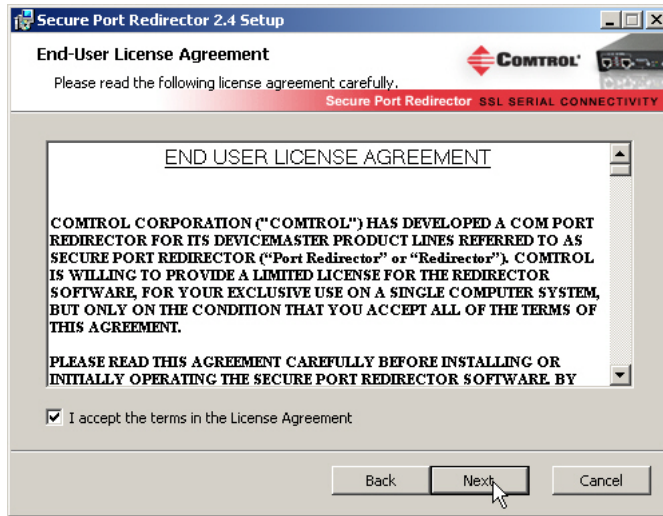
2. Double-click the **setup-spr.msi** file.
3. If prompted, click **Run**.



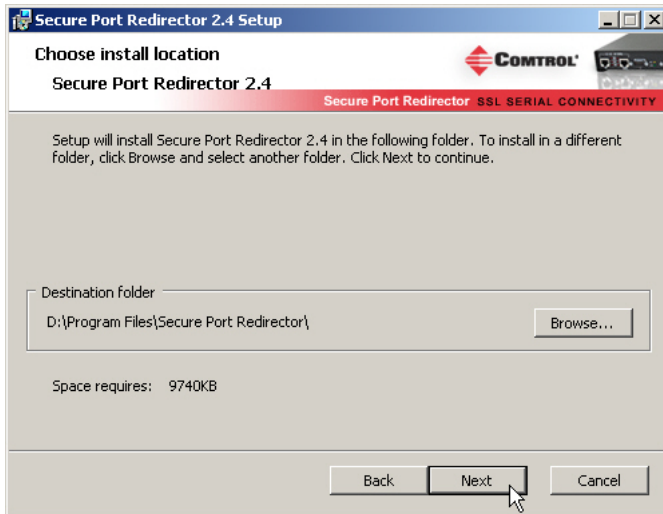
4. Click **Next** at the *Setup Wizard*.



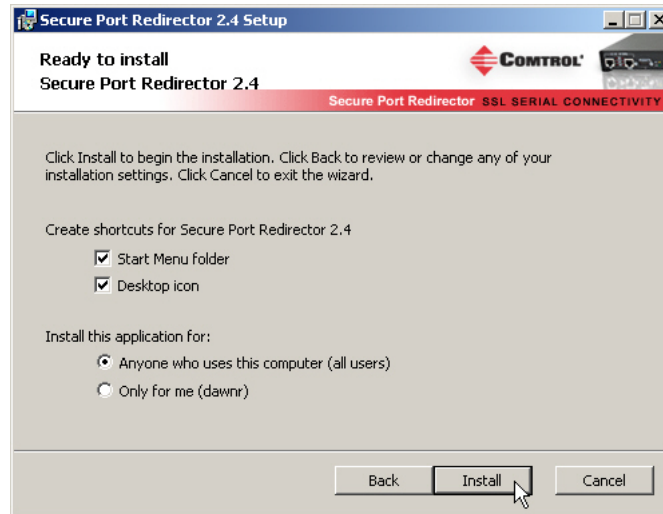
5. Click **I accept the terms in the License Agreement** and **Next**



6. Optionally, browse and select a different installation path, and then click **Next**



7. Verify the installation selections and then click **Install**



8. Click **Finish** to complete the installation and open the secure port redirector.



9. Configure the port with the secure port redirector using the next subsection.

Configuring Secure Redirector COM Ports

Use the following procedures to:

- Add a DeviceMaster port
- Configure the port for the secure port redirector

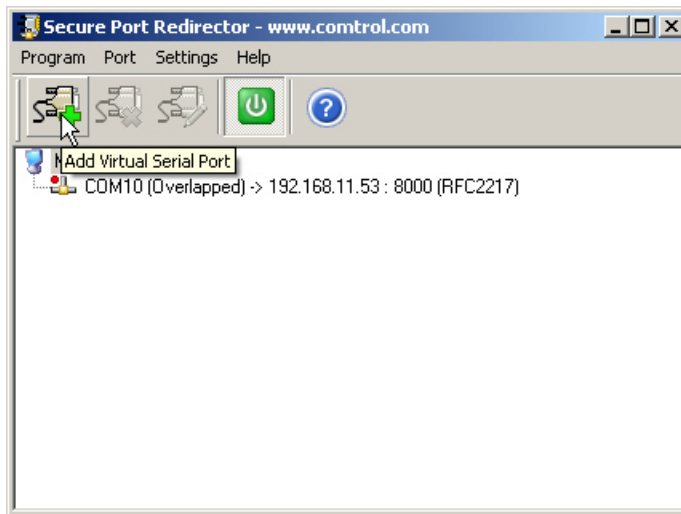
If necessary, refer to the secure port redirector help system for more information.

Adding a Secure Port

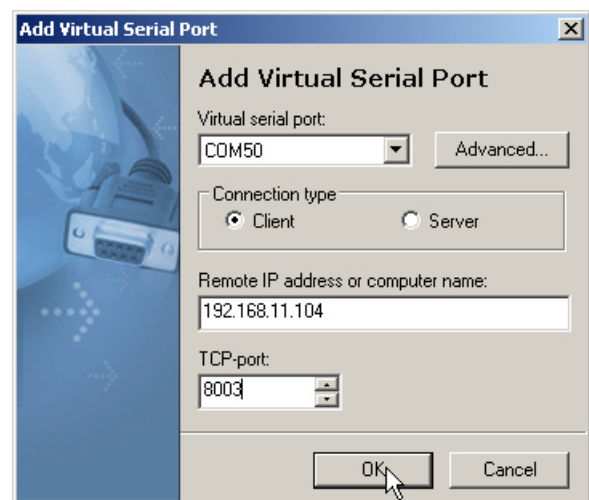
Use the following procedure to add a secure port or ports.

Note: You must have enabled the security feature in SocketServer and have the IP address and TCP port numbers and enabled the TCP Connection for each port before performing the following procedure.

1. If necessary, open the *Secure Port Redirector*; click **Start > Programs > Secure Port Redirector > Secure Port Redirector**.
2. Click **Port** and **Add**.



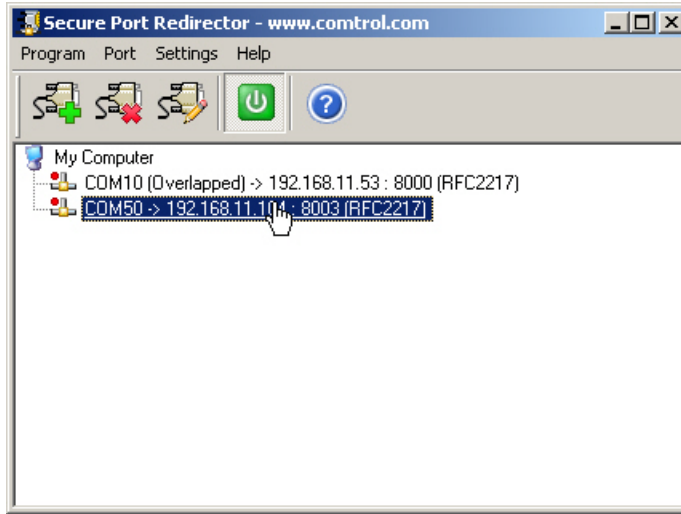
3. Select an available COM port in the *Virtual serial port* drop list
4. Click **Client** or **Server** depending on the COM port requirements.
5. Enter the Remote IP address of the DeviceMaster.
6. Enter the TCP port number for which you want to communicate on the DeviceMaster.
7. Click **Ok**.
8. Repeat [Step 2](#) for each port that you want to use as a secure COM port.



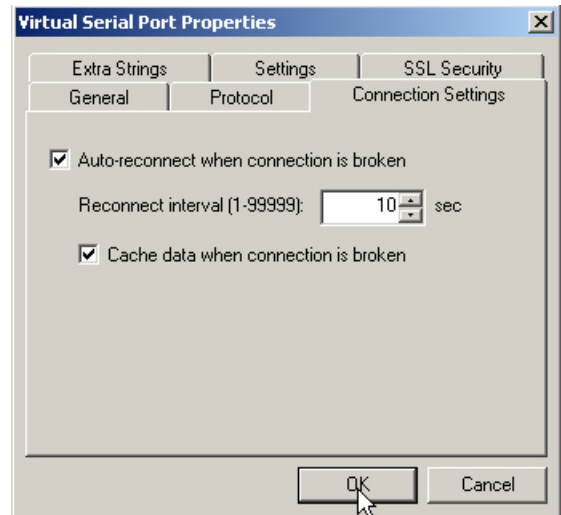
Configuring the Secure COM Port

Use the following procedure to configure the port.

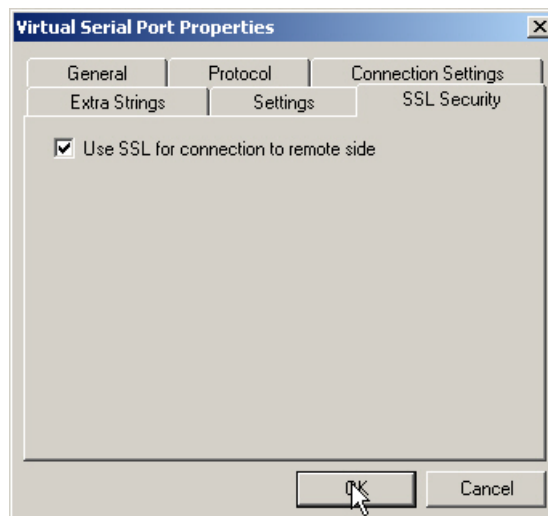
1. Double-click the port that you want to configure.



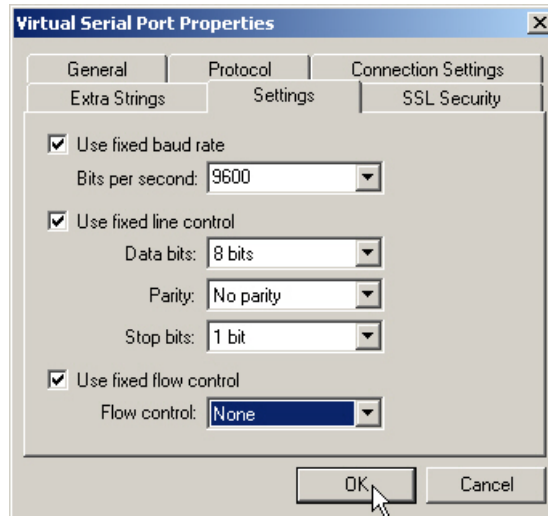
2. Optionally click the *Connection Settings* tab, click **Auto-reconnect when connection is broken**, set the **Reconnect interval**, set **Cache data when the connection is broken**, and then **Ok**.



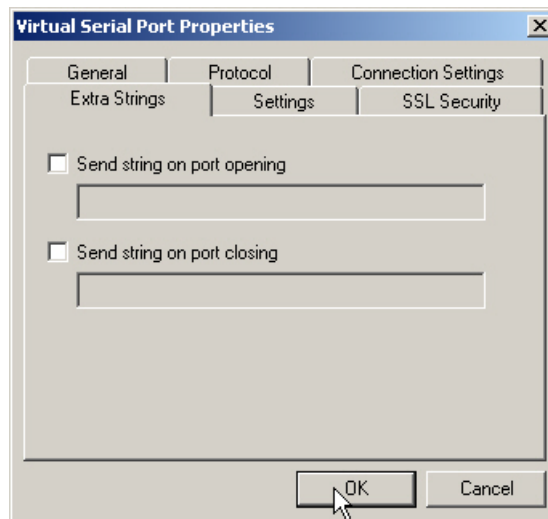
3. Click the *SSL Security* tab and then click **Use SSL for connection to remote side**.



- Click the *Settings* tab and select the appropriate serial port settings.



- Optionally, click the *Extra Strings* tab and enter the appropriate values.



- Click **OK** to save the settings for the DeviceMaster.
- Repeat the above procedure for each port that you want to use as a secure COM port.
- Close the Secure Port Redirector window when you are done.

You are now ready to connect the serial devices to the DeviceMaster ports. If necessary, refer to [Connecting Serial Devices on Page 99](#) for cabling information.

Socket Port Configuration

This section provides an overview of SocketServer and provides basic operating procedures. SocketServer and DeviceMaster security are discussed in detail in [DeviceMaster Security](#) on Page 75.

Note: *Technical Supports recommends that you update to the latest version of SocketServer before installing an NS-Link device driver, the secure COM port redirector, 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 pre-installed on your DeviceMaster. When you install an [NS-Link device driver](#), an NS-Link version of SocketServer loads on the DeviceMaster.

The home SocketServer web page (*Server Configuration*) provides access to configure:

- Socket port characteristics for:
 - Serial
 - TCP connection
 - UDP connection

See [SocketServer Architecture](#) on Page 72 for more information about socket port support

- Network settings (after initial configuration)
- [Security](#), which is discussed in detail starting on Page 75
- Email notification services
- RFC1006 (ISO over TCP)

Note: *For socket service configuration procedures or detailed information each field, 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 [SocketServer Architecture](#) on Page 72.

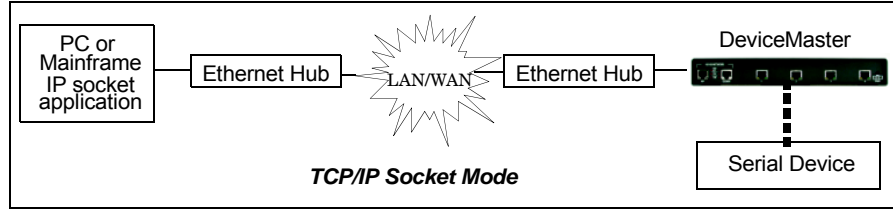
The *Help* system for the web page is available on the CD on the *Supporting Documents* page for your DeviceMaster or you can download the latest version from: ftp://ftp.comtrol.com/dev_mstr/rts/software/socketserver/help/ssvr_help.zip.

To use the help system:

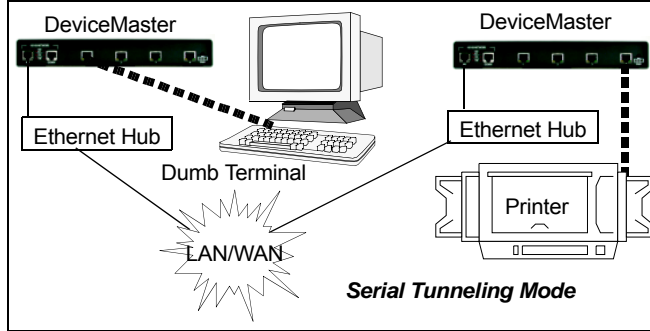
1. Unzip the files in a folder.
2. Open the **ssvr_help.htm** file.
3. Use your browser find function to locate the option or information for which are searching.

SocketServer Architecture

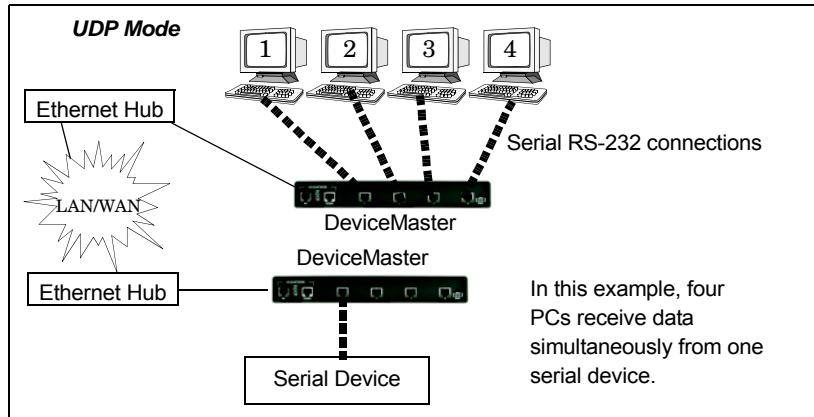
TCP/IP socket mode operation is used to connect serial devices with an application that supports TCP/IP socket communications addressing.



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 acknowledgements to the sender.



Accessing Socket Configuration

There are several ways to access the socket configuration pages (either version, SocketServer or NS-Link). Use the method that fits your environment best.

- *Web Browser*
- *PortVision Plus*

Web Browser

To access the socket configuration page for the DeviceMaster using a web browser, 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 the IP address in PortVision Plus.*
3. Click the port number that you want to configure socket port settings (serial, TCP connection configuration, and UDP connection configuration).

Note: *See the web page Help system, if you need information about configuring sockets or serial tunneling. The Help system provides detailed configuration procedures and descriptions for all fields. See [Web Page Help System](#) on Page 71 for information about downloading the help file separately.*

4. Click **Save** to return to the *Server Configuration* page.
5. Optionally, access the following pages to configure additional settings.
 - a. Click **Configure Network** to change the network settings.
 - b. Click **Configure Security** to enable DeviceMaster security.
 - c. Click the **Configure Email Messages** to configure email notification services.
 - d. Click the **Configure RFC1006 (ISO over TCP)** to configure RFC1006 settings.

PortVision Plus

There are several ways to access the socket configuration (NS-Link or SocketServer) page for the DeviceMaster using PortVision Plus.

1. If necessary, start PortVision Plus, right-click the DeviceMaster that you want to configure, and click **Web Manager**.
2. Click the port for which you want to configure socket port settings (serial, TCP connection configuration, and UDP connection configuration).
Note: *For socket configuration information see the Help system. Click the ? in a configuration area for field specific information or the Help button at the bottom of the page to view page level help. To locate configuration procedures, scroll to the top of the Help file and view the Table of Contents.*
3. Click **Save** to return to the *Server Configuration* page.
4. Optionally, access the following pages to configure additional settings.
 - e. Click **Configure Network** to change the network settings.
 - f. Click **Configure Security** to enable DeviceMaster security.
 - g. Click the **Configure Email Messages** to configure email notification services.
 - h. Click the **Configure RFC1006 (ISO over TCP)** to configure RFC1006 settings.

SocketServer Versions

The [SocketServer Overview](#) 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.



Server Configuration ?

Software:	SocketServer 8.00
IP Config:	Static
IP Address:	192.168.11.30
IP Netmask:	255.255.0.0
IP Gateway:	192.168.11.1
Configure Network	
Configure Security	
Configure Email Messages	
Configure RFC1006 (ISO over TCP)	

[Port 1](#)

[Port 2](#)

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



Server Configuration ?

Software:	NS-Link 8.00
IP Config:	Static
IP Address:	192.168.11.20
IP Netmask:	255.255.0.0
IP Gateway:	192.168.11.1
Configure Network	
Configure Security	
Configure Email Messages	
Configure RFC1006 (ISO over TCP)	

[Port 1](#)

[Port 2](#)

[Port 3](#)

[Port 4](#)

[Port 5](#)

[Port 6](#)

[P](#)

DeviceMaster Security

This subsection provides a basic understanding of the DeviceMaster security options, and the repercussions of setting these options. See [Removing DeviceMaster Security Features](#) on Page 174 if you need to reset DeviceMaster security options. See [Returning the DeviceMaster to Factory Defaults](#) on Page 176 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
CA (Client Authentication certificate) †	<p>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.</p> <p>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.</p> <p>See Key and Certificate Management on Page 91 for more information. This section does not discuss the creation of CA Certificates.</p>
Client Authentication	<p>A process using paired keys and identity certificates to prevent unauthorized access to the DeviceMaster. Client authentication is discussed in Client Authentication on Page 84 and Changing Keys and Certificates on Page 94.</p>
DH Key Pair Used by SSL Servers †	<p>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.</p> <p>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.</p> <p>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 man in the middle attacks. 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.</p> <p>See Certificates and Keys on Page 84 and Key and Certificate Management on Page 91 for more information.</p>
<p>† All DeviceMaster units are shipped from the factory with identical configurations. They all have the identical, self-signed, Control Server RSA Certificates, Server RSA Keys, Server DH Keys, and no Client Authentication Certificates. For maximum data and access security, you should configure all DeviceMaster units with custom certificates and keys.</p>	

Term or Issue	Explanation
Digital Certificate	<p>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.</p> <p>See Key and Certificate Management on Page 91 for more information.</p>
PKI (public key infrastructure)	<p>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.</p> <p>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.)</p> <p>A public key infrastructure consists of:</p> <ul style="list-style-type: none"> • 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 <p>For more information, see SSL Authentication on Page 83, SSL Performance on Page 85, SSL Cipher Suites on Page 85, and DeviceMaster Supported Cipher Suites on Page 86.</p>

Term or Issue	Explanation
RSA Key Pair†	<p>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.</p> <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> - One half of the <i>key pair</i> used in conjunction with a public key - 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. <p>Thus, if <i>User A</i> sends <i>User B</i> a message, <i>User A</i> can find out <i>User B's</i> public key (but not <i>User B's</i> private key) from a central administrator and encrypt a message to <i>User B</i> using <i>User B's</i> public key. When <i>User B</i> receives it, <i>User B</i> decrypts it with <i>User B's</i> private key. In addition to encrypting messages (which ensures privacy), <i>User B</i> can authenticate <i>User B</i> to <i>User A</i> (so that <i>User A</i> knows that it is really <i>User B</i> who sent the message) by using <i>User B's</i> private key to encrypt a digital certificate.</p> <p>See Key and Certificate Management on Page 91 for more information.</p>
SSH (Secure Shell)	<p>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 password is empty.</p> <p>See SSH Server on Page 82 for more information.</p>
SSL (Secure Sockets Layer)	<p>The Secure Sockets Layer (SSL) is the predecessor of (TLS) Transport Layer Security.</p> <p>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.</p> <p>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.</p> <p>SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.</p> <p>See Pages 83 through 86 for detailed information about SSL.</p> <p>Note: <i>Two slightly different SSL protocols are supported by the DeviceMaster: SSLv3 and TLSv1.</i></p>
<p>† All DeviceMaster units are shipped from the factory with identical configurations. They all have the identical, self-signed, Control Server RSA Certificates, Server RSA Keys, Server DH Keys, and no Client Authentication Certificates. For maximum data and access security, you should configure all DeviceMaster units with custom certificates and keys.</p>	

Term or Issue	Explanation
<p>TLS (Transport Layer Security)</p>	<p>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).</p> <p>TLS and SSL are not interoperable. The TLS protocol does contain a mechanism that allows TLS implementation to back down to SSL 3.0.</p>
<p>Secure Data Mode</p>	<p>TCP connections that carry data to/from the DeviceMaster serial ports are encrypted using SSL or TLS security protocols. See Security Modes on Page 81 and Configure/Enable Security Features on Page 87 for more information.</p>
<p>Secure Config Mode</p>	<p>Unencrypted access to administrative and diagnostic functions are disabled. See Security Modes on Page 81 and Configure/Enable Security Features on Page 87 for more information.</p>
<p>Secure Monitor Data Mode via Telnet</p>	<p>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 89.</p>
<p><i>Man in the Middle attack</i></p>	<p>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.</p> <p>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.</p>
<p><i>How Public and Private Key Cryptography Works</i></p>	<p>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).</p> <p>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.</p> <p>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).</p> <p>Thus, if <i>User A</i> sends <i>User B</i> a message, <i>User A</i> can find out <i>User B's</i> public key (but not <i>User B's</i> private key) from a central administrator and encrypt a message to <i>User B</i> using <i>User B's</i> public key. When <i>User B</i> receives it, <i>User B</i> decrypts it with <i>User B's</i> private key. In addition to encrypting messages (which ensures privacy), <i>User B</i> can authenticate <i>User B</i> to <i>User A</i> (so <i>User A</i> knows that it is really <i>User B</i> who sent the message) by using <i>User B's</i> private key to encrypt a digital certificate. When <i>User A</i> receives it, <i>User A</i> can use <i>User B's</i> public key to decrypt it.</p>

Term or Issue	Explanation
Who Provides the Infrastructure?	<p>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:</p> <ul style="list-style-type: none"> • RSA, which has developed the main algorithms used by PKI vendors. • Verisign, which acts as a certificate authority and sells software that allows a company to create its own certificate authorities. • 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.
<p>The following topic references are from: http://searchsecurity.techtarget.com/</p> <ul style="list-style-type: none"> • PKI (public key infrastructure) • How Public/Private Key Cryptography Works • Who Provides the Infrastructure • Digital Certificate • DH Key • Man in the Middle attack <p>The RSA Key pair topic reference is from: http://en.wikipedia.org/wiki/RSA</p>	

PortVision Plus Considerations When Setting Security

The following list provides basic PortVision Plus operations that affect security:

- PortVision Plus must scan the DeviceMaster *BEFORE* configuring security
- PortVision Plus must be aware of the DeviceMaster before setting either **Secure Data Mode** or **Secure Config Mode**.
- If PortVision Plus discovers the DeviceMaster *AFTER* setting security, the following conditions occur:
 - The IP address of the DeviceMaster does not display.
 - The *Configure Device* tabs are not present
 - The IP mode displays as DHCP without the ability to modify.
 - The **Upload** and **Reboot** icons on the *Launch Bar* are grayed out

TCP and UDP Socket Ports Used by the DeviceMaster

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

Socket Port Number	Description
22 SSH 23 Telnet	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 may be disabled.
80 HTTP 443 SSL or HTTPS	TCP Ports 80 (http) and 443 (https) are used by the web server for administration 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 Plus if you want to update firmware without setting up a TFTP server and this port cannot be disabled.
4607	TCP Port 4607 is only used for diagnostic purposes and isn't required for normal operation and this port cannot be disabled. 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. 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.

