DEVICE•MASTER®
LT

User Guide

COMTROL®

Trademark Notices

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

Microsoft and Windows are registered trademarks of Microsoft Corporation.

HyperTerminal is a registered trademark of Hilgraeve, Inc.

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

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

Third Edition, March 20, 2017
Copyright © 2014 - 2017. Comtrol Corporation.
All Rights Reserved.

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

Document Number: 2000586 Rev. C

Table of Contents

Introduction

This section discusses the following topics:

DeviceMaster LT Port Usage

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

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

Installation Overview

DeviceMaster LT installation and configuration follows these steps:

1. Hardware installation.

   Power up the DeviceMaster LT. Technical Support suggests installing one DeviceMaster LT at