DeviceMaster Security Features

The following subsections provide information about DeviceMaster security features.

Security Modes

The DeviceMaster supports two security modes.

Security Mode	Description
Secure Data	SSL encryption for serial port data streams for both NS-Link and SocketServer. Secure Data mode: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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 RedBoot and SocketServer/NS-Link applications.

Secure Data Mode and Secure Config Mode Comparison

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

	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

	Secure Data	Secure Config	Secure Data/Secure Config
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

DeviceMaster Security Feature Comparison

This table displays addition information about security feature comparisons.

Supported by:	Weakest			Strongest		
	0	1	2	3	3	4
	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 †	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
Secure Port Redirector	yes	yes	yes	yes	yes	yes
Email	yes	yes	yes	disabled	disabled	disabled
SNMP	yes	yes	yes	disabled	disabled	disabled
RFC1006	yes	yes	yes	disabled	disabled	disabled

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

† admin commands 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 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 *man-in-the-middle* attacks on the communications channel.
- Two slightly different SSL protocols are supported by the DeviceMaster, SSLv3 and TLSv1.
- The DeviceMaster uses third-party MatrixSSL library from PeerSec Networks: <http://www.peersec.com/matrixssl.html>.

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, port redirectors, 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 **openssl** 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 **openssl** 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 also significant. The time required to open a connection to SocketServer varies depending on the public-key encryption scheme used for the initial handshaking. Typical setup times for the three public-key encryption schemes supported by the DeviceMaster are shown below:
 - 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 blocks 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
- 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
 - 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
 - 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
 - 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 attached 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: <http://en.wikipedia.org/wiki/TLS>
- **openssl** contains command-line tools to do the following. More information is available at: <http://www.openssl.org/>
 - 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: <http://www.rtfm.com/ssldump/>.
 - 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)

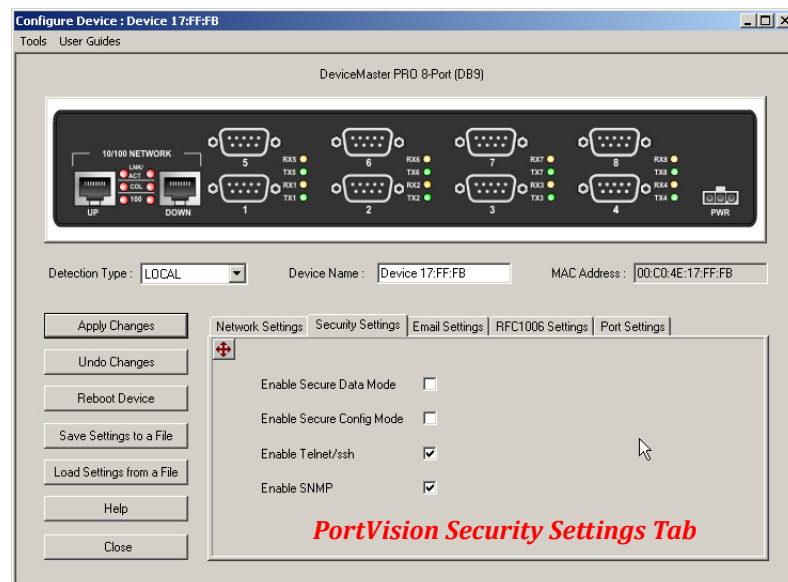
Configure/Enable Security Features

You can enable DeviceMaster security features using PortVision Plus or the web page (SocketServer or the NS-Link version).

Key and Certificate Management must be done using the *Edit Security Configuration* web pages of the DeviceMaster

PortVision Plus

DeviceMaster security features may be enabled in either the web page of the DeviceMaster or by using PortVision Plus. These options are based on selecting the appropriate check boxes.



For a descriptions of how the options work, see the table on Page 88.

Web Page - Security Configuration Area

The options in the *Edit Security Configuration* area are discussed in the following table.



Edit Security Configuration Default Screen

Security Option	Description
<p>Enable Secure Data Mode</p>	<p>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:</p> <ul style="list-style-type: none"> • TCP connections to the per-serial-port TCP ports (default is 8000, 8001, 8002, and so forth) are encrypted using SSL/TLS. • TCP connections to TCP Port 4606 on which the DeviceMaster implements the Control proprietary serial driver protocol are encrypted using SSL/TLS. • Since SSL/TLS can not be used for either UDP data streams or for the Control 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. <p>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 Client Authentication discussion on Page 84 for details.</p>

Security Option	Description
Enable Secure Config Mode	<p>If Secure Config Mode is enabled, unencrypted access to administrative and diagnostic functions is disabled. Secure Config Mode changes DeviceMaster behavior as follows:</p> <ul style="list-style-type: none"> • 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. • Encrypted access to the web server via Port 443 (https://URLs) is still allowed. • Administrative commands that change configuration or operating state which are received using the Control proprietary TCP driver protocol on TCP Port 4606 are ignored. • Administrative commands that change configuration or operating state that are received using the Control MAC mode proprietary Ethernet protocol number 0x11FE are ignored.
Enable Monitoring Secure Data via Telnet	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • monitor [-ac] portnumber <p>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).</p> <p style="text-align: right;"><i>(continued)</i></p>

Security Option	Description
<p>(Continued from the previous page)</p> <p>Enable Monitoring Secure Data via Telnet</p>	<p>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 Example 1 on Page 90 for more information.</p> <ul style="list-style-type: none"> - The -a option enables displaying of ASCII representation of data in a column to the right the hex representation. See Example 2 on Page 90. - 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 Example 3 on Page 91. <ul style="list-style-type: none"> • 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. Currently, because of issues with the DeviceMaster ssh implementation, monitoring serial port data via the ssh command-line interface is not supported. It is expected that it will be supported in the future. Once it is supported, the securemon setting will not affect the ability to monitor secure data via ssh (which will always be allowed).
<p>Enable Telnet/ssh</p>	<p>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></p>
<p>Enable SNMP</p>	<p>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></p>

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
```

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
> 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

```

```

< abcABC123
> abcABC123
< abcABC123
> abcABC123
< 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:

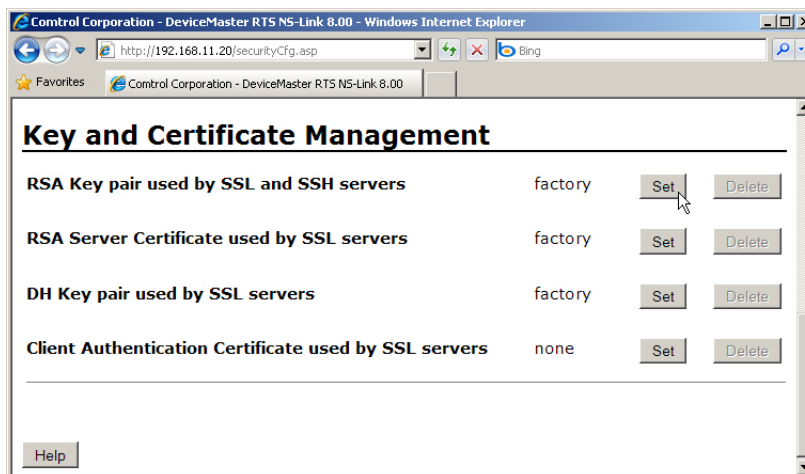
```

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 *Edit Security Configuration* web page.



Key and Certificate Management Options	Description
RSA Key pair used by SSL and SSH servers	<p>This is a private/public key pair that is used for two purposes:</p> <p>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.</p> <p>It is used to sign the Server RSA Certificate in order to verify that the &dm; is authorized to use the server RSA identity certificate. Possession of the private portion of this key pair allows somebody to pose as the &dm;.</p> <p>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.</p>
RSA Server Certificate used by SSL servers	<p>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.</p> <p>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.</p>
DH Key pair used by SSL servers	<p>This is a private/public key pair that is used by some cipher suites to encrypt the SSL/TLS handshaking messages.</p> <p>Note: <i>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.</i></p>
Client Authentication Certificate used by SSL servers	<p>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.</p> <p>See Client Authorization for more detailed information</p>
<ul style="list-style-type: none"> • <i>All DeviceMaster units are shipped from the factory with identical configurations. They all have the identical, self-signed, Control Server RSA Certificates, Server RSA Keys, Server DH Keys, and no Client Authentication Certificates.</i> • <i>For maximum data and access security, you should configure all DeviceMaster units with custom certificates and keys.</i> 	

Using a Web Browser to Set Security Features

The follow procedures are discussed below:

- [Changing Security Configuration](#)
- [Changing Keys and Certificates](#) on Page 94

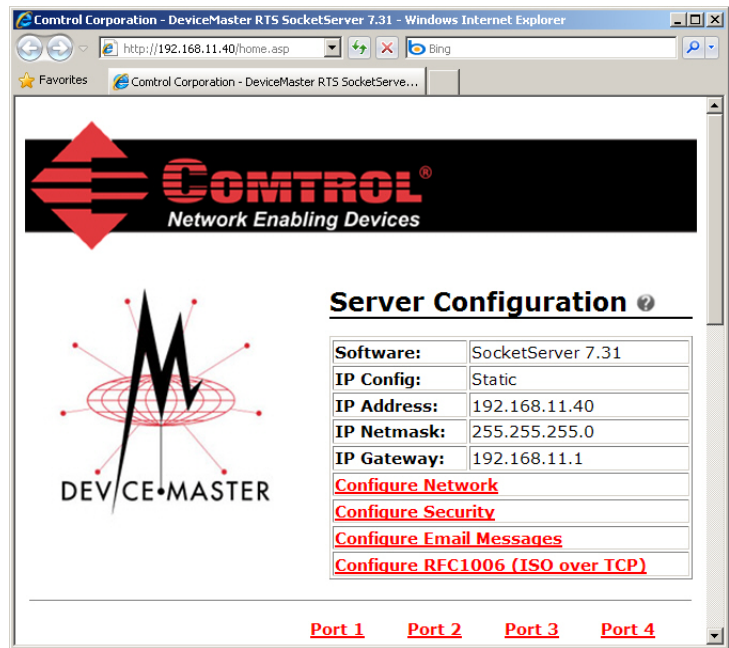
Changing Security Configuration

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 the **Configure Security** link.
3. Click the appropriate check boxes in the *Edit Security Configuration* area to enable or disable security accordingly.

Refer to the help system or [Web Page - Security Configuration Area](#) on Page 88 for detailed information.

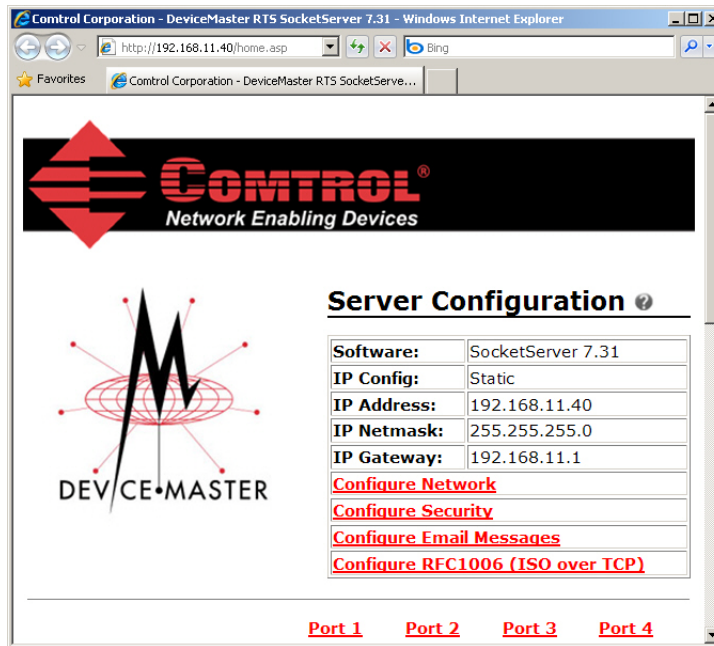
4. After making changes to the *Edit Security Configuration* area, you must click **Save** and then **OK**.



Changing Keys and Certificates

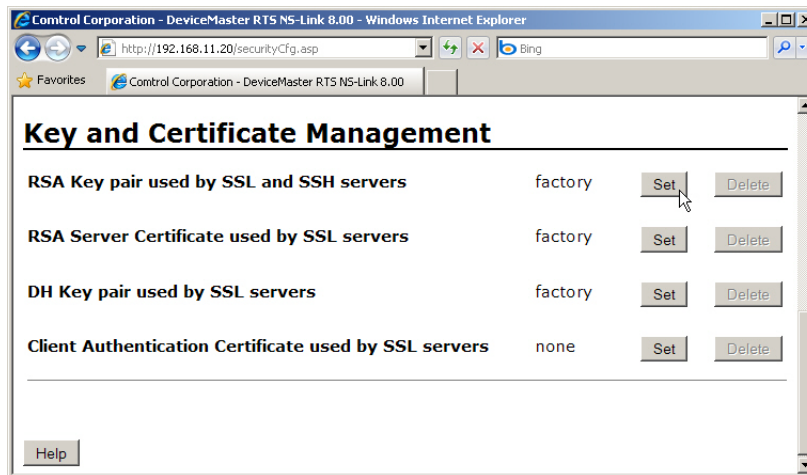
Use the following steps to update security keys and certificates in the DeviceMaster.

1. Enter the IP address of the DeviceMaster in the *Address* field of your web browser and press the **Enter** key.
2. Click the **Configure Security** link.



3. Click **Set** for the appropriate key or certificate option in the *Keys and Certificate Management* area to configure security keys and certificates.

Refer to the help system or [Key and Certificate Management](#) subsection on Page 94 for detailed information.



4. Click **Browse** to locate the key or certificate file, highlight the file, and click **Open**.
5. Click **Upload** when you return to the *Key and Certificate Management* area.
The key or certificate notation changes from *factory* or *none* to **User** when the DeviceMaster is secure.
6. You do not need to click **Save**, but changes will not take effect until the DeviceMaster is rebooted.

Modbus Server Application Overview

The Modbus Server application was designed to provide enhanced connectivity for OPC servers and applications that require Modbus/RTU communications. While standard gateways provide connectivity for only one application per serial port, Modbus Server provides connectivity for up to six applications per serial port.

Modbus Server greatly enhances system maintenance capabilities. Included are comprehensive device and port specific diagnostic web pages that display status, message response timing, timeout, and other error counts, and overall message statistics. A serial log is also included to provide message level diagnosis.

See the *Modbus Server User Guide* for information about configuring or using Modbus Server on the Software and Documentation CD or from ftp://ftp.comtrol.com/dev_mstr/rts/software/modbus_server/docs.

Recommended Chassis

The following table lists the recommended DeviceMaster RTS or DeviceMaster UP chassis based on Modbus/RTU message throughput.

Throughput	1 Port	2 Ports	4 Ports	8 Ports	16 Ports	32 Ports
Very High - Message rate of up to one message every 50 ms per port (20 messages per port per second)	X	X				
High - Message rate of up to one message every 100 ms per port (10 messages per port per second)	X	X	X			
Medium - Message rate of up to one message every 200 ms per port (5 messages per port per second)	X	X	X	X		
Low - Message rate of up to one message every 500 ms per port (2 messages per port per second)	X	X	X	X	X	
Very Low - Message rate of up to one message every second per port (1 message per port per second)	X	X	X	X	X	X
Latency						
Transmit (From application to device)	2-10 ms (*)		5-20 ms (*)		0-30 ms (*)	
Receive (From device to application)	2-10 ms (*)		5-20 ms (*)	5-50 ms	10-100 ms	
(*) = Based on one Ethernet TCP/IP connection per serial port running in a normal uncongested system. The maximum overall latency will increase as the number of Ethernet TCP/IP connections increase.						

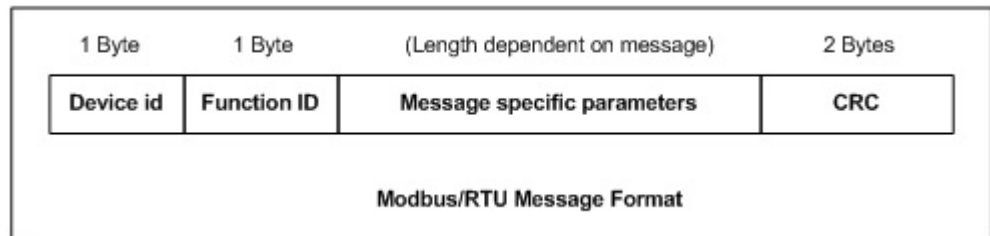
Note: These estimates are based on a Modbus/RTU request and/or response message size

of 20 bytes. Actual throughput will vary depending on message size and system requirements.

What is Modbus?

Modbus/RTU (Supported by Modbus Server)

Modbus/RTU is native Modbus in hexadecimal format. These are the base Modbus messages that contain simple read and write requests. The format is as follows:



Where:

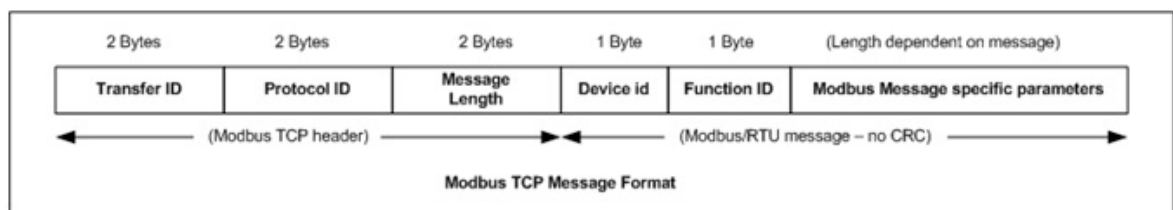
- The terms Master or Client are used to identify the sender of the message.
- The terms Slave or Server are used to identify the devices responding to the message.

Modbus/RTU is used for:

- Serial port connectivity. RS-485 is the most common, but RS-232 and RS-422 are also used.
- Ethernet TCP/IP socket connections. This is not the same as Modbus/TCP (please see next section), but does provide a very simple method of interfacing to remote devices. It is used by many applications and some OPC servers. Note: This communication method is not used by PLCs.

Modbus/TCP (Not supported by Modbus Server)

Modbus/TCP is an Ethernet network based protocol that contains a Modbus/RTU message, with the exception of the 2 byte CRC. The Modbus/TCP message contains a header with information designed to provide message identification and routing information. The format is as follows:



Where:

- The terms Master or Client are used to identify the sender of the message.
- The terms Slave or Server are used to identify the devices responding to the message.
- Modbus/TCP messages are typically sent to and received on a defined Ethernet TCP/IP socket of 502.
- Modbus/TCP implementations provide more capability, but also require more processing than simpler Modbus/RTU implementations.

Modbus/TCP is used for connecting advanced Ethernet based devices, such as PLCs, HMIs, SCADA Systems, and most OPC Servers to:

- Other Ethernet devices supporting Modbus/TCP.
- Remote serial Modbus/RTU devices through gateways (such as the DeviceMaster UP).

- Remote serial or Ethernet TCP/IP ASCII devices through a gateway (such as the DeviceMaster UP).

Note: Refer to the DeviceMaster UP for Modbus/TCP functionality.

Modbus Server Functionality

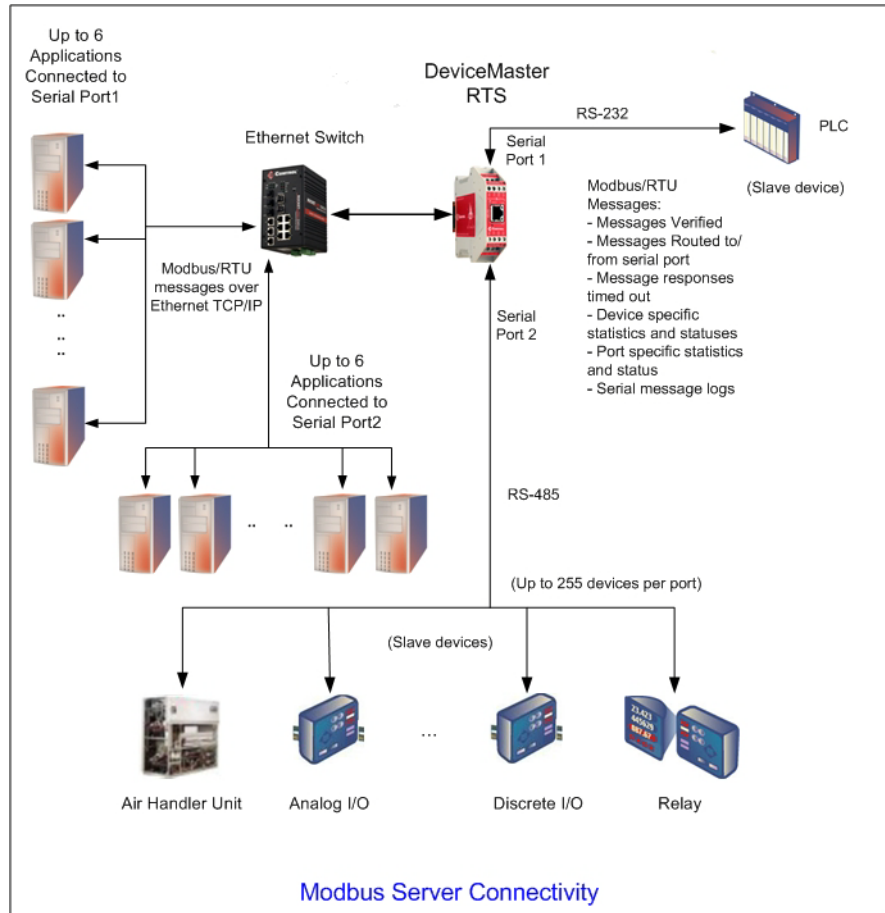
The Modbus Server application provides the following functionality:

- Supports Modbus/RTU over Ethernet TCP/IP connections to the corresponding serial port through intelligent Modbus message handling and routing.
- Supports only Modbus/RTU over Ethernet TCP/IP connections to a serial port.

Note: For Modbus/TCP functionality, see the [DeviceMaster UP](#).

- Supports up to six Ethernet TCP/IP connections to each serial port
 - One TCP/IP connection can be created with the *Connect To* connection method.
 - The *Listen* connection method accepts up to five or six connections, depending if the *Connect To* connection is active.
- Supports up to 255 Modbus devices per port. Both valid, (1-247), and reserved, (248-255), device Ids are supported.
- Modbus/RTU specific message handling:
 - CRC verification of all messages received on the TCP/IP and serial interfaces.
 - Timing out of responses from slave Modbus/RTU devices.
 - Broadcast message handling on connected port only.
- System monitoring to ensure gateway operation:
 - Gateway busy.
 - Application message time-outs.
- Advanced diagnostics web pages:
 - Modbus/RTU device specific statistics and status. Up to 255 Modbus/RTU devices per port can be monitored simultaneously.
 - Serial port specific statistics, response timing, and status.
 - Serial port message logging.

- Combined with a serial port redirector, such as the Control Secure Port Redirector, can support up to six COM port connections to each serial port.



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.

Use the appropriate procedure to connect asynchronous serial devices to the DeviceMaster ports.

- [DB9 and RJ45 Connectors](#)
- [Serial Terminals \(4\) - 1E](#) on Page 104
- [Serial Terminals \(8\) - 2E](#) on Page 107

Note: Go to [Building the Serial Ribbon Cable](#) on Page 18 for connector information for the DeviceMaster 1-Port Embedded adapter.



Make sure that you have configured the ports using the NS-Link driver or SocketServer 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.

DB9 and RJ45 Connectors

You can use this information to connect serial devices to DB9 and RJ45 connectors.

1. Connect your serial devices to the appropriate serial port on the DeviceMaster using the appropriate cable. You can build your own DB9 or RJ45 cables using the appropriate discussion:

- [DB9 Connectors](#) on Page 99
- [RJ45 Connectors](#) on Page 102

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

2. Verify that the devices are communicating properly.
 - The amber Rx LEDs on the ports show that the port is connected to another RS-232 device or receiving data in RS-422/485 mode.
 - The green Tx LED on the ports show that the data is transmitting.

Note: The port LED activity on the RTS 16/32RM may be inconsistent until the port has been opened. After a port is opened the LED activity works as documented.

3. Go to [DeviceMaster LEDs](#) on Page 172 for information about the remaining LEDs, which may provide information about the installation.



* Represents port number.



RJ45 LEDs



DB9 Connectors

You can build your own null-modem or straight-through DB9 serial cables using the

following subsections.

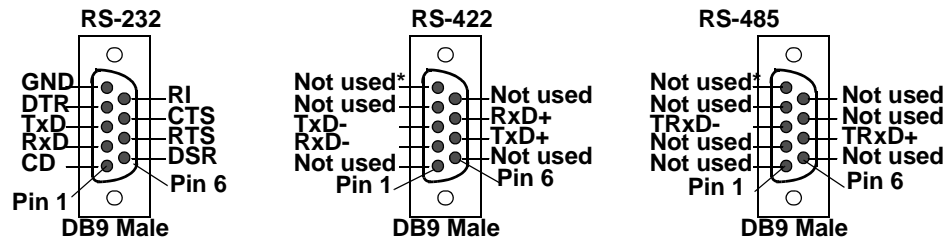
DB9 Connector Pinouts			
Pin	RS-232	RS-422 RS-485 Full-Duplex (Master/Slave)†	RS-485 Half-Duplex
1	DCD	Not used	Not used
2	RxD	RxD-	Not used
3	TxD	TxD-	TRxD-
4	DTR	Not used	Not used
5	GND	Not used††	Not used†
6	DSR	Not used	Not used
7	RTS	TxD+	TRxD+
8	CTS	RxD+	Not used
9	RI	Not used	Not Used

† Only 2-port models support RS-485 full-duplex.
 †† Pin 5 is tied to ground on the board, but is not used in the cable.

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

Refer to the hardware manufacturer’s installation documentation if you need help with connector pinouts or cabling for the serial device.

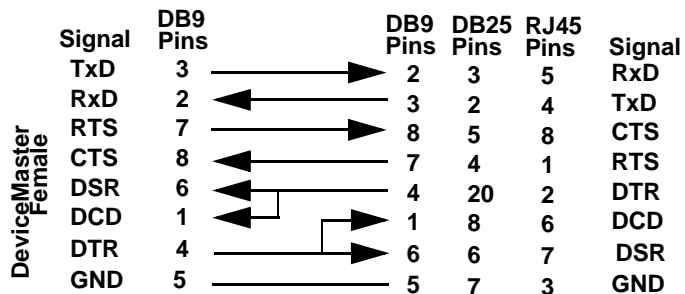
This illustrates the DB9 connector signals.



* Pin 5 is tied to ground on the board, but is not used in the cable.

DB9 Null-Modem Cables (RS-232)

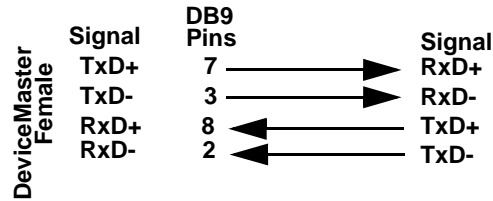
Use the following figure if you need to build an RS-232 null-modem cable. A null-modem cable is required for connecting DTE devices.



Note: You may want to purchase or build a straight-through cable and purchase a null-modem adapter. For example, a null-modem cable can be used to connect COM2 of one PC to COM2 of another PC.

DB9 Null-Modem Cables (RS-422)

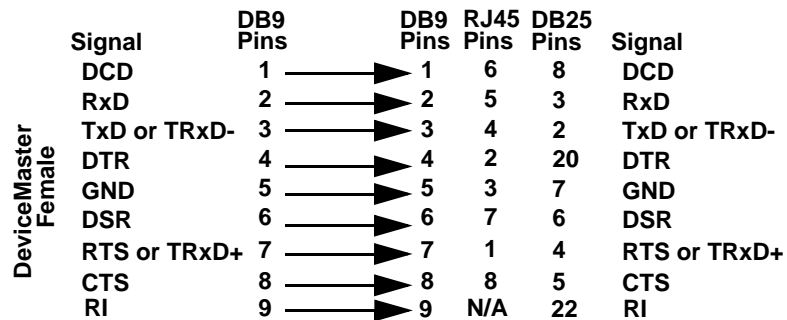
Use the following figure if you need to build an RS-422 null-modem cable.



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



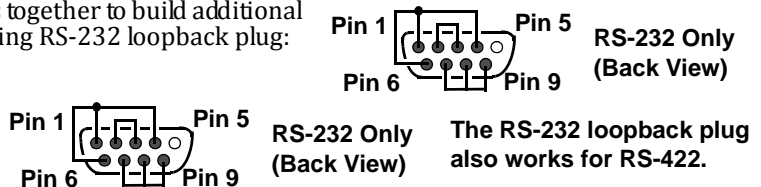
DB9 Loopback Plugs

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 single loopback plug (RS-232/422).

Note: You can use Test Terminal (Windows) or minicom (Linux) to test the serial ports, see [Testing Ports Using Test Terminal](#) on Page 160.

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



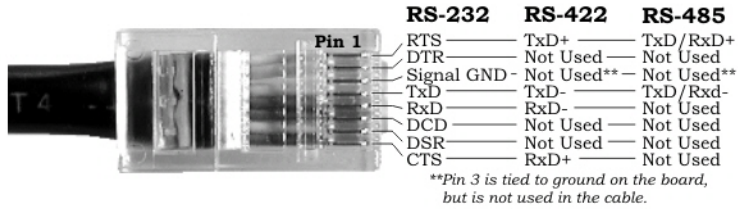
Wire the following pins together for an RS-422 loopback plug:

- Pins 2 to 3
- Pins 7 to 8



RJ45 Connectors

You can build your own null-modem or straight-through RJ45 serial cables using the following subsections.

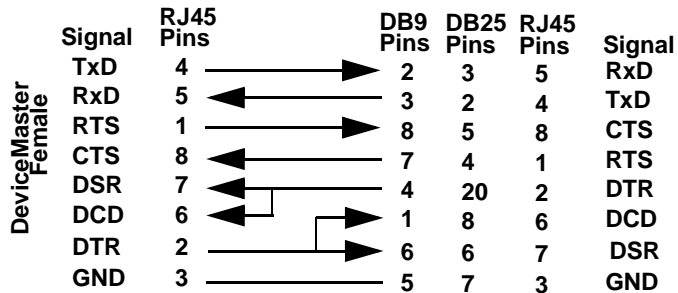


Pin	RS-232	RS-422	RS-485
1	RTS	TxD+	TRxD+
2	DTR	Not used	Not used
3	Signal GND	Not used†	Not used†
4	TxD	TxD-	TRxD-
5	RxD	RxD-	Not used
6	DCD	Not used	Not used
7	DSR	Not used	Not used
8	CTS	RxD+	Not used

† Pin 3 is tied to ground on the board, but is not used in the cable.

RJ45 Null-Modem Cables (RS-232)

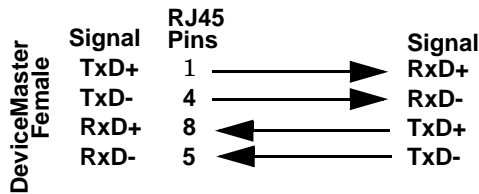
Use the following figure if you need to build an RS-232 null-modem cable. A null-modem cable is required for connecting DTE devices.



Note: You may want to purchase or build a straight-through cable and purchase a null-modem adapter. For example, a null-modem cable can be used to connect COM2 of one PC to COM2 of another PC.

RJ45 Null-Modem Cables (RS-422)

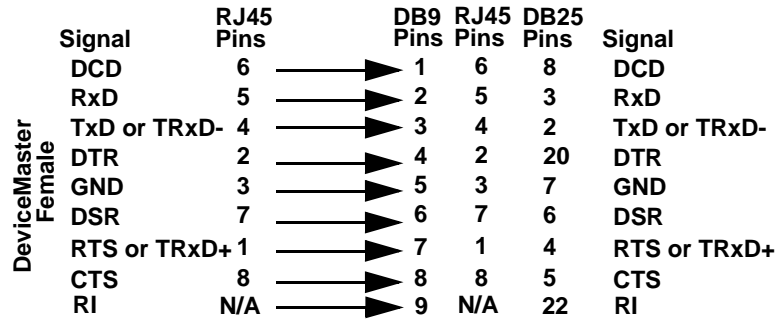
Use the following figure if you need to build an RS-422 null-modem RJ45 cable. A null-modem cable is required for connecting DTE devices.



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

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

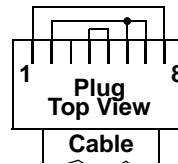
Use the following figure if you need to build an RS-232 or RS-485 straight-through cable. Straight-through cables are used to connect modems and other DCE devices. For example, a straight-through cable can be used to connect COM2 of one PC to COM2 to a modem.



RJ45 Loopback Plugs

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

- Pins 4 to 5
- Pins 1 to 8
- Pins 2 to 6 to 7

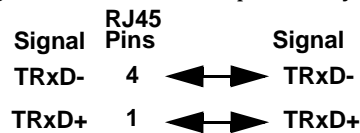


The RS-232 loopback plug also works for RS-422.

Note: You can use Test Terminal (Windows) or minicom (Linux) to test the serial ports, see [Testing Ports Using Test Terminal](#) on Page 160.

RJ45 RS-485 Test Cable

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



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

Serial Terminals (4) - 1E

Use the following information to connect the DeviceMaster 2-port 1E with serial terminals.

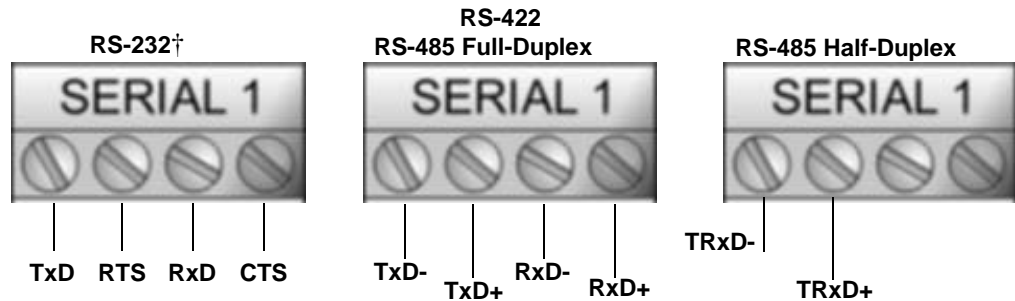
1. Connect your serial devices to the appropriate serial port on the DeviceMaster using the appropriate cable. You can build your own cables or loopbacks using the appropriate discussions.

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

2. Verify that the devices are communicating properly. Use the LED description table on Page 23 if you need information about the LEDs.

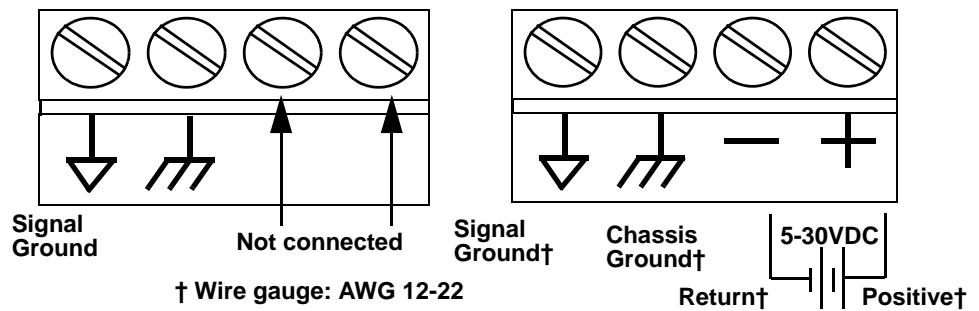
Serial Terminal (4) Connectors

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



† RS-232 ground must be connected to the appropriate signal ground terminal.

RS-232: Connecting the Ground



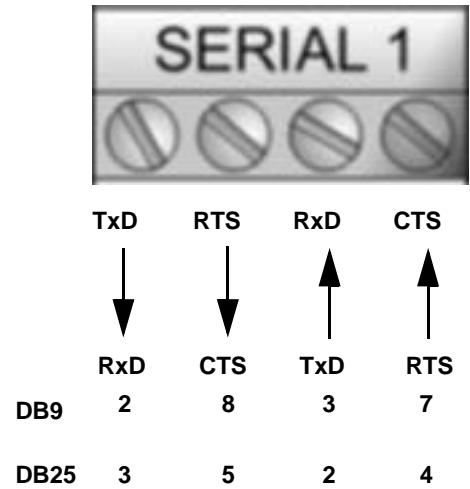
RS-232†	TxD	RTS	RxD	CTS
RS-422/RS-485 Full-Duplex	TxD-	TxD+	RxD-	RxD+
RS-485 Half-Duplex	TRxD-	TRxD+		

† RS-232 ground must be connected to the appropriate signal ground terminal.

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

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

RS-232 Null-Modem Cable

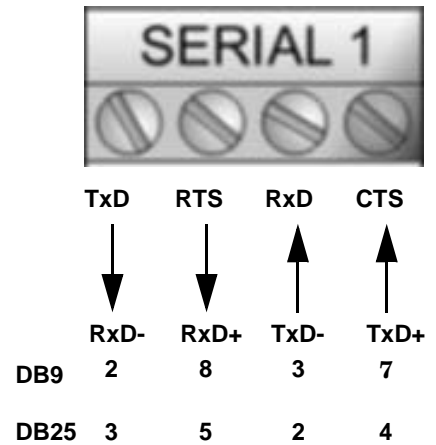


*Serial Terminal (4)
Null-Modem Cables
(RS-422)*

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

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

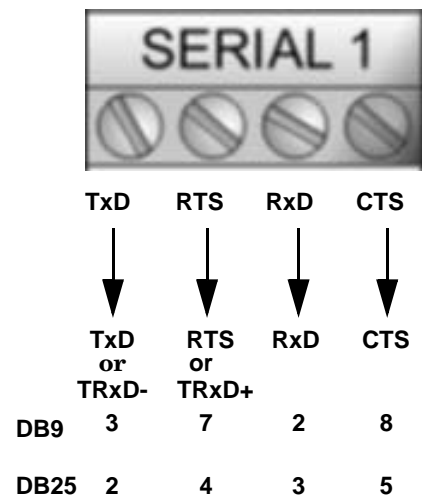
RS-422 Null-Modem Cable



*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



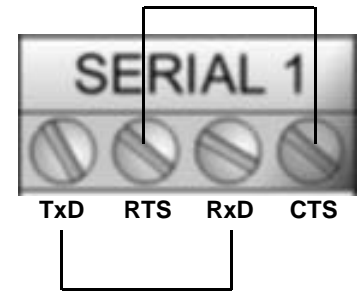
1E Loopback Signals

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

See [Testing Ports Using Test Terminal](#) on Page 160 to test the serial ports.

Wire the terminals together to create a loopback.

- TxD to RxD
- RTS to CTS



Serial Terminals (8) - 2E

Use the following information to connect the DeviceMaster 2-port 2E with serial terminals.

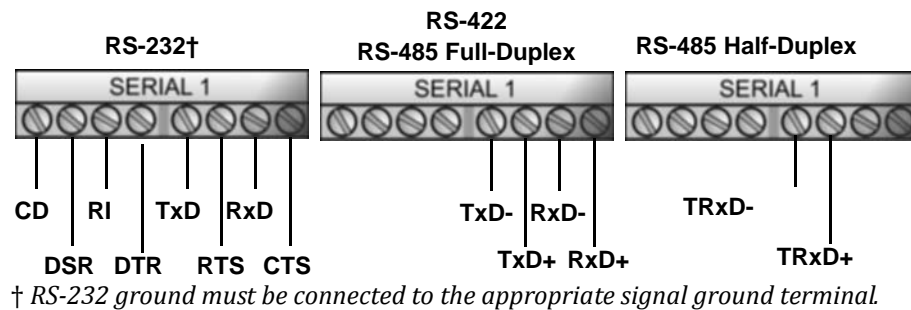
1. Connect your serial devices to the appropriate serial port on the DeviceMaster using the appropriate cable.

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

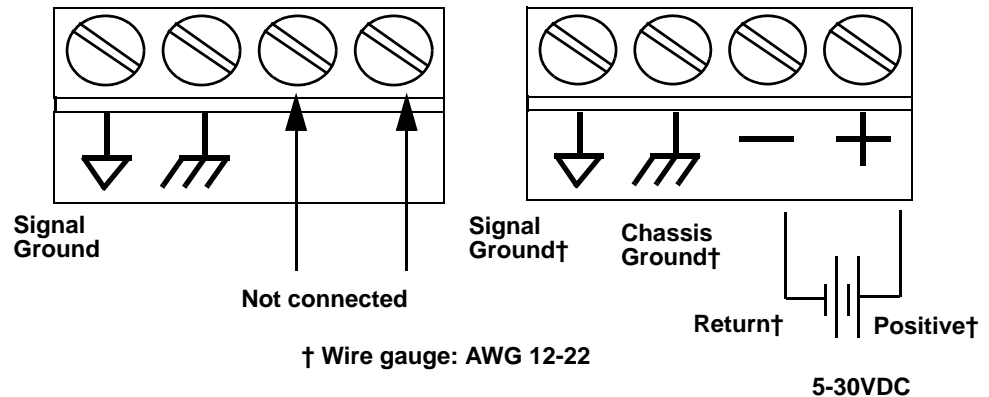
2. Verify that the devices are communicating properly. Use the LED description table on Page 23 if you need information about the LEDs.

Serial Terminal (8) Connectors

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



RS-232: Connecting the Ground

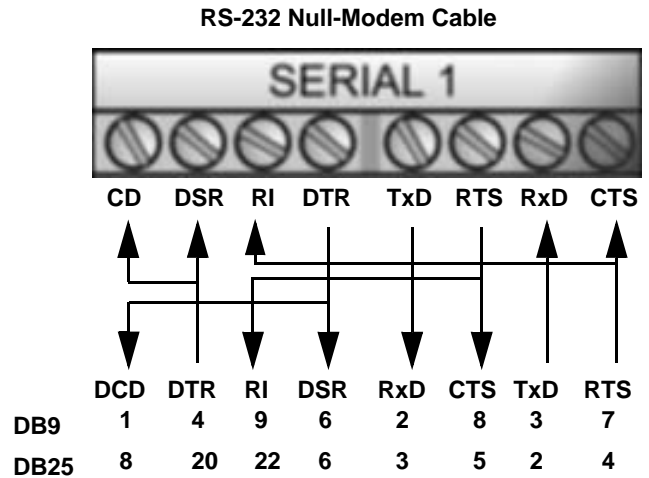


RS-232	CD	DSR	RI	DTR	TxD	RTS	RxD	CTS
RS-422/RS-485 Full-Duplex	N/A	N/A	N/A	N/A	TxD-	TxD+	RxD-	RxD+
RS-485 Half-Duplex	N/A	N/A	N/A	N/A	TRxD-	TRxD+	N/A	N/A

† RS-232 ground must be connected to the appropriate signal ground terminal.

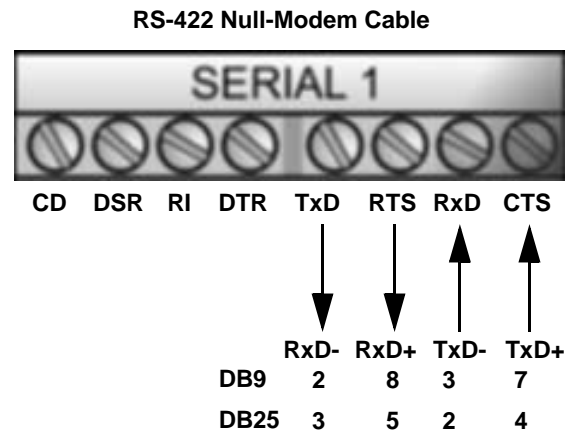
*Serial Terminal (8)
Null-Modem Cables
(RS-232)*

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



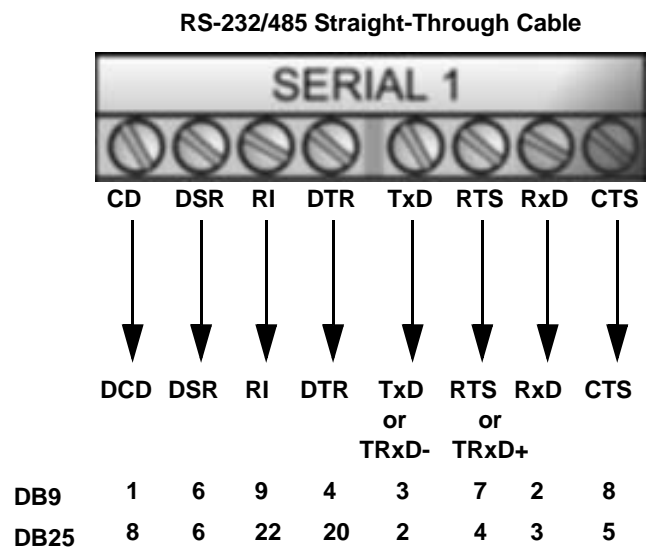
*Serial Terminal (8)
Null-Modem Cables
(RS-422)*

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



*Serial 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.

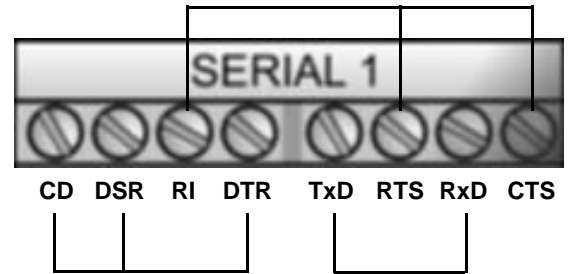


2E Loopback Signals

Use the drawing below to wire a loopback, which is used in conjunction with application software (Test Terminal or minicom) to test serial ports, see [Testing Ports Using Test Terminal](#) on Page 160.

Wire the terminals together to create a loopback.

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



Managing the DeviceMaster

This section discusses the following DeviceMaster maintenance procedures:

- [Rebooting the DeviceMaster](#)
- [Uploading SocketServer to Multiple DeviceMasters on Page 112](#)
- [Configuring Multiple DeviceMasters Network Addresses on Page 113](#)
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.
- [Adding a New Device on Page 114](#)
- [Using Configuration Files on Page 116](#)
- [Changing the Bootloader Timeout on Page 119](#), which discusses changing the Bootloader timeout
- [Managing Bootloader on Page 123](#), which also discusses checking the Bootloader version and downloading the latest Bootloader
- [Checking the NS-Link Version on Page 125](#)
- [Restoring Factory Defaults \(2-Port, Only\) on Page 127](#)
Note: You can optionally refer to [RedBoot Procedures on Page 129](#) if you want to perform procedures at the RedBoot level.

Rebooting the DeviceMaster

There are many ways to reboot the DeviceMaster. Use the method that most fits your situation.

Method	Procedure
PortVision Plus	<i>Main screen:</i> Right-click the DeviceMaster or DeviceMasters, click Reboot Device and then Yes . <i>Configure Device screen:</i> Click Reboot Device and then Yes . <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	<i>Main page (Server Configuration):</i> Scroll to the bottom of the page, click Reboot and then Yes: Reboot .
Telnet	Type reset .
DeviceMaster 2-Port Models	DeviceMaster 2-port models have a reset/restore switch. <ul style="list-style-type: none">• If the reset/restore switch is depressed for less than 2 seconds, DeviceMaster RTS 2-port models reboot• If the reset/restore switch is depressed for greater than approximately 5 seconds it restores the default password and network setting values.

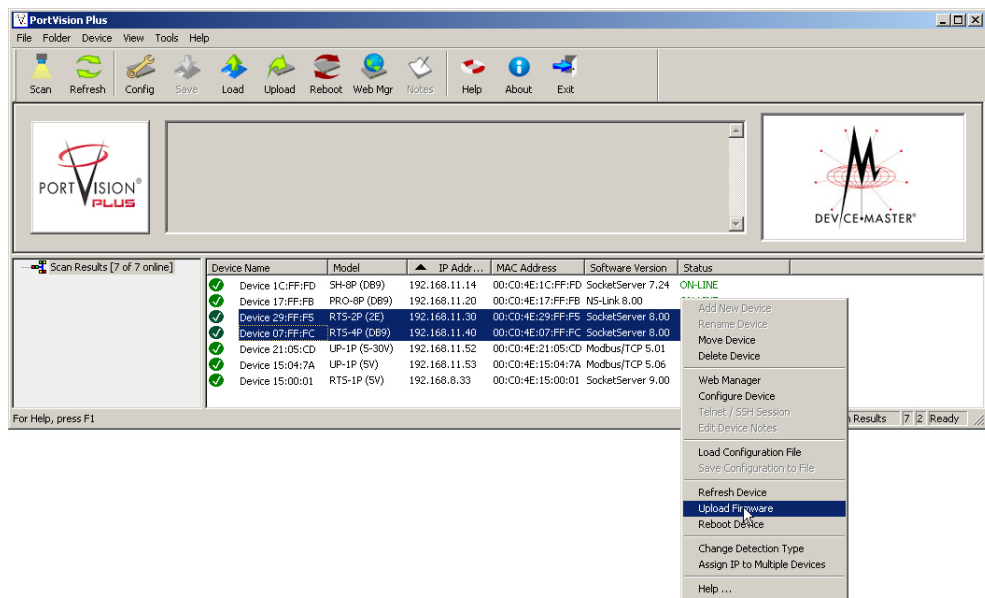
Optionally, you can power cycle the DeviceMaster.

Uploading SocketServer to Multiple DeviceMasters

If the Windows NS-Link driver 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 Plus ([Installing PortVision Plus 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 **Upload Firmware**.
 - Click **Upload Firmware** on the **Device** menu.



3. Browse, click the firmware (.bin) 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 device. The device will reboot 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 Plus will update the *List View* pane and display the new firmware version.

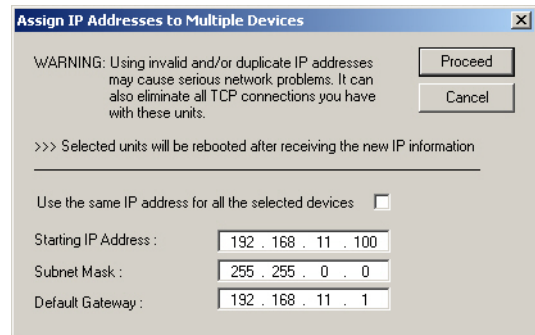
Configuring Multiple DeviceMasters Network Addresses

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 DeviceMasters and save the settings to a configuration file that you can load to all or selected DeviceMasters. See [Using Configuration Files on Page 116](#) 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 Plus ([Installing PortVision Plus on Page 35](#)) and **Scan** the network.
2. Shift-click the DeviceMasters for which you want to program network information, right-click, and click **Assign IP to Multiple Devices**.
3. Enter the starting IP address, subnet mask, IP Gateway and click **Proceed**.

PortVision Plus displays the programmed IP addresses in the *List View* 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.

>>> Selected units will be rebooted after receiving the new IP information

Use the same IP address for all the selected devices

Starting IP Address : 192 . 168 . 11 . 100

Subnet Mask : 255 . 255 . 0 . 0

Default Gateway : 192 . 168 . 11 . 1

Proceed Cancel

Adding a New Device

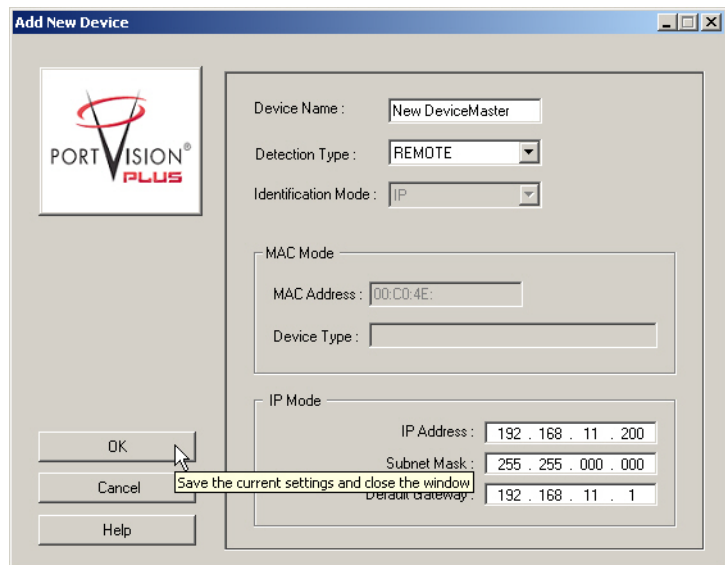
You can add a new DeviceMaster manually, if you do not want to scan the network to locate and add new DeviceMasters, but there may be cases where you want to use the *New Device* window to:

- Configure DeviceMaster units that are not on the local network (remote) using [Remote Using the IP Address on Page 114](#).
- Pre-configure a DeviceMaster in PortVision Plus (local) using [Local Using the IP Address or MAC Address on Page 115](#).

Remote Using the IP Address

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

1. Access the *New Device* window using one of these methods:
 - Click **Add New Device** on the *Device* menu.
 - Right-click in the *List View* 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. Enter a *Device Name* for the new DeviceMaster.
3. Select **REMOTE** for the *Detection Type*.
4. Enter the DeviceMaster IP address.
5. Click **Ok** to close the *Add New Device* window.
6. If necessary, click **Refresh** for the new DeviceMaster to display in the *List View* pane.



Local Using the IP Address or MAC Address

Use the following procedure to add a local DeviceMaster to PortVision Plus.

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** on the *Device* menu.
- Right-click in the *List View* 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. Enter a **Device Name** for the new DeviceMaster.
4. Select **LOCAL** for the *Detection Type*.
5. 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.

6. Click **Ok**.
7. If necessary, click **Refresh** for the new DeviceMaster to display in the *List View* pane.

Using Configuration Files

If you are deploying multiple DeviceMaster units that share common values, you can save the configuration file (.dmc) from the *Main* or *Configure Device* screens in PortVision Plus and load that configuration onto other DeviceMaster units.

If you save a configuration file from the *Main* or *Configure Device* screen, you can choose what properties you want saved or loaded.

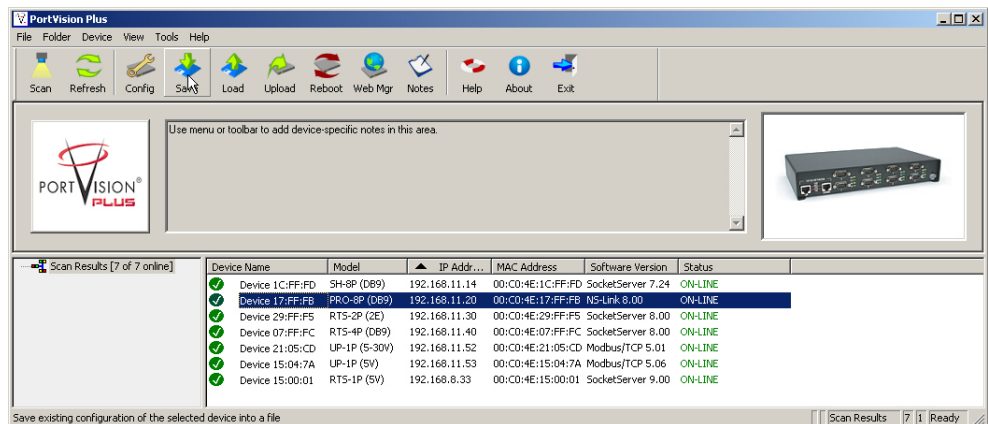
You may want to program the network settings in multiple DeviceMasters using [Configuring Multiple DeviceMasters Network Addresses on Page 113](#).

Saving a Configuration File

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

Note: *Optionally, you can save a configuration file by clicking the **Save Settings to a File** button on the Configure Device screen.*

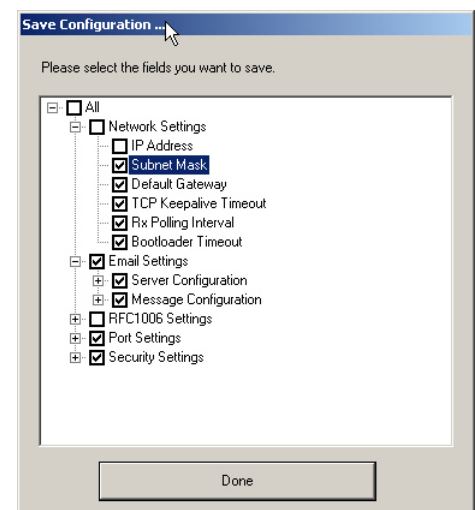
1. If you have not done so, install PortVision Plus ([Installing PortVision Plus on Page 35](#)) and **Scan** the network.
2. Highlight the DeviceMaster on the *Main* screen that you want to save its configuration and use one of the following methods:
 - Click the **Save** button.
 - Right-click and then click **Save Configuration to File**.



3. Browse to the location you want to save the file, enter a file name, and click **Save**.
4. Click the **All** checkbox or click only the properties that you want saved for each property page in the configuration file and click **Done**.

Note: *Selecting the **All** option with multiple DeviceMasters highlighted will apply the same IP address to all of the selected DeviceMasters.*

5. Click **Ok** to close the *Save Configuration Completed* message.



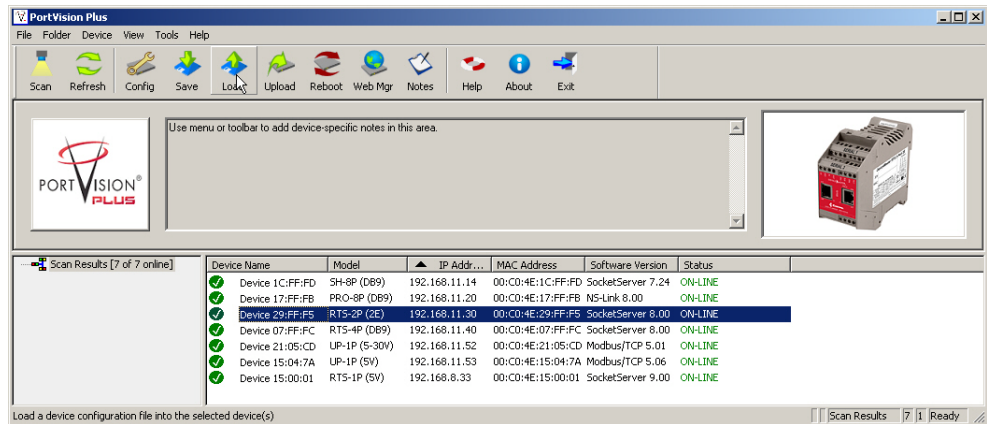
Loading a Configuration File

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* or *Configure Device* screen.

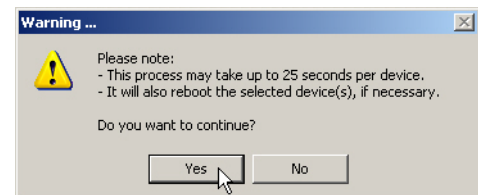
Use this procedure to load a configuration file using the *Main* screen to one or more DeviceMaster units.

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.*

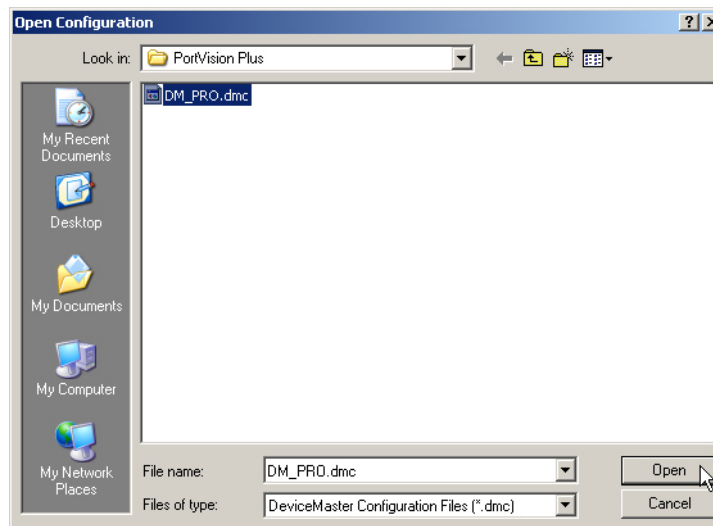
1. Highlight the device or devices on the *Main* screen that you want to load and use one of the following methods:
 - Click the **Load** button
 - Right-click and then click **Load Configuration to File**
 - Click **Load Configuration to File** on the *Device* menu



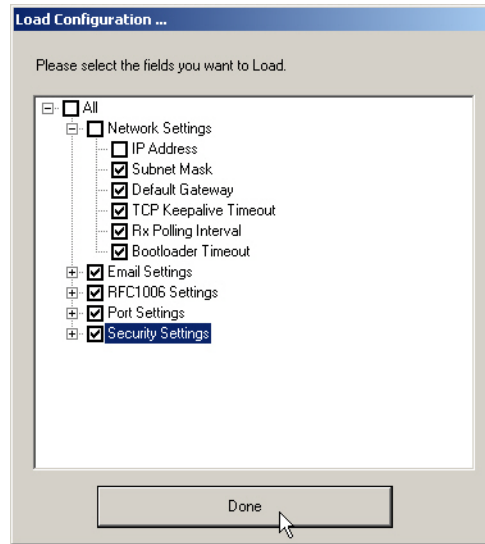
2. Click **Yes** to the warning that it will take 25 seconds per device and it may also reboot the devices.



3. Browse to the location of the configuration file, click the file name and then **Open**.

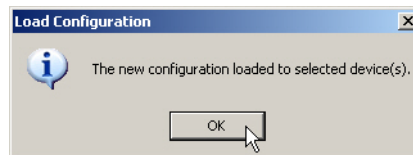


4. Click the **All** checkbox or click only the properties that you want to load for each property page in the configuration file and then click **Done**.



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

5. Close the *Load Configuration* popup message.



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 [Configuring the Network Settings on Page 36](#).*

You can use one of the following procedures to change the Bootloader Timeout value:

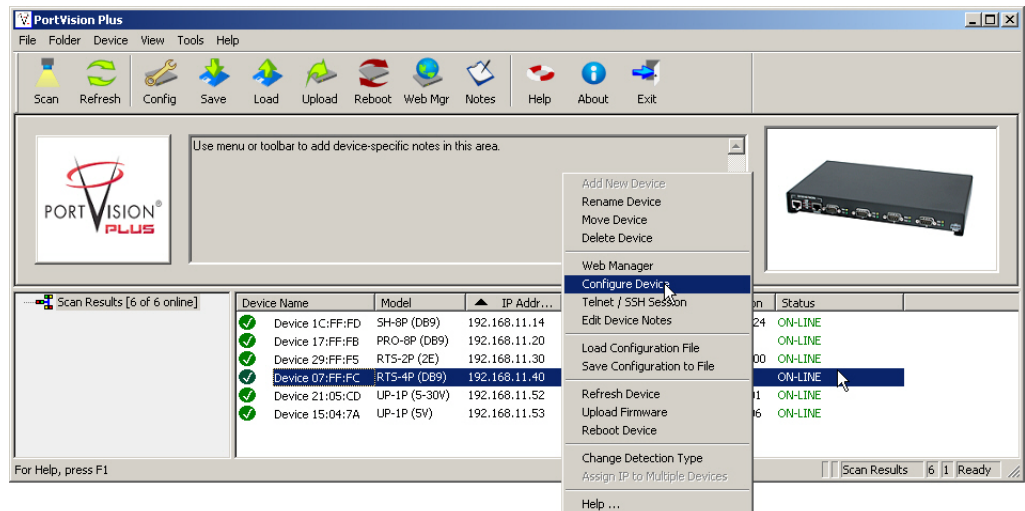
- [Configure Device Screen \(SocketServer v6.05 or Higher\)](#), which is the easiest method of changing the Bootloader timeout value.
- [Telnet/SSH Session \(SocketServer v6.04 and Below\) on Page 120](#)

Configure Device Screen (SocketServer v6.05 or Higher)

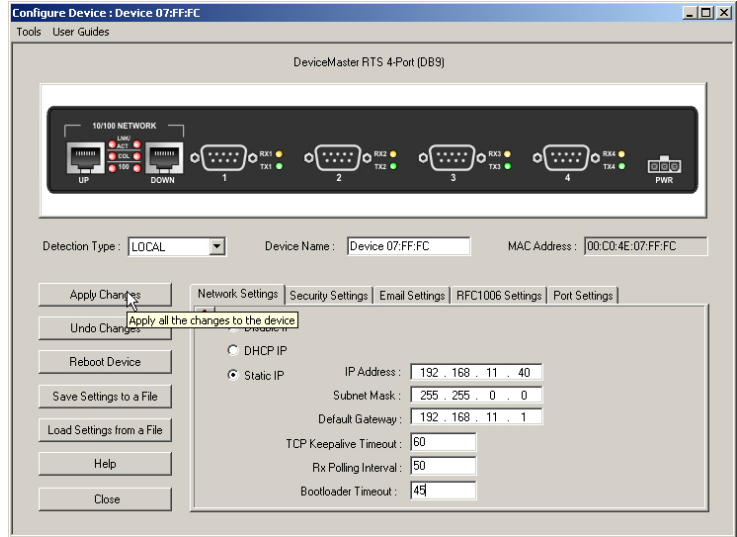
You must be using SocketServer v6.05 or higher and have loaded PortVision Plus 3.05 or higher for the following procedure to work.

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 Plus, from **Programs > Control > PortVision Plus > PortVision Plus**.
2. Right-click the DeviceMaster in the *View* pane and click **Configure Device**.



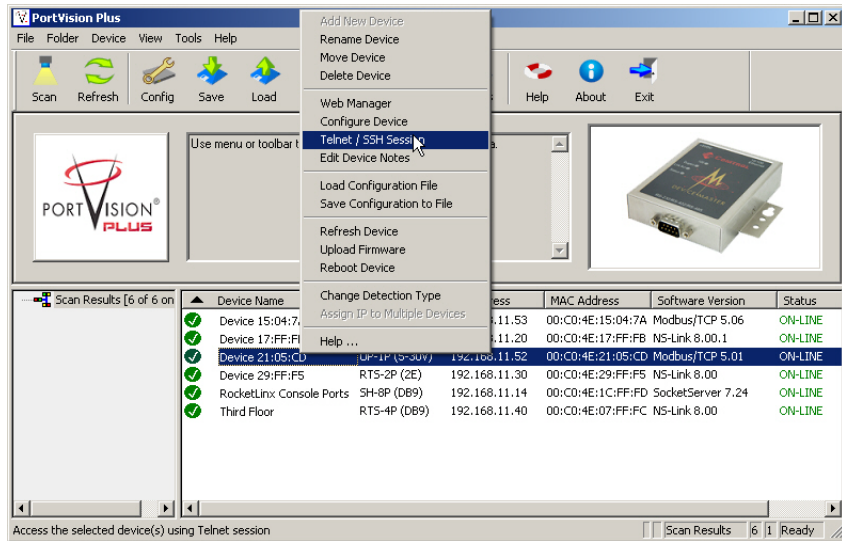
3. Type 45 in the **Bootloader Timeout** text box and click **Apply**.



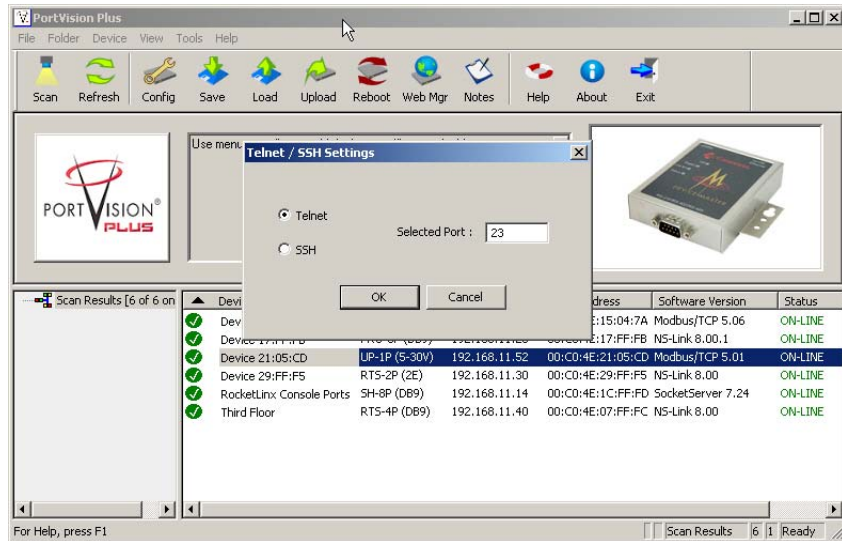
Telnet/SSH Session (SocketServer v6.04 and Below)

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.

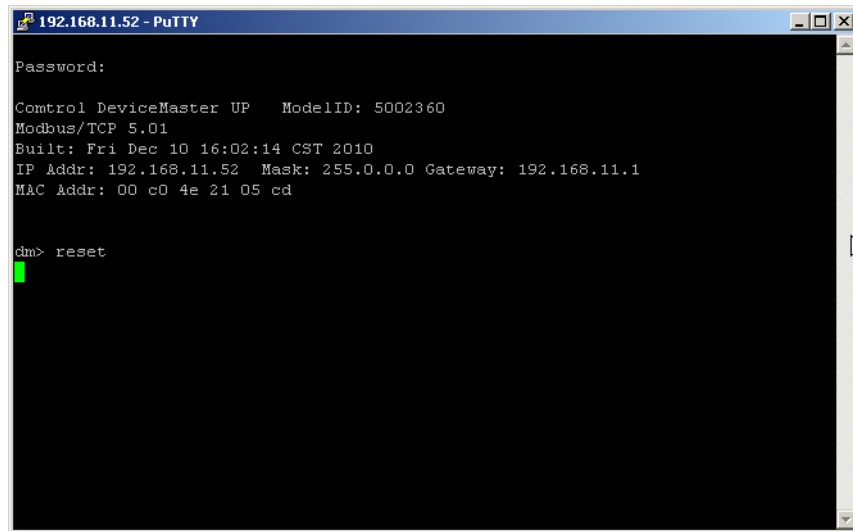
1. If necessary, start PortVision Plus, from **Start > Programs > Control > PortVision Plus > PortVision Plus**.
2. Right-click the DeviceMaster in the *View* pane and click **Telnet/SSH Session**.



- Click the **Telnet** radio button, leave **23** as the *Selected Port*, and click **Ok**.

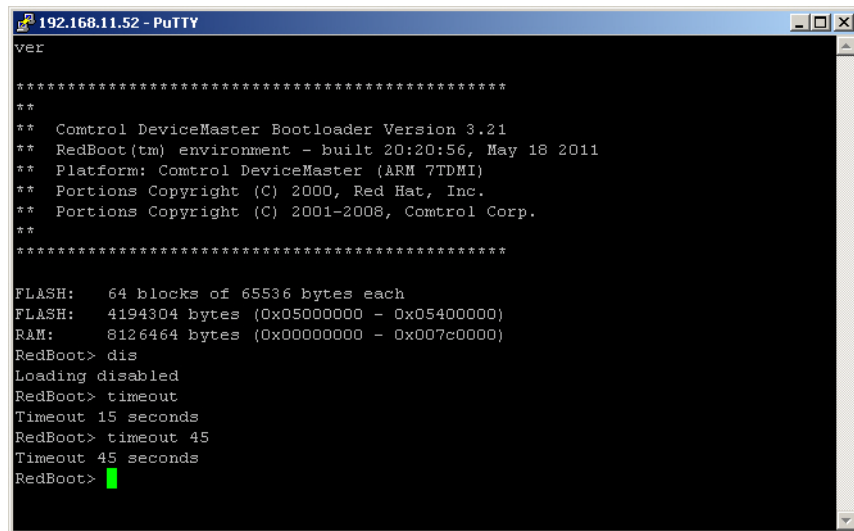


- If a password has been configured for the DeviceMaster, enter the password and press **Enter** or press **Enter** if no password has been configured.
- Type **reset** at the **dm>** prompt, press **Enter**, and close the window.



- Immediately** reopen the telnet window (Steps 2 and 3), and type **dis** at the RedBoot> prompt
- Type **timeout** and press **Enter** to determine the existing *timeout* value.

8. Type **timeout 45** and press **Enter** to set the *timeout* to 45 seconds.



```
192.168.11.52 - PuTTY
ver
*****
**
** Control DeviceMaster Bootloader Version 3.21
** RedBoot(tm) environment - built 20:20:56, May 18 2011
** Platform: Control DeviceMaster (ARM 7TDMI)
** Portions Copyright (C) 2000, Red Hat, Inc.
** Portions Copyright (C) 2001-2008, Comtrol Corp.
**
*****

FLASH: 64 blocks of 65536 bytes each
FLASH: 4194304 bytes (0x05000000 - 0x05400000)
RAM: 8126464 bytes (0x00000000 - 0x007c0000)
RedBoot> dis
Loading disabled
RedBoot> timeout
Timeout 15 seconds
RedBoot> timeout 45
Timeout 45 seconds
RedBoot> █
```

9. Type **reset**, press **Enter**, close the window, and try to upload SocketServer again.
10. If SocketServer loads correctly, you can use the above procedure to reset the Bootloader *timeout* back to it's default value of 15 seconds.

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 Control Technical Support.*

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

- **PortVision Plus** 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 [RedBoot Procedures on Page 129](#) for procedures.

Checking the Bootloader Version

The following procedure uses PortVision Plus to check the Bootloader version. Optionally, you can use RedBoot, see [Determining the Bootloader Version on Page 133](#).

1. If you have not done so, install PortVision Plus ([Installing PortVision Plus on Page 35](#)) and **Scan** the network.
2. Right-click the DeviceMaster and click **Reboot Device**.
3. Click **Yes** to the *Confirm Reboot* query.
4. Right-click the DeviceMaster, click **Refresh Device** as many times as necessary to catch the reboot cycle in the *List View* pane. The Bootloader version is briefly displayed during the reboot cycle before [SocketServer](#) loads.
5. Check the Control web site to see if a [later version](#) is available.
6. Go to the next subsection to 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 Control Technical Support

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 Control so that it can be reflashed.

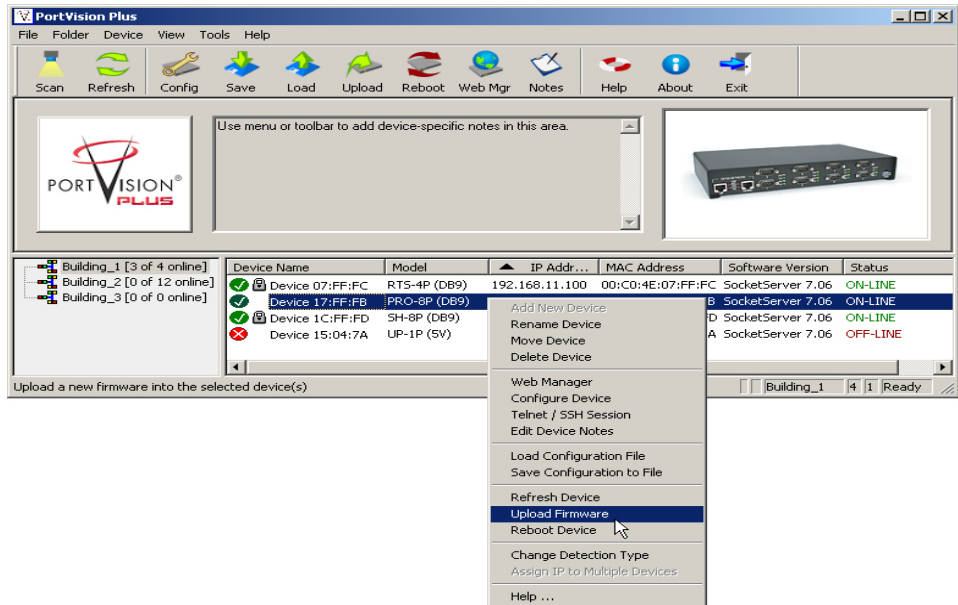
If you are not successful uploading SocketServer into the DeviceMaster, do not upload Bootloader.



If the NS-Link driver for Windows 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 Plus ([Installing PortVision Plus 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 **Upload Firmware**, browse to the Bootloader **.bin** file, and then click **Open**.

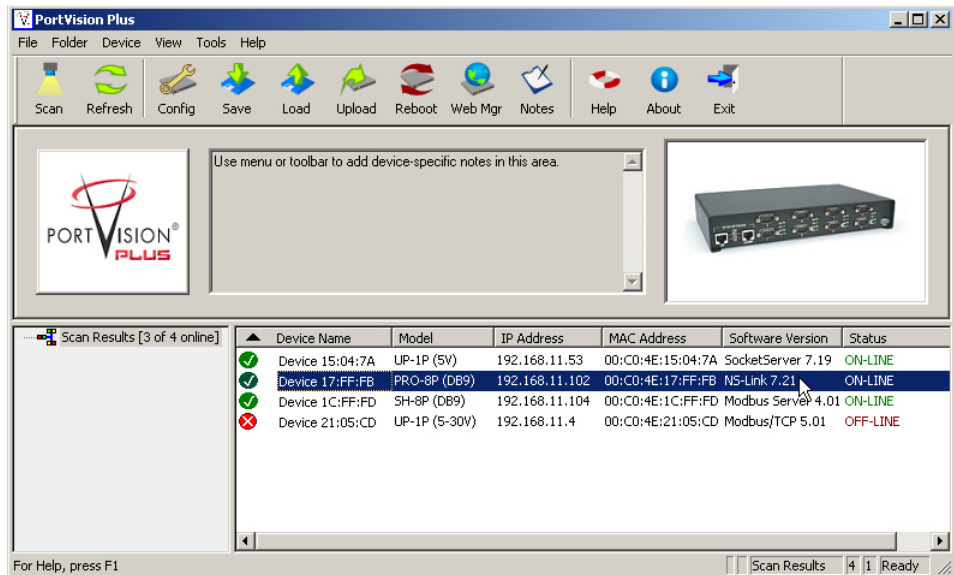


4. Click **Yes** to the *Upload Firmware* message that warns you that this is a sensitive process.
5. Click **Ok** to the second *Upload Firmware* message and then click **Refresh** until the Bootloader version displays in the *List View* pane, which should show the new version.

Checking the NS-Link Version

Use this procedure to check the NS-Link web page version.

1. Start PortVision Plus.
2. If necessary, click **Scan** to locate the DeviceMaster.



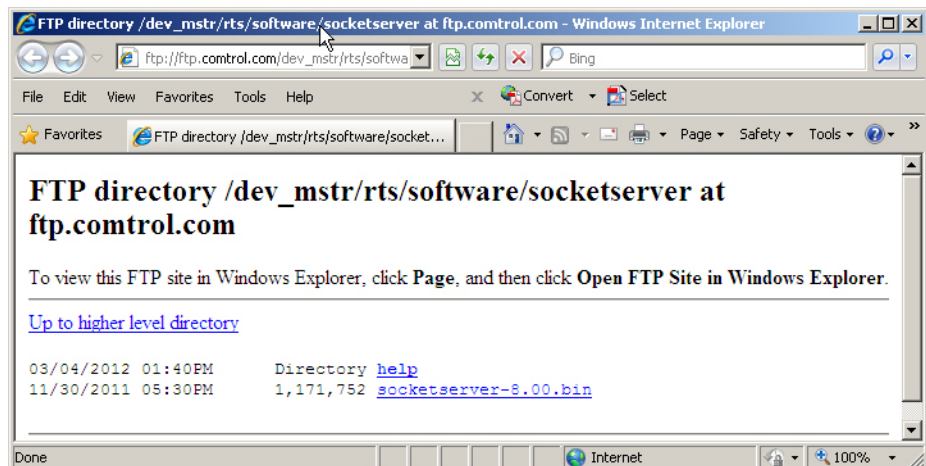
The *List View* pane displays the NS-Link version.

3. Check the Control 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. The device drivers always include latest version of SocketServer as a component that appears through the driver as NS-Link.

You can use this link to check to see what version of SocketServer/NS-Link is available at: ftp://dev_mstr/rtts/software/socketserver.

4. Compare the version number displayed in PortVision Plus to the version displayed in the ftp directory.



Note: In this example, the DeviceMaster contains v7.31 but v8.00 is available.

5. If a higher version of SocketServer is available and you want to update the DeviceMaster with the latest software:
 - a. Update SocketServer using [Uploading SocketServer with PortVision Plus on Page 39](#).
 - b. Download the latest driver from ftp://ftp.comtrol.com/dev_mstr/rts/drivers/win7.
-

To view this FTP site in Windows Explorer, click **Page**, and then click **Open FTP Site in Windows Explorer**.

[Up to higher level directory](#)

01/26/2012 09:40AM	4,937,728	nslink_windows_9.02.msi
03/04/2012 01:40PM	Directory	sw_doc

- c. Update to the latest driver using the *DeviceMaster Device Driver (NS-Link) User Guide*, which can be downloaded using Page 12 or viewed on the Control CD shipped with the DeviceMaster.

Restoring Factory Defaults (2-Port, Only)

Use the following procedures to restore a DeviceMaster 2-port model to the factory defaults. To return to default port settings, see [Restoring Serial Port Settings on Page 127](#).

Note: For other models, see [Returning the DeviceMaster to Factory Defaults on Page 176](#).

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

Restoring the DeviceMaster 2-port models resets the following to their factory defaults:

- 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 Control Drivers Management Console using **Start > Programs > Control > DeviceMaster** or under *Control Panel*, **Control Drivers 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 73](#)).
2. Scroll to the bottom of the *Server Configuration* page (main) and click **Reboot**.
3. When the **Reboot** page appears, click the **Set configuration for all ports to factory default settings** check box.
4. Click the **Yes, Reboot** button.

RedBoot Procedures

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

- [Accessing RedBoot Overview](#) on Page 129
- [Establishing a Serial Connection](#) on Page 130
- [Establishing a Telnet Connection](#) on Page 131
- [Determining the Network Settings](#) on Page 132
- [Configuring the Network Settings](#) on Page 132
- [Changing the Bootloader Timeout](#), Page 133
- [Determining the Bootloader Version](#) on Page 133
- [Resetting the DeviceMaster](#) on Page 134
- [Uploading Firmware](#) on Page 134
- [Configuring Passwords](#) on Page 138
- [RedBoot Command Overview](#) on Page 139.

Optionally, you can install PortVision Plus on a Windows system on the network and perform all of these tasks except configuring a password. PortVision Plus provides a Telnet/SSH session, which is discussed in

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 130). If you plan on using the serial method, you will need a null modem cable and a terminal program installed and configured on the PC.

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 131), 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 Plus using **Tools > Application > Test Terminal (WCom2)**.

Note: *Optionally, you can use Test Terminal, which is included in PortVision Plus 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 [Connecting Serial Devices](#) on Page 99, 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.

```
#!DM
RedBoot>dis
Loading disabled
```

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 129 or use the [RedBoot Command Overview](#) on Page 139 to perform the desired task.

Establishing a Telnet Connection

Use the following procedure to telnet to the DeviceMaster.

1. Open a telnet session, enter the DeviceMaster IP address. If using Windows, open a **Command** window and type **telnet [ip_address]**
2. Press the **Enter** key if you did not program a password or type the password and press **Enter**.

```

♥♦
Password:

Control DeviceMaster RTS Model ID: 5002535

SocketServer 8.00
Built: Wed Nov 30 15:36:45 CST 2011
IP Addr: 192.168.11.30, Mask: 255.255.0.0, Gateway: 192.168.11.1
MAC Addr: 00:c0:4d:29:ff:f5

dm> reset

```

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.

```

*****
**
** Control DeviceMaster Bootloader Version 3.21
** RedBoot(tm) environment - built 20:20:56, May 18 2011
** Platform: Control DeviceMaster (ARM 7TDMI)
** Portions Copyright (C) 2000. Red Hat, Inc.
** Portions Copyright (C) 2001-2008 Control Corp.
*****

FLASH: 64 blocks of 65536 bytes each
FLASH: 4194304 bytes (0x05000000 - 0x05400000)
RAM: 8126464 bytes (0x00000000 - 0x007c0000)
RedBoot> dis
Loading disabled
RedBoot> _

```

6. Verify that the system responds with a **Loading disabled** message.

Determining the Network Settings

Default Network Settings
IP address:
192.168.250.250
Subnet mask:
255.255.0.0
Gateway address:
192.168.250.1

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

1. Establish communications with the DeviceMaster using the serial (Page 130) or telnet (Page 131) method.
2. At the **RedBoot** prompt, type **ip**.

```
RedBoot>dis  
Loading disabled  
RedBoot> ip  
IP Config: IpAddr 192.168.250.250 IpMask 255.255.0.0 IpGate 192.168.250.1  
RedBoot>
```

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

Note: *Optionally, you can install PortVision Plus on a Windows system on the network and see the IP information in the List View 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 130) or telnet (Page 131) 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 ###.###.###.### ###.###.###.### ###.###.###.###  
RedBoot>  
IP Config: IpAddr ###.###.###.### IpMask ###.###.###.### IpGate ###.###.###.###  
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 130) or telnet (Page 131) 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 130) or telnet (Page 131) method.
2. At the **RedBoot** prompt, type **version**.

```
RedBoot> version
*****
**
** Control DeviceMaster Bootloader Version 3.21
** RedBoot(tm) environment - built 20:20:56, May 18 2
** Platform: Comtrol DeviceMaster (ARM 7TDMI)
** Portions Copyright (C) 2000. Red Hat, Inc.
** Portions Copyright (C) 2001-2008 Comtrol Corp.
*****

FLASH: 64 blocks of 65536 bytes each
FLASH: 4194304 bytes (0x05000000 - 0x05400000)
RAM: 8126464 bytes (0x00000000 - 0x007c0000)
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 Plus on a Windows system on the network and see the Bootloader version in the List View 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 [LEDs](#) 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.

```
RedBoot> dis
Loading disabled
RedBoot> reset
```

Uploading Firmware

Use the appropriate procedure for your environment:

- [Serial Method](#) (below)
- [Telnet Method \(Linux\)](#) on Page 136

Note: Optionally, you can install [PortVision Plus](#) on a Windows system on the network and upload firmware. [PortVision Plus](#) is the recommended method for uploading firmware. See [Installing PortVision Plus](#) on Page 35 and [Uploading SocketServer with PortVision Plus](#) on Page 39.

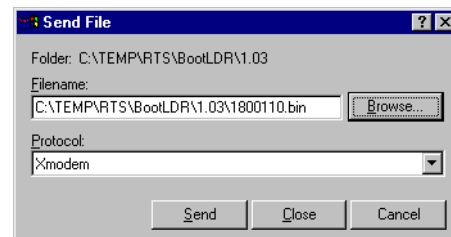
Serial Method

The procedure for updating the Bootloader and SocketServer are the same, but the **.bin** files are unique.

1. Verify that you have the **.bin** file ([Locating Software and Documentation](#) on Page 12) and performed [Establishing a Serial Connection](#) on Page 130.
2. Verify that the system responds with an **Loading disabled** message.
3. Type **load -r -b 0 -m x** at the **RedBoot>** prompt and press **Enter**.

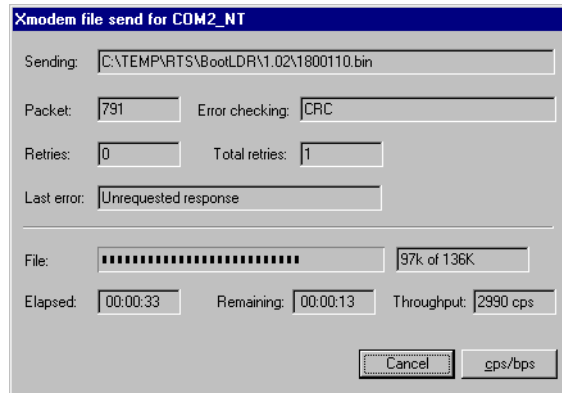
```
RedBoot> load -r -b 0 -m x
CC
```

4. Upload the file using Xmodem for the protocol. For example, if you are using HyperTerminal:
 - a. Click **Transfer**.
 - b. Click **Send File**.
 - c. Browse to the location where you saved the **.bin** file.
 - d. Click **Xmodem** as the protocol.



The file name in this screen shows the Bootloader.

- e. Click **Send**.



The file name in this screen shows the Bootloader.

5. When the **RedBoot>** prompt appears (after approximately one minute for the Bootloader and approximately three minutes for SocketServer), type **go**.

```
CCCCCRaw load done: 542721 bytes read
Address range: 00000000-00084800, Entry point: 00000000,
xyzModem - CRC mode, 4241(SOH)/0(STX)/0(CAN) packets, 8 tries
RedBoot> go
... Erase from 0x05030000-0x050c0000: .....
... Program from 0x00000000-0x00084801 at 0x05060000: ...
... Erase from 0x050f0000-0x05400000: .
... Program from 0x007a0000-0x007b0000 at 0x053f0000: .
```

Note: In a few seconds, the ethernet and **PWR** or **Status LEDs** cycle through a light sequence once and then upgrade is complete.

6. **If you updated SocketServer:** type, **fis list** and press **Enter** at the RedBoot> prompt

```
RedBoot> fis list
Name          FLASH addr  Mem addr    Length      Entry point
FIS_directory 0x053F0000  0x053F0000  0x00010000  0x00000000
default       0x05030000  0x00000000  0x00090000  0x00000000
RedBoot>
```

Note: You should see file information for a file called **default**. If you do not see this file, repeat the process starting with [Step 1](#).

7. Reset the DeviceMaster by typing **reset** at the RedBoot> prompt.

```
RedBoot> reset
. . .Resetting
```

Note: In a few seconds the ethernet and **PWR** or **Status LEDs** cycle through a light sequence once and the update is complete.

8. Start your internet browser and enter the IP address of the DeviceMaster to verify that the new version of SocketServer loads.

Telnet Method (Linux)

Use the following procedure to update the Bootloader or SocketServer with telnet to the DeviceMaster.

A TFTP server is required to perform firmware updates using RedBoot.

- If you are using Windows, see [Using TFTP \(Windows\)](#) on Page 40 to install and use a TFTP server with PortVision Plus.
- If you are using Linux and do not have a TFTP server installed, you can use [Setting Up a TFTP Server in Linux](#) (below). If you have a TFTP server installed, you can skip to [Uploading the Firmware](#) on Page 136.

Setting Up a TFTP Server in Linux

Use this procedure to set up a TFTP server.

1. Install and enable the tftp server software:

```
/usr/bin/up2date tftp-server
/sbin/chkconfig tftp on
```

2. Enter the following command so that it runs via **xinetd reload** to pick up the configuration file change:

```
/sbin/service xinetd reload
```

3. Edit the `/etc/sysconfig/iptables-config` file and change the **IPTABLES_MODULES** line to read:

```
IPTABLES_MODULES="ip_conntrack_tftp"
```

If you already have something in that line you can add the new module with a space in between, for example:

```
IPTABLES_MODULES="ip_conntrack_ftp ip_conntrack_tftp"
```

4. Add firewall rules to the `/etc/sysconfig/iptables` file. You only need UDP, though typically Control support recommends that you also add the TCP rules. The rules are both listed in **/etc/services for port 69**:

```
-A RH-Firewall-1-INPUT -s 192.168.250.250/16 -m tcp -p tcp --dport 69 -j ACCEPT
-A RH-Firewall-1-INPUT -s 192.168.250.250/16 -m udp -p udp --dport 69 -j ACCEPT
```

Note: The above IP address is the DeviceMaster default IP address.

5. Restart **iptables** to pick up the changes from Steps 3 and 4:

```
/sbin/service iptables restart
```

6. Add the proper lines to `/etc/hosts.allow`:

```
in.tftpd: 192.168.250.250
```

7. Go to [Uploading the Firmware](#) on Page 136 to load the firmware.

Uploading the Firmware

This Linux procedure requires that a TFTP server is installed.

1. Verify that you have the **.bin** file ([Locating Software and Documentation](#) on Page 12) and place the **.bin** file in `/tftpboot` so that you can retrieve it with the DeviceMaster.
2. Open a telnet session, enter the DeviceMaster IP address.
3. 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.
4. Type **reset**, and close the session.
5. Open a new telnet session and enter the DeviceMaster IP address.

```
$ telnet 192.168.250.250 ←————— Default IP Address
Trying 192.168.250.250...
Connected to 192.168.250.250.
Escape character is '^]'.

```


6. Enter the webserver password and **Enter**, or press **Enter** if a password has not been set up.

```

Password:
*****
**
** Control DeviceMaster Bootloader Version 3.21
** RedBoot(tm) environment - built 20:20:56 May 18 2011
** Platform: Control DeviceMaster (ARM 7TDMI)
** Portions Copyright (C) 2000. Red Hat, Inc.
** Portions Copyright (C) 2001-2008 Control Corp.
*****

FLASH: 64 blocks of 65536 bytes each
FLASH: 4194304 bytes (0x05000000 - 0x05400000)
RAM: 8126464 bytes (0x00000000 - 0x007c0000)
RedBoot>

```

7. At the **RedBoot >** prompt: type **dis** and press **Enter** to disable the Bootloader.

```

RedBoot>dis
Loading disabled

```

8. Verify that the system responds with an **Loading disabled** message.
9. Load the file from a TFTP server using the following command and then press **Enter**:
load -r -b 0 -h <TFTP-Server_IP_Addr> <Downloaded_File_Name>

```

RedBoot> load -r -b 0 -h 192.168.250.1 1800110.bin
CCCCRaw load done: 139521 bytes read
Address range: 00000000-00022100, Entry point: 00000000.
xyzModem - Cksum mode, 1091(SOH)/0(STX)/0(CAN) packets, 6 retries
RedBoot>

```

10. When the RedBoot> prompt appears (after approximately one minute if you are uploading the Bootloader and approximately three minutes if you are uploading SocketServer), type **go**.

```

RedBoot>go

```

If uploading Bootloader: In a few seconds the ethernet and **PWR** or **Status LEDs** cycle through a light sequence once and the update is complete.

If uploading SocketServer:

- a. At the RedBoot> prompt, type: **fis list** and press **Enter**.

```

RedBoot> fis list
Name          FLASH addr    Mem addr      Length      Entry point
FIS_directory 0x053F0000    0x053F0000    0x00010000  0x00000000
default       0x05030000    0x00000000    0x00090000  0x00000000
RedBoot>

```

Note: You should see file information for a file called **default**. If you do not see this file, repeat the process starting with [Step 9](#).

- b. Reset the DeviceMaster by typing **reset** at the RedBoot> prompt

Note: In a few seconds the ethernet and **PWR** or **Status LEDs** cycle through a light sequence once.

- c. Start your internet browser and enter the IP address of the DeviceMaster to verify that the new version of SocketServer loads.

Configuring Passwords

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

Note: See the *PortVision Plus* 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 130) or telnet method (Page 131).
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.

```
Password:
*****
**
** Control DeviceMaster Bootloader Version 3.05
** RedBoot(tm) environment - built 20:20:56, May 18 2011
** Platform: Control DeviceMaster (ARM 7TDMI)
** Portions Copyright (C) 2000. Red Hat, Inc.
** Portions Copyright (C) 2001-2008 Control Corp.
*****

FLASH: 64 blocks of 65536 bytes each
FLASH: 4194304 bytes (0x05000000 - 0x05400000)
RAM: 8126464 bytes (0x00000000 - 0x007c0000)
RedBoot> dis
Loading disabled
RedBoot> password dev1357
Password 'dev1357'
RedBoot>
```

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

See the **auth** command in the [RedBoot Command Overview](#) on Page 139, if you want to set up Web browser authentication.

RedBoot Command Overview

The following table is an overview of RedBoot commands available. You can access the list of commands online by entering **help** and pressing the **Enter** key. For more detailed information, see the *eCos Reference Manual* that is located on the *Control Software and Documentation* CD or you can download it from: ftp://ftp.comtrol.com/dev_mstr/rts/software/redboot/user_guide.

RedBoot Commands	
auth {noaccess, none, basic, md5, invalid}	Sets or displays web authentication. The default is set to none , which means that there is no authentication required to access the web server. 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. 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>]	Displays or switches the console channel.
chassis	Displays chassis information.
cksum -b <location> -l <length>	Computes a 32-bit checksum [POSIX algorithm] for a range of memory.
disable	Disables automatic load of the default application.
dump -b <location> [-l <length>] [-s] [-1 2 4]	Displays (hex dump) of a range of memory.
fis {cmds}	Manages flash images. See Chapter 2 of the eCos Reference Manual for {cmds} information.
flash	Shows flash information.
go [-w <timeout>] [-c] [-n] [entry]	Executes code at a location.
help <topic>	Displays available RedBoot commands.
?	Displays short help.
history	Displays command history.
ip [addr mask gateway]	Displays or sets the IP address configuration.
load [-r] [-v] [-h <host>] [-p <TCP port>] [-m <TFTP xyzmodem>] [-c <channel_number>] [-b <base_address>] <file_name>	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.
ncmp -s <location> -d <location> -l <length> [-1 -2 -4]	Compares two blocks of memory.

RedBoot Commands (Continued)	
mcopy -s <location> -d <location> -l <length> [-1 -2 -4]	Copies memory from one address to another.
mfill -b <location> -l <length> -p <pattern> [-1 -2 -4]	Fills a block of memory with a pattern.
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>	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.
snmp [disable enable]	Sets or displays SNMP enable.
telnet [disable enable]	Sets or displays telnet server enable. Disables telnet
timeout [seconds]	Shows or sets telnet time-out
terse	Terse command response mode.
timeout {seconds}	Displays or sets Bootloader time-out value.
t485 port #1 port #2	Runs port-to-port RS-485 test. This is not available on the DeviceMaster Serial Hub.
version	Displays RedBoot version information.
x -b <location> [-l <length>] [-s] [-1 2 4]	Displays (hex dump) a range of memory.
<i>† Do not use these commands to change the values. Doing so may cause the DeviceMaster to stop functioning.</i>	

Hardware Specifications

Locating DeviceMaster Specifications

Specifications can be found on the Control web site at the following addresses.

Product	Ports	Connector/ Number of Ethernet Ports	Specification Web Page
DeviceMaster PRO	8	DB9/2E	http://www.comtrol.com/pub/products/product/pid/163
DeviceMaster PRO	16	DB9/2E	http://www.comtrol.com/pub/products/product/pid/164
DeviceMaster RTS (5V)	1	DB9/1E	http://www.comtrol.com/pub/products/product/pid/167
DeviceMaster RTS VDC (5-30VDC)	1	DB9/1E	http://www.comtrol.com/pub/products/product/pid/168
DeviceMaster RTS VDC embedded (5-30VDC)	1	DB9/1E	http://www.comtrol.com/pub/products/product/pid/169
DeviceMaster RTS	2	Screw terminals/1E	http://www.comtrol.com/pub/products/product/pid/170
DeviceMaster RTS	2	Screw terminals/2E	http://www.comtrol.com/pub/products/product/pid/171
DeviceMaster RTS	2	DB9/1E	http://www.comtrol.com/pub/products/product/pid/165
DeviceMaster RTS	2	DB9/2E	http://www.comtrol.com/pub/products/product/pid/166
DeviceMaster RTS	4	DB9/2E	http://www.comtrol.com/pub/products/product/pid/172
DeviceMaster RTS	4	DB9/2E	http://www.comtrol.com/pub/products/product/pid/173
DeviceMaster RTS	8	DB9/2E	http://www.comtrol.com/pub/products/product/pid/174
DeviceMaster RTS	8	RJ45/2E	http://www.comtrol.com/pub/products/product/pid/175
DeviceMaster RTS	16	RJ45/1E	http://www.comtrol.com/pub/products/product/pid/177
DeviceMaster RTS	16	RJ45/2E	http://www.comtrol.com/pub/products/product/pid/176
DeviceMaster RTS	32	RJ45/1E	http://www.comtrol.com/pub/products/product/pid/178
DeviceMaster Serial Hub	8	DB9/2E	http://www.comtrol.com/pub/products/product/pid/179
DeviceMaster Serial Hub	16	DB9/2E	http://www.comtrol.com/pub/products/product/pid/180

External Power Supply Specifications

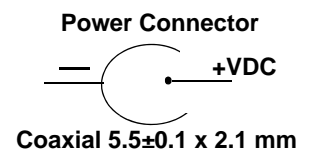
This subsection discusses information that you may need if you wish to use your own external power supplies.

- [1-Port 5VDC Power Supply](#) (below)
- [1-Port 5-30VDC Power Supply](#) on Page 142
- [2-Port \(Serial Terminals\) Power Supply](#) on Page 143
- [2-Port \(DB9\) Power Supply](#) on Page 143
- [4-Port Power Supply](#) on Page 144
- [8-Port Power Supply](#) on Page 144
- [16-Port Power Supplies](#) on Page 145

1-Port 5VDC Power Supply

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

Control Power Supply: 1-Port 5VDC	
Input line frequency	47 - 63 Hz
Input line voltage	90 - 132VAC (<i>standard RTS</i>) 90 - 260VAC (<i>IAD model</i>)
Output voltage	5VDC
Output current	2.4A @ 5VDC



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

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

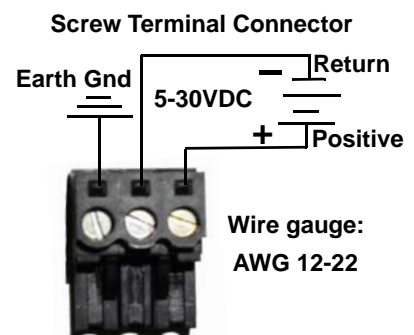
1-Port 5-30VDC Power Supply

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

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

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

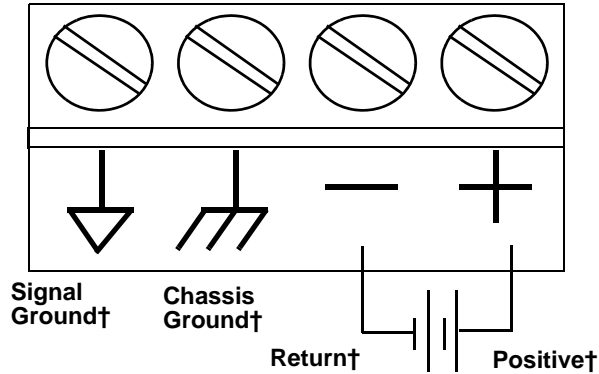
External Power Supply: 1-Port 5-30VDC	
Output voltage†	5-30VDC
Current†	100 mA (Min) @ 24VDC
Power	2.5 W
† Any power supply that meets current consumption, voltage, power, and connector pinouts requirements can be used.	



2-Port (Serial Terminals) Power Supply

This table provides the specifications to purchase a power supply for a DeviceMaster 2-port 1E/2E model with serial terminal connectors.

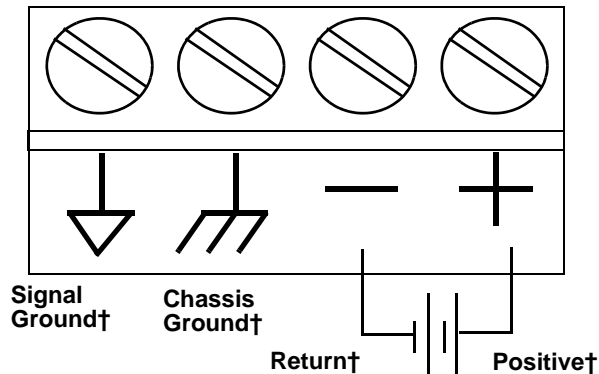
External Power Supply: 2-Port (Serial Terminal Connectors) 5-30VDC	
Output voltage†	5-30VDC
Current†	100 mA (Min) @ 24VDC
Power	2.5 W
† Any power supply that meets current consumption, voltage, power, and connector pinouts requirements can be used.	



2-Port (DB9) Power Supply

This table provides the specifications to purchase a power supply for a DeviceMaster 2-port 1E/2E model with serial terminal connectors.

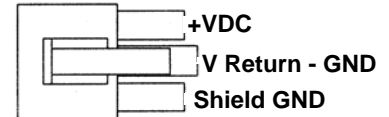
External Power Supply: 2-Port (Serial Terminal Connectors) 6-30VDC	
Output voltage†	6-30VDC
Current†	100 mA (Min) @ 24VDC
Power	2.5 W
† Any power supply that meets current consumption, voltage, power, and connector pinouts requirements can be used.	



4-Port Power Supply

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

Control Power Supply: 4-Port	
Input line frequency	47 - 63 Hz
Input line voltage	90 - 260 VAC
Output voltage	24VDC
Output current	500 mA @ 24VDC



Housing Molex P/N:
39-01-4030
Pins Molex P/N:
44485-1211

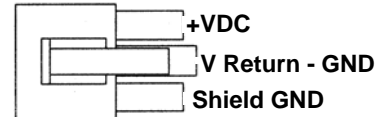
This table provides the specifications, if you intend on using your own power supply.

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

8-Port Power Supply

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

Control Power Supply: 8-Port	
Input line frequency	47 - 63 Hz
Input line voltage	90 - 260 VAC
Output voltage	24VDC
Output current	500 mA @ 24VDC



Housing Molex P/N:
39-01-4030
Pins Molex P/N:
44485-1211

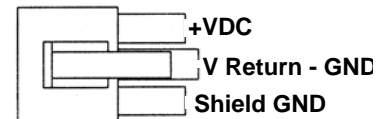
The following table provides the specifications, if you intend on purchasing your own power supply.

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

16-Port Power Supplies

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

Control Power Supply: 16-Port Models	
Input line frequency	47 - 63 Hz
Input line voltage	90 - 260 VAC
Output voltage	24VDC
Output current	500 mA @ 24VDC
Note: <i>The DeviceMaster RTS 16-port and 32-port models with a single Ethernet port have internal power supplies.</i>	



Housing Molex P/N:
39-01-4030
Pins Molex P/N:
44485-1211

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

External Power Supply: 16-Port DeviceMaster PRO	
Input line frequency	47 - 63 Hz
Input line voltage	90 - 260VAC
Output voltage†	9-30VDC
Output current†	290 mA (Min) @ 24VDC
† <i>Any power supply that meets current consumption, voltage, power, and connector pinouts requirements can be used.</i>	

External Power Supply: 16-Port DeviceMaster RTS	
Output voltage†	9-30VDC
Current†	490 mA (Min) @ 24VDC
Power	11.76 W
† <i>Any power supply that meets current consumption, voltage, power, and connector pinouts requirements can be used.</i>	

External Power Supply: 16-Port DeviceMaster Serial Hub	
Input line frequency	47 - 63 Hz
Input line voltage	90 - 260VAC
Output voltage†	9-30VDC
Output current†	132 mA (Min) @ 24VDC
† <i>Any power supply that meets current consumption, voltage, power, and connector pinouts requirements can be used.</i>	

DeviceMaster Product Pictures

This subsections provides you with detailed pictures of the different DeviceMaster models:

- [1-Port \(DB9\) 5VDC](#) on Page 146
- [1-Port \(DB9\) 5-30VDC](#) on Page 147
- [1-Port Embedded](#) on Page 148
- [2-Port \(Single Ethernet Port\) with Serial Terminals](#) on Page 148
- [2-Port \(Dual Ethernet Ports\) with Serial Terminals](#) on Page 148
- [2-Port \(Single Ethernet Port\) DB9](#) on Page 149
- [2-Port \(Dual Ethernet Ports\) DB9](#) on Page 149
- [4-Port \(DB9\)](#) on Page 150
- [8-Port \(DB9\)](#) on Page 150
- [16-Port \(RJ45\) External Power Supply](#) on Page 150
- [DeviceMaster Serial Hub 16-Port \(DB9\)](#) on Page 150
- [16-Port \(RJ45\) Internal Power Supply](#) on Page 150
- [DeviceMaster PRO 16-Port \(RJ45\)](#) on Page 150
- [DeviceMaster RTS 32-Port \(RJ45\)](#) on Page 151

1-Port (DB9) 5VDC

This illustrates the DeviceMaster 1-Port 5VDC.



See [DeviceMaster LEDs](#) on Page 172 for information about the LEDs.

1-Port (DB9) 5-30VDC

This illustrates the DeviceMaster 1-Port 5-30VDC.

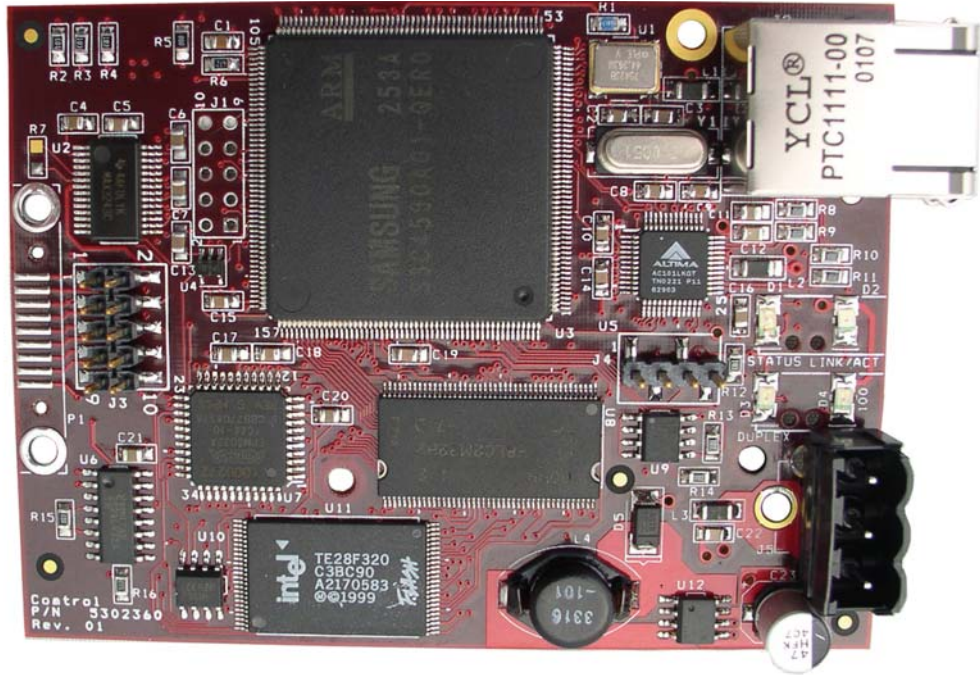


Note: The supported input voltage (5VDC or 5-30VDC) is printed on the top and bottom of the DeviceMaster.

See [DeviceMaster LEDs](#) on Page 172 for information about the LEDs.

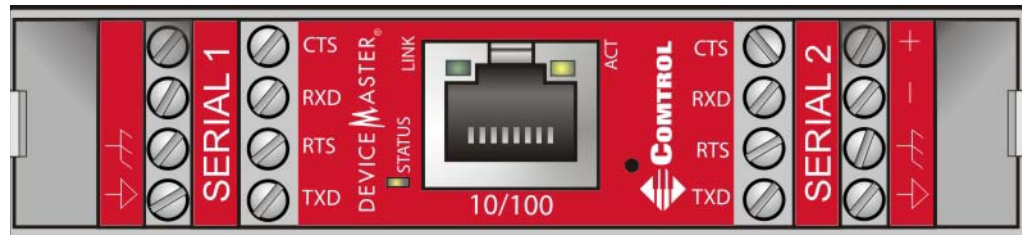
1-Port Embedded

This illustrates the DeviceMaster 1-port Embedded system that uses a 5-30VDC power supply. See [1-Port 5-30VDC Power Supply](#) on Page 142 so that you can provide a power supply for the DeviceMaster. See [DeviceMaster LEDs](#) on Page 172 for information about the LEDs.



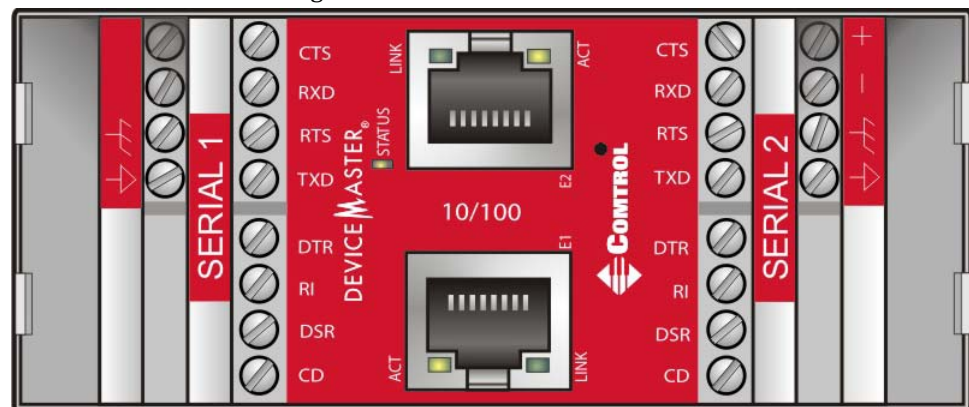
2-Port (Single Ethernet Port) with Serial Terminals

The DeviceMaster 2-port 1E with serial terminals uses a 5-30VDC power supply. See [2-Port \(Serial Terminals\) Power Supply](#) on Page 143 for information about the power supply. See [DeviceMaster LEDs](#) on Page 172 for information about the LEDs.



2-Port (Dual Ethernet Ports) with Serial Terminals

The DeviceMaster 2-port 2E with serial terminals uses a 5-30VDC power supply. See [2-Port \(Serial Terminals\) Power Supply](#) on Page 143 for information about the power supply. See [DeviceMaster LEDs](#) on Page 172 for information about the LEDs.



2-Port (Single Ethernet Port) DB9

The DeviceMaster 2-port 1E DB9 uses a 5-30VDC power supply. See [2-Port \(DB9\) Power Supply](#) on Page 143 for information about the power supply. See [DeviceMaster LEDs](#) on Page 172 for information about the LEDs.

**2-Port (Dual Ethernet Ports) DB9**

The DeviceMaster 2-port 2E DB9 uses a 5-30VDC power supply. See [2-Port \(DB9\) Power Supply](#) on Page 143 for information about the power supply. See [DeviceMaster LEDs](#) on Page 172 for information about the LEDs.

**4-Port (DB9)**

The **PWR** LED for the DeviceMaster 4 with DB9 ports is on the other side of the unit. See [DeviceMaster LEDs](#) on Page 172 for information about the LEDs.

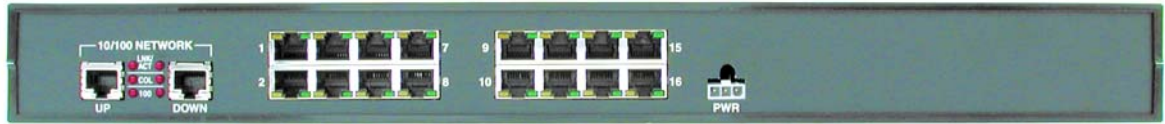
**8-Port (DB9)**

The **PWR** LED for the DeviceMaster 8 with DB9 ports is on the other side of the unit. See [DeviceMaster LEDs](#) on Page 172 for information about the LEDs.



16-Port (RJ45) External Power Supply

The PWR LED for this model is on the other side of the unit. See [DeviceMaster LEDs](#) on Page 172 for information about the LEDs.



16-Port (RJ45) Internal Power Supply

The power switch for this model is on the other side of the unit. See [DeviceMaster LEDs](#) on Page 172 for information about the LEDs.



DeviceMaster PRO 16-Port (RJ45)

The power connector for this model is on the other side of the unit. See [DeviceMaster LEDs](#) on Page 172 for information about the LEDs.



DeviceMaster Serial Hub 16-Port (DB9)

The power switch for this model is on the other side of the unit.



DeviceMaster RTS 32-Port (RJ45)

The power switch for this model is on the other side of the unit. See [DeviceMaster LEDs](#) on Page 172 for information about the LEDs.



Notices

Radio Frequency Interference (RFI) (FCC 15.105)

This equipment has been tested and found to comply with the limits for Class A digital devices pursuant to Part 15 of the FCC Rules.

This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Labeling Requirements (FCC 15.19)

This equipment complies with part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

Modifications (FCC 15.21)

Changes or modifications to this equipment not expressly approved by Control Corporation may void the user's authority to operate this equipment.

Serial Cables (FCC 15.27)

This equipment is certified for Class A operation when used with unshielded cables on models with the RJ45 connectors and with shielded cables on all models with DB9 connectors.

Underwriters Laboratory

This equipment is Underwriters Laboratory "UL" listed.

Important Safety Information



Warning

To avoid contact with electrical current:

- Never install electrical wiring during an electrical storm.
- Never install the power plug in wet locations.
- Use a screwdriver and other tools with insulated handles.

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.

- [Troubleshooting Checklist](#) on Page 153
- [General Troubleshooting](#) on Page 155
- [Testing Ports Using Port Monitor \(PMon2\)](#) on Page 157
- [Testing Ports Using Test Terminal](#) on Page 160
- [Socket Mode Serial Port Testing](#) on Page 166
- [Daisy-Chaining DeviceMaster 2E/4/8/16-Port Units](#) on Page 171
- [DeviceMaster LEDs](#) on Page 172
- [Removing DeviceMaster Security Features](#), Page 174
- [Returning the DeviceMaster to Factory Defaults](#) on Page 176

If you cannot diagnose the problem, you can contact [Technical Support](#) on Page 179.

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 Control Technical Support are eventually traced to cabling or network problems.

Model	Connected to	Ethernet Cable	Connector Name
1-Port	Ethernet hub or NIC	Standard	10/100 ETHERNET
1-Port Embedded	Ethernet hub or NIC	Standard	RJ45 port (not labeled)
2-Port - 1E (All models)	Ethernet hub or NIC	Standard	10/100
2-Port - 2E (All dual Ethernet ports)	NIC or Ethernet hub	Standard	10/100 - E1/E2
4/8-Port	NIC	Standard	DOWN
	Ethernet hub	Standard	UP
16-Port (external power supply)	NIC	Standard	DOWN
	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 Control tools.
 - *Advanced* tab in the Control Drivers Management Console which helps identify problems.
 - PortVision Plus 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 [Testing Ports Using Test Terminal](#) on Page 160 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 [Testing Ports Using Port Monitor \(PMon2\)](#) on Page 157 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 172) 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.
5 quick flashes	The default application is starting up.
10 sec. on. 1 sec. off, 10 sec. on.1 sec. off...	The default application is running.

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 NS-Link.
- If you have a spare DeviceMaster, try replacing the device.

General Troubleshooting

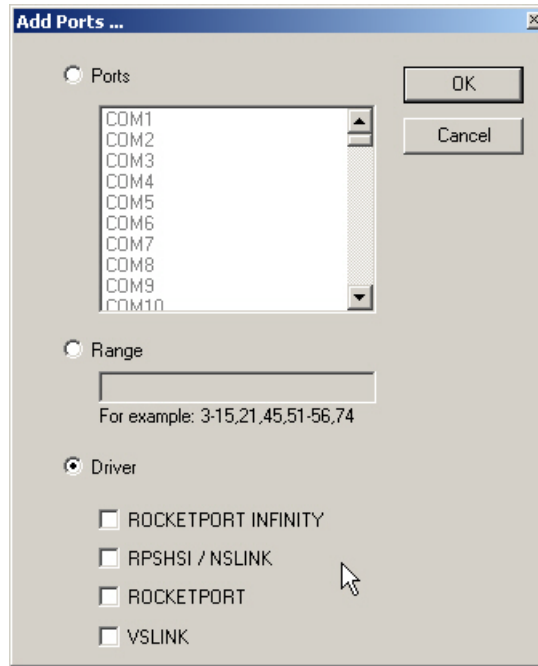
This table illustrates some general troubleshooting tips.

Note: Make sure that you have reviewed the [Troubleshooting Checklist](#) on Page 153.

General Condition	Explanation/Action
PWR or Status LED flashing	<p>Indicates that boot program has not downloaded to the DeviceMaster.</p> <ol style="list-style-type: none"> If applicable, remove the NS-Link driver. Make sure that you have downloaded the most current driver: ftp://ftp.comtrol.com/dev_mstr/rts/drivers/. Install the latest driver and configure the DeviceMaster using the MAC address. Make sure that you reboot the system. See Device Driver (NS-Link) Installation on Page 49 for procedures. <p>Note: If the PWR or Status LED is still flashing, contact Technical Support.</p>
PWR or Status LED not lit	<p>Indicates that power has not been applied or there is a hardware failure. Contact Technical Support</p>
<p>Can ping the Control device, but cannot open the ports from a remote location.</p> <p>(You must have previously programmed the IP address, subnet mask, and IP gateway.)</p>	<p>The NS-Link driver uses Port 4606 (11FE h) to communicate with the DeviceMaster.</p> <p>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</p> <p>If the 4606 packet is found on one side of a firewall or router, using sniffer, and not on the other side, then that port needs to be opened up to allow the 4606 to pass.</p> <p>This will most often be seen with firewalls, but is also seen in some routers.</p>
Cannot ping the device through Ethernet hub	<p>Isolate the DeviceMaster from the network. Connect the device directly to the NIC in the host system (see Page 153).</p>
Cannot ping or connect to the DeviceMaster	<p>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.</p> <p>In most cases, it will be necessary to program in an address that conforms to your network. See Configuring the Network Settings on Page 36 to use PortVision Plus to program the IP address.</p> <p>If you do not use PortVision Plus (or the NS-Link driver for Windows) to program the IP address, you can use RedBoot.</p> <p>If you use RedBoot, you only have 15 seconds to disable the Bootloader with RedBoot to get into the setup utility. See RedBoot Procedures on Page 129 for the RedBoot method of programming an IP address.</p>

General Condition	Explanation/Action
<p>DeviceMaster continuously reboots when connected to some Ethernet switches with the NS-Link driver</p>	<p>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.</p> <p><i>Resolution:</i> There will be no firmware fix for this problem. Only one of the following fixes is required for resolution.</p> <ol style="list-style-type: none"> 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. <p><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.</p> <p>The normal NS-Link driver load process is:</p> <ol style="list-style-type: none"> 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. <p>If the device is not loaded after timeout seconds (default 15), it loads SocketServer.</p> <p>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.</p>
<p>DeviceMaster continuously reboots when connected to some Ethernet switches or routers</p>	<p>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.</p>

- Click **Driver**, click **RPSHSI/NSLINK**.



- 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.

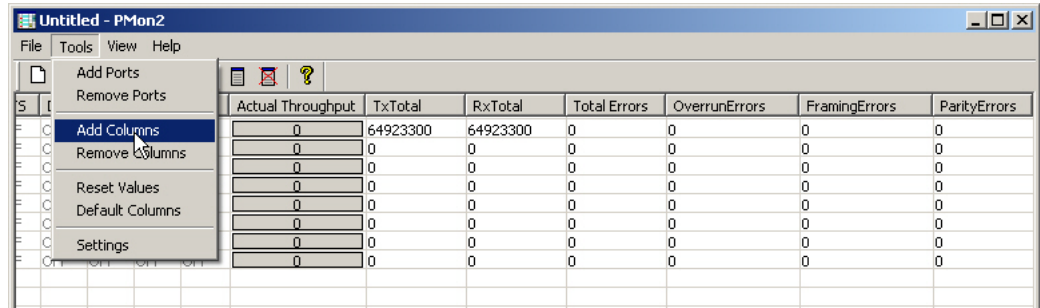
Port Name	Status	CTS	DSR	CD	RTS	DTR	Actual Throughput	TxTotal	RxTotal	Total Errors	OverrunErrors
COM11	OPEN	ON	ON	ON	ON	ON	114600	205891	205638	0	0
COM12	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0
COM13	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0
COM14	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0
COM15	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0
COM16	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0
COM17	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0
COM18	CLOSED	OFF	OFF	OFF	OFF	OFF	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**.

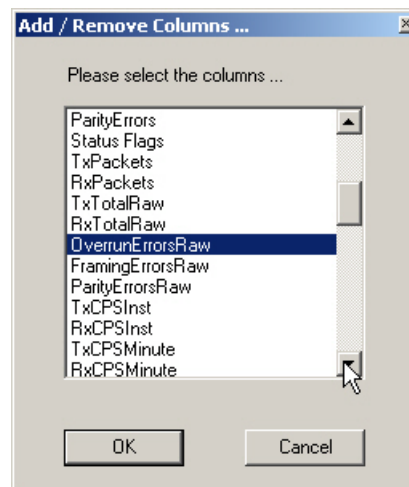
If the errors are:

- **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 a 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**.

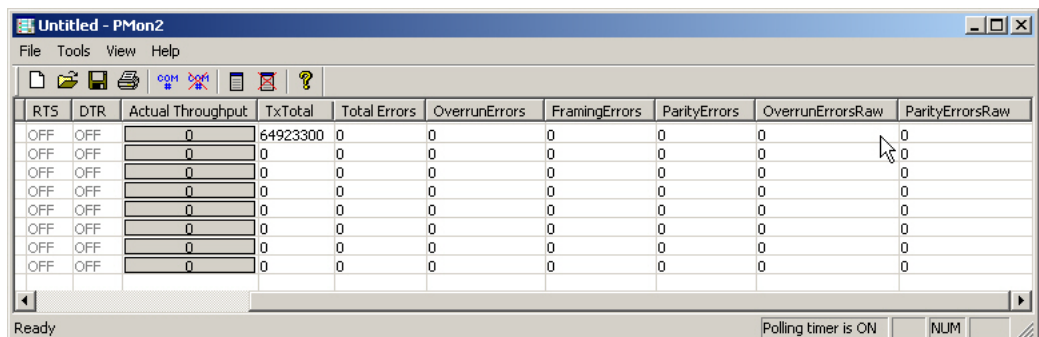


7. Highlight or shift-click to add multiple statistics and click **Ok**.




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.



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, go to <ftp://ftp.control.com/html/default.htm> to locate the latest 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 [Connecting Serial Devices](#) on Page 99.

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.

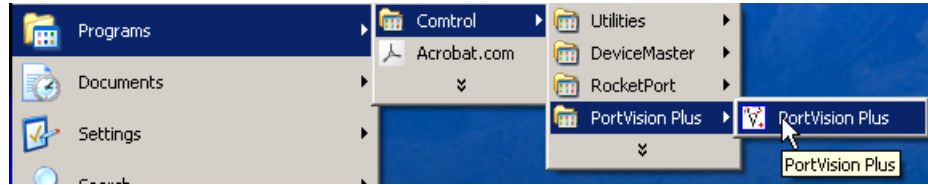
Opening Ports

The following procedure shows how to use **Test Terminal** to send and receive test data to the serial ports. If necessary, use [Installing PortVision Plus](#) on Page 35 or [PortVision Plus](#) on Page 13 to install PortVision Plus, which contains Test Terminal.

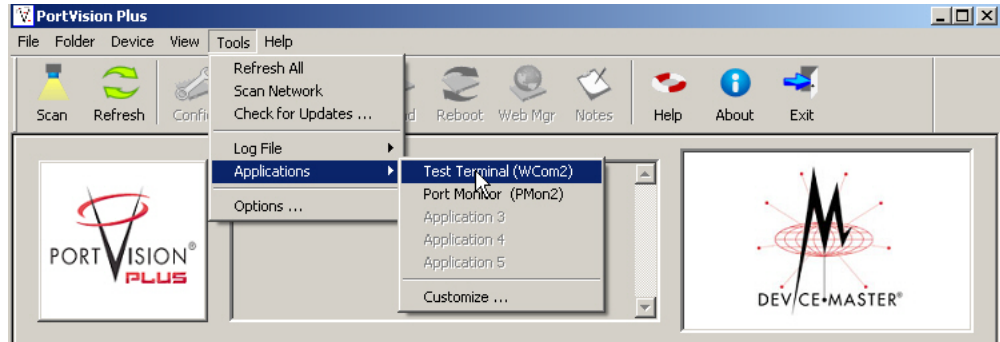
1. Stop all applications that may be accessing the ports such as RRAS or any faxing, or production software. See the appropriate help systems or manuals for instructions on stopping these services or applications.

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 Plus from the **Start** menu, select **Programs > Control > PortVision Plus > PortVision Plus** or click the desktop shortcut



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

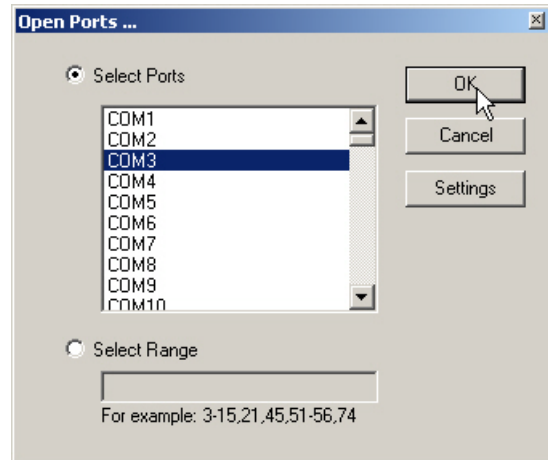


4. Select **File > Open Port**, the appropriate port (or ports) from the *Open Ports* drop list and **Ok**.

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.

- [Sending and Receiving Test Data \(RS-232/422/485: 4-Wire\)](#) (below)
- [Sending and Receiving Data \(RS-485: 2-Wire\)](#) on Page 163



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

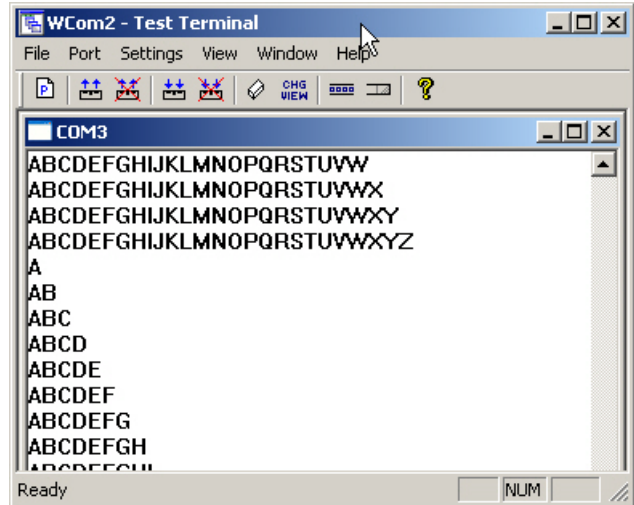
You can use this procedure to send and receive test data through the RS-232/422/485 (4-wire, full-duplex) port or ports that you want to test.

1. If you have not done so, perform [Steps 1](#) through [2](#) on Page 160.
2. Install the loopback plug onto the port (or ports) that you want to test. See [Connecting Serial Devices](#) on Page 99, 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 is 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 162 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.*

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 160, [Steps 1](#) through [2](#)).
2. Click **Port > Loopback Test**.

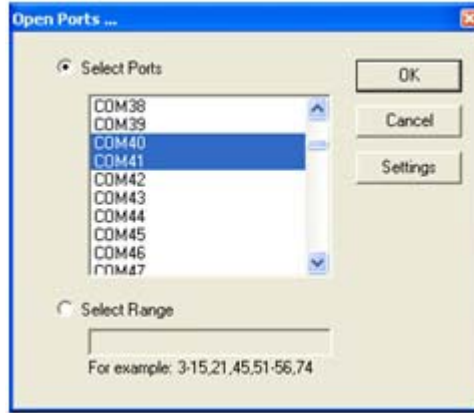
This is a pass fail test and will take a second or two to complete. Repeat for each port that needs testing.

If the Loopback Test and the Send and Receive Test Data tests successfully complete, then the port is operational as expected.

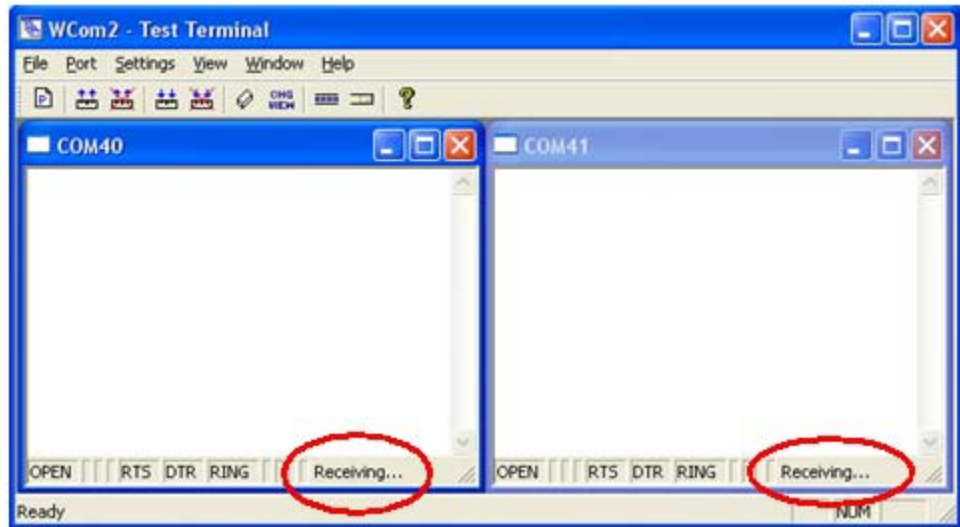
Sending and Receiving Data (RS-485: 2-Wire)

This procedure shows how to use Test Terminal (WCom2) to test two RS-485 (2-Wire, Half-Duplex) ports.

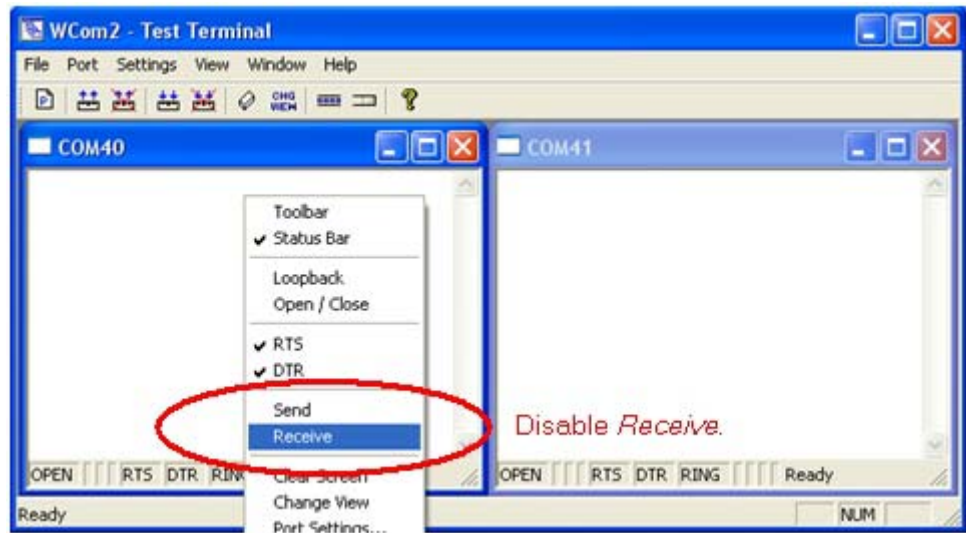
1. In PortVision Plus, click **Tools>Applications>Test Terminal (WCom2)** to start Test Terminal.
2. Open two ports RS-485 ports. This example uses COM40 and COM41.



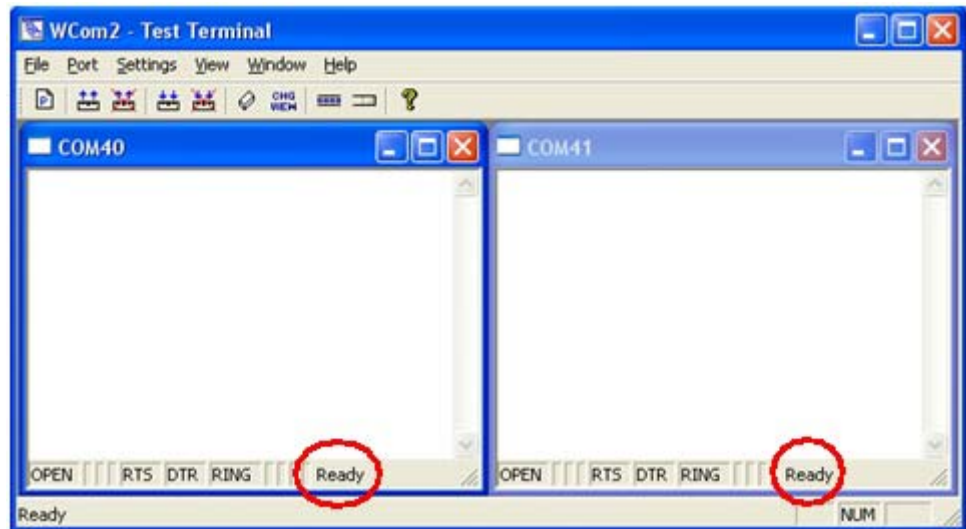
Test Terminal will open two windows, note that both ports show *Receiving* on the status bar.



3. Right-click in both COM windows and remove the check mark for **Receive**.

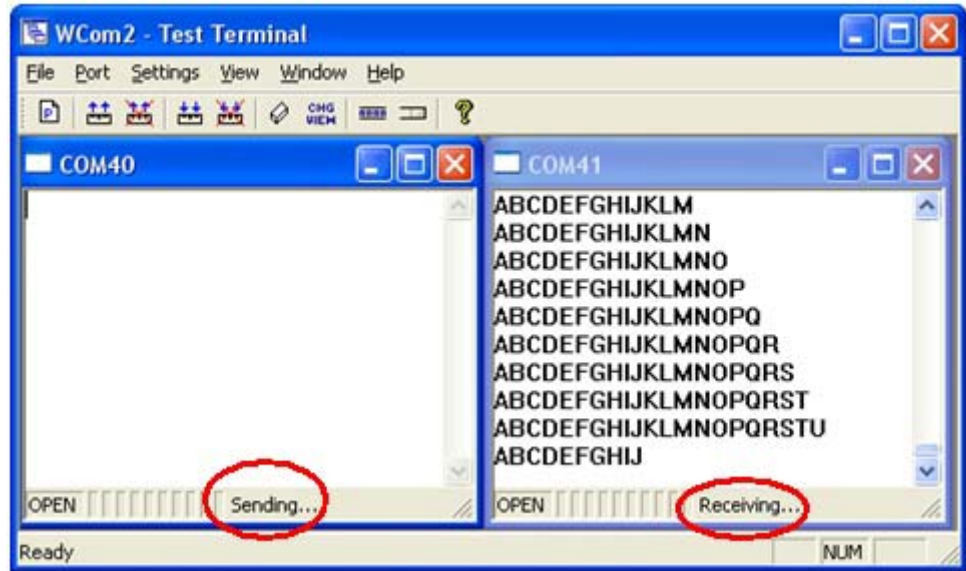


Both COM ports show *Ready* on the status bar.



4. Right-click in ONE window and select the **Receive** option from the pop up.

- Right-click the OPPOSITE window and click **Send**.

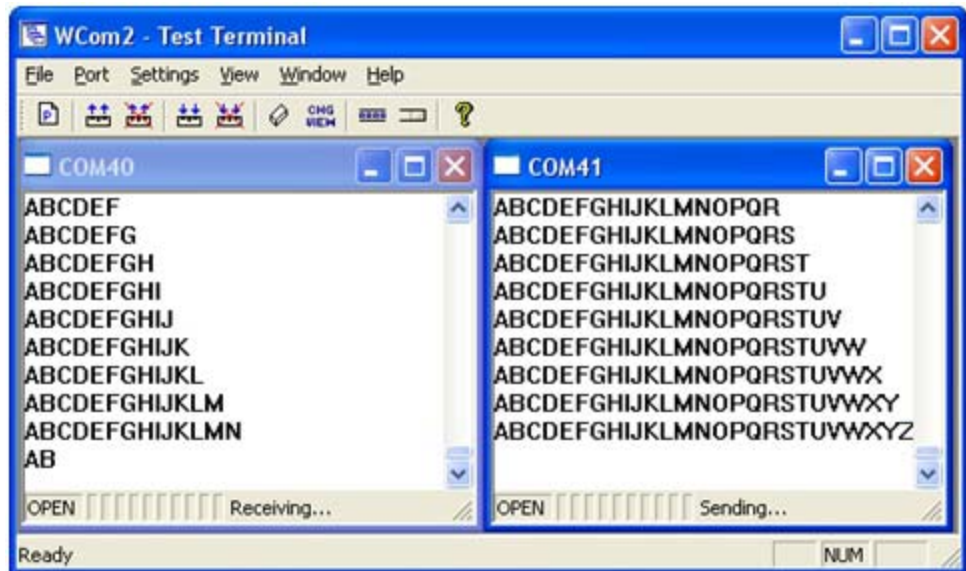


The *Status* line shows *Sending* or *Receiving*.

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.

- Right-click and remove the check mark on the *Sending* COM port.
- 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.

- Reverse the sending/receiving windows one at a time. Set the **Receive** option first, then in the opposite window, select the **Send** option.

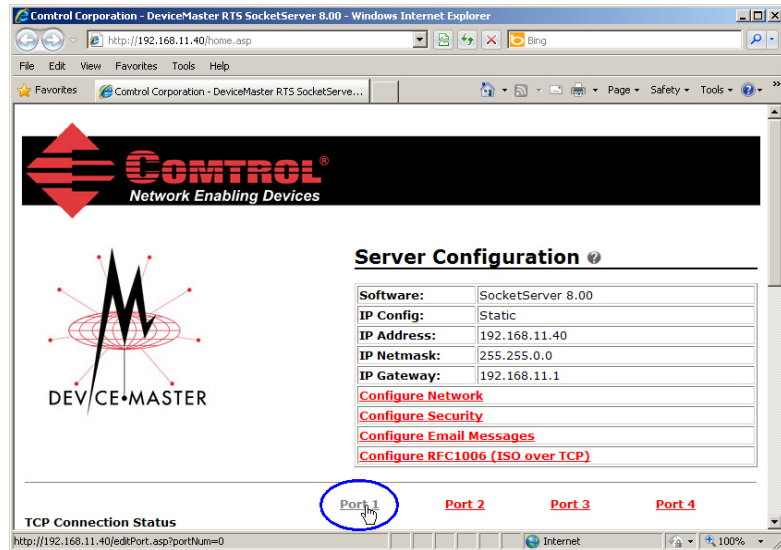
The *Status* line shows *Sending* or *Receiving* in the reverse windows.

Data is now scrolling in the COM40 window. COM41 is static as it is not receiving data but transmitting data.

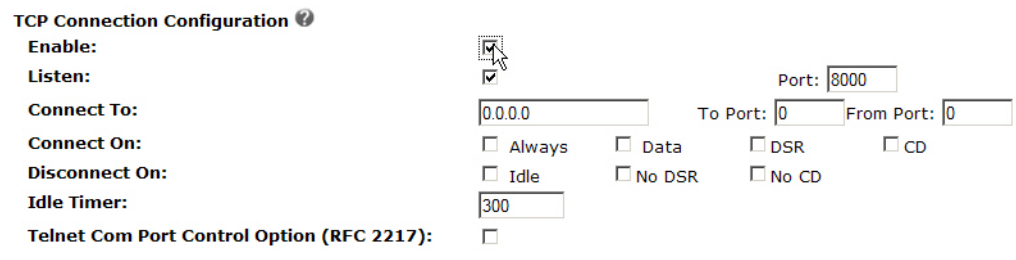
Socket Mode Serial Port Testing

This procedure illustrates using Windows XP, which includes Hyperterminal. For other operating systems, you can use any other Winsock compatible application.

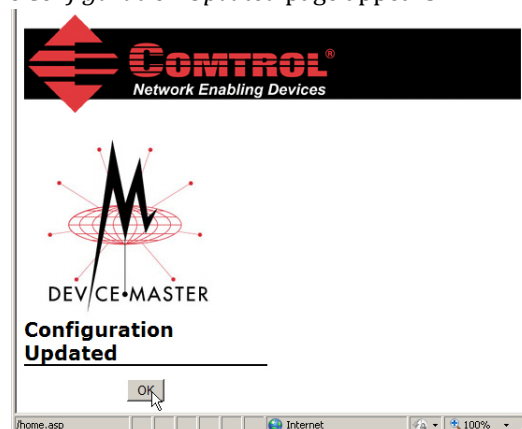
1. Open your web browser and enter the DeviceMaster IP address.
2. Click the port that you want to test



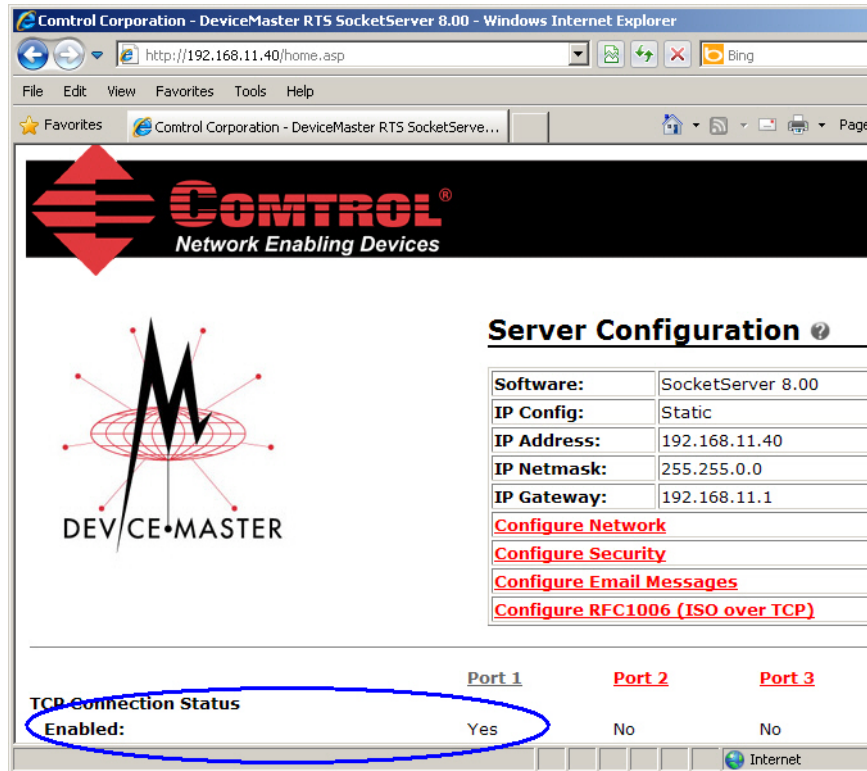
3. Scroll down *TCP Connection Configuration* options, click the **Enable** option, and leave all other settings on this page at their default values.



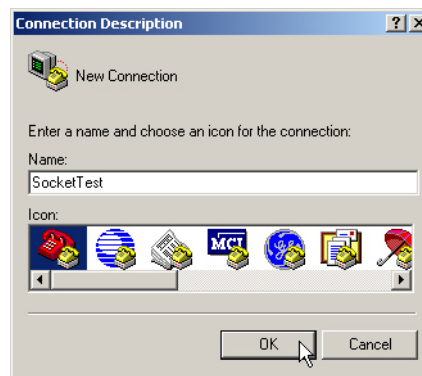
4. Scroll to the bottom of the page and click the **Save** button.
5. Click **Ok** when the *Configuration Updated* page appears.



- Verify that the port has been enabled.



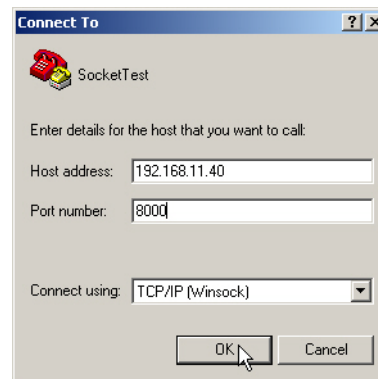
- Leave the web page open.
- Attach the loopback plug that was shipped with the DeviceMaster to the serial port of the DeviceMaster. See [Connecting Serial Devices](#) on Page 99 if you need to build a loopback plug.
- Open Hyperterminal from the **Start** button, select **Programs> Accessories> Communications> Hyperterminal**.
- Enter a name, select an icon, and click **Ok**.



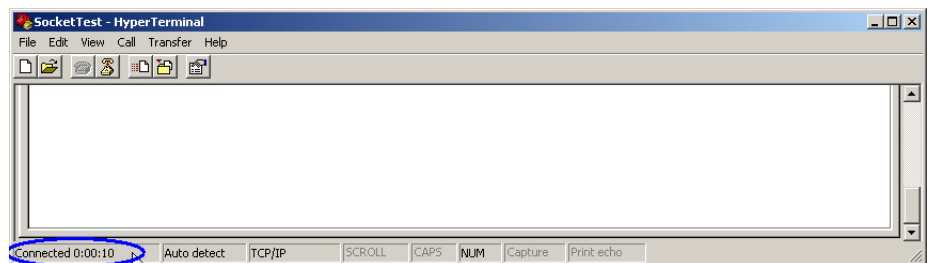
11. Select **TCP/IP Winsock** from the *Connect using* drop-list.



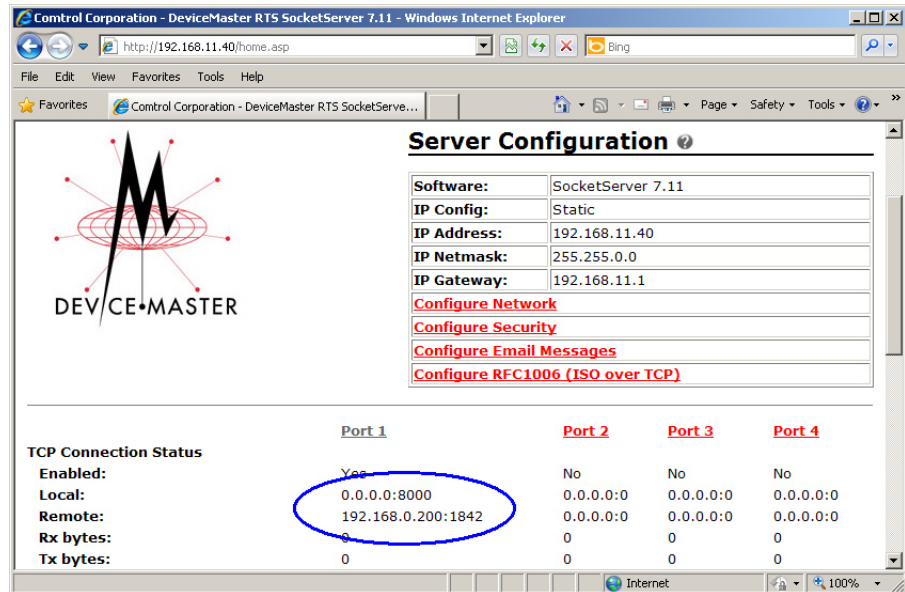
12. Enter the DeviceMaster IP address in the *Host Address* field, 8000 in the *Port Number* field, and click **Ok**.



The *Status* bar on the bottom left of the Hyperterminal screen should show that it is connected with a timer running.



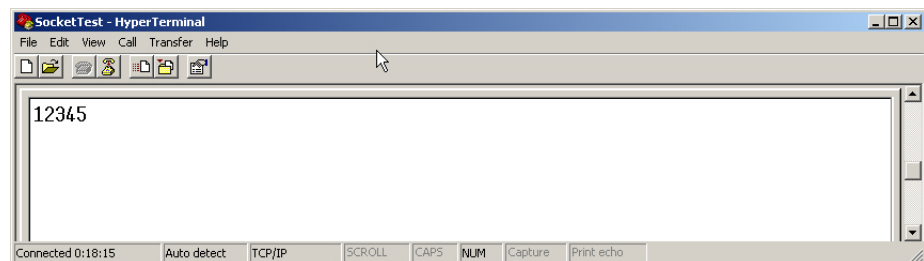
13. Return to the DeviceMaster web page, click **Refresh**. The web page should look like this:



- The *Remote: IP address* will be the IP address of the system running Hyperterminal.
- The values to the right of the colon (:) are the socket numbers in use.
- 8000 is the listening socket on the DeviceMaster.
- 1842 is the source socket on the PC.
- The Rx bytes and Tx bytes are 0 as no data has been sent.

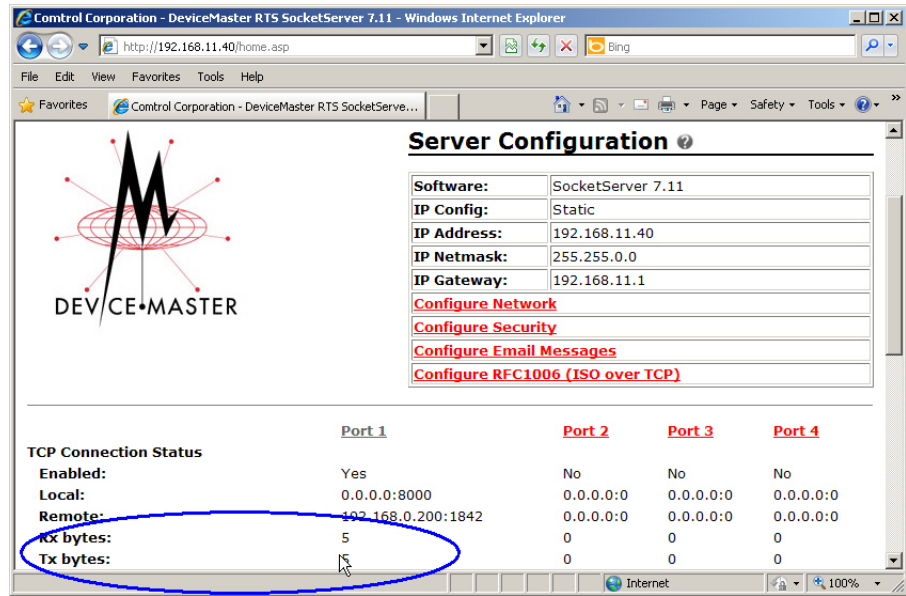
This establishes that you now have an active socket connection.

14. Return to Hyperterminal and type, **12345**, which you will see echoed in the Hyperterminal window.



This means that the loopback plug is receiving the data from the serial port and looping it right back into the serial port for return to Hyperterminal to be displayed on the screen.

15. Return to the web page and click **Refresh**.



Notice that the Rx and Tx bytes show that 5 bytes have been transmitted and received.

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

18. You can close Hyperterminal and save or not save the session as you desire.

Daisy-Chaining DeviceMaster 2E/4/8/16-Port Units

The DeviceMaster 2E/4/8/16-port models with external power supplies follow the IEEE specifications for standard Ethernet 10/100BASE-TX topologies.

When using the **UP** and **DOWN** ports, the DeviceMaster 2E/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 2E/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.

Control has tested with seven DeviceMaster 2E/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 inter-repeater link segments with no stations connected.

Additional information may be found at <http://compnetworking.about.com/cs/ethernet1/> or by searching the web.

DeviceMaster LEDs

The DeviceMaster has network and port LEDs to indicate status.

Port LEDs

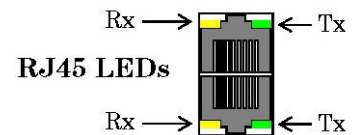
Port LEDs are amber and green on 4, 8, 16, and 32-port models. The 1-port and 2-port models do not have port LEDs.

After a port has been opened in RS-232 mode, an amber LED means that there is link between the port and the serial device. After a port has been opened in RS-422 or RS-485 mode, an amber LED means that data is receiving data. A green port LED indicates transmit activity.

Note: The port LED activity on the RTS 16/32RM may be inconsistent until the port has been opened. After a port is opened the LED activity works as documented.



* Represents port number.



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 Plus, you can check the DeviceMaster status on-line.

Ports	Model	Network LEDs
1	DeviceMaster RTS	<ul style="list-style-type: none"> The Status LED on the front of the unit is lit, which indicates that it has power and has completed the boot cycle. <p>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.</p> 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).
1	DeviceMaster RTS Embedded	<p>The LEDs are located between the RJ45 connector and the power terminal block.</p> <ul style="list-style-type: none"> The amber Status LED (D1) on the adapter is lit, which indicates that it has power and has completed the boot cycle. <p>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.</p> The red Link Act LED (D2) is lit, which indicates a working Ethernet connection. If the red Duplex LED (D3) is lit, it indicates full-duplex activity. If the red 100 LED (D4) is lit, it indicates a working 100 MB Ethernet connection (100 MB network, only).

Ports	Model	Network LEDs
2	DeviceMaster RTS	<ul style="list-style-type: none"> The STATUS LED on the device is lit, indicating you have power and it has completed the boot cycle. <i>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.</i> If the LINK (green) LED is lit, it indicates a working Ethernet connection. If the ACT (yellow) LED flashes, it indicates network activity.
4 8 16	DeviceMaster PRO (8) DeviceMaster RTS† DeviceMaster Serial Hub (8)	<ul style="list-style-type: none"> The PWR LED on the front of the unit is lit, which indicates it has power and has completed the boot cycle. <i>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.</i> The red LNK/ACT LED is lit, which indicates a working Ethernet connection. If the red 100 LED is lit, it indicates a working 100 MB Ethernet connection (100 MB network, only).
16 32	DeviceMaster PRO (16) DeviceMaster RTS†† DeviceMaster Serial Hub (16)	<ul style="list-style-type: none"> The Status LED on the front of the unit is lit, which indicates it has power and has completed the boot cycle. <i>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.</i> The red LNK/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).
† External power supply.		
†† Internal 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 Control after obtaining a return material authorization (RMA) so that Control 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 www.angryip.org 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 Plus.

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 Plus 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 [Connecting Serial Devices](#) on Page 99 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.*

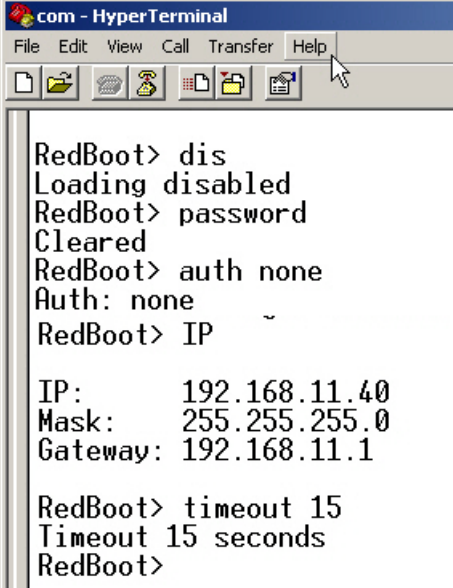
6. Enter **password** and press **Enter**, which clears the existing password.
7. Enter **auth none** and press **Enter**, which removes the authentication level.
8. If you do not know the IP address, enter **ip** and press **Enter**.
9. Enter **timeout 15** and press **Enter**, which sets a reasonable 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 Control for re-flashing.*

10. Connect the DeviceMaster directly to the PC/laptop running PortVision Plus.

Note: *If necessary, see [Installing PortVision Plus](#) on Page 35.*

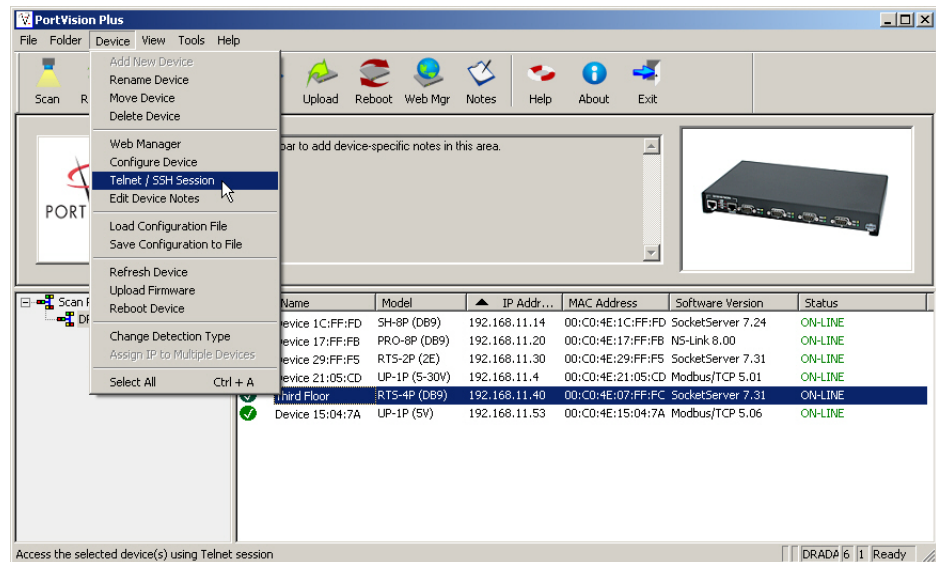
11. Open PortVision Plus.
12. Scan the network so that PortVision Plus discovers the DeviceMaster.
13. Highlight the DeviceMaster, click the **Device** menu, and then click **Telnet/SSH Session**.



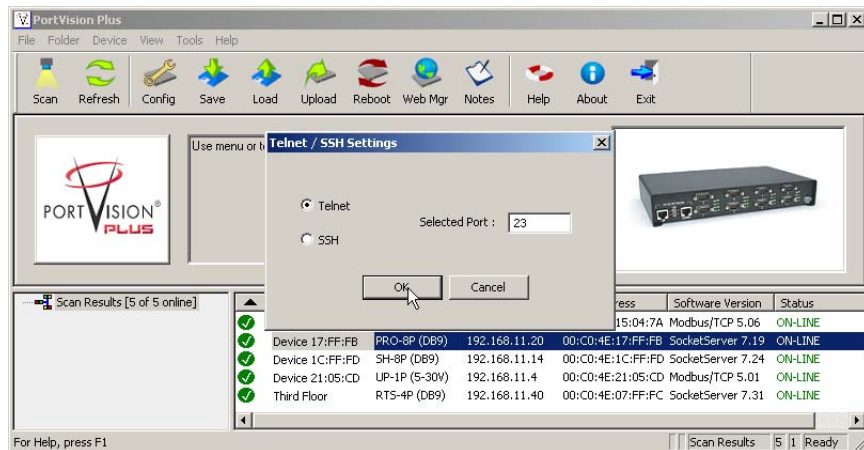
```

com - HyperTerminal
File Edit View Call Transfer Help
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>

```



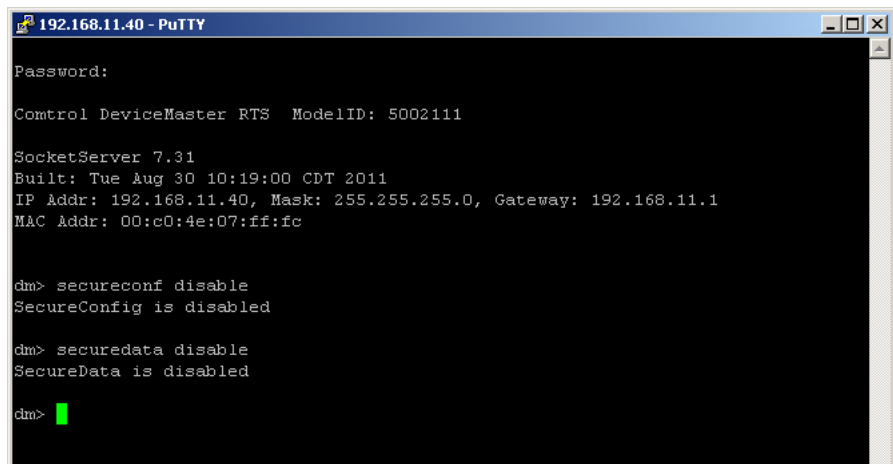
14. Click **Telnet**, leave Port 23 as the *Selected Port* and click **Ok**



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.

The EEPROM memory is programmed with a number of default values. The values that you can modified are shown in the following table.

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.*

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 [Establishing a Serial Connection](#) on Page 130 ([Steps 1](#) 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:

- [Telnet Access](#)
- [Serial Port Access](#) on Page 178
- [Web Server Access](#) on Page 178

Telnet Access

Use the following procedure to access the DeviceMaster configuration through telnet,

Note: To reset authentication, see [Serial Port Access](#) on Page 178 or use the [RedBoot Command Overview](#) on Page 139.

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 [Establishing a Serial Connection](#) on Page 130. 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 [Serial Port Access](#) on Page 178 or use the [RedBoot Command Overview](#) on Page 139.

To reset the password, see [Configuring Passwords](#) on Page 138 or [Telnet Access](#) on Page 177.

1. Open your web browser and enter the IP address of the DeviceMaster.
2. Click the **Configure Security** link:
 - 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 **Configure Email Messages** link:
 - 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**.
4. Return to the *Server Configuration* (home) page and click **Reboot**.
5. Click **Set configuration for all ports to factory default settings**.
6. Click **Yes: Reboot**.

7. Click the **Configure Network** link 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 will reboot. 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 12) 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.

Control Contact Information	
Downloads	ftp://ftp.comtrol.com/html_up_main.htm
Web site	http://www.comtrol.com
Phone	(763) 957-6000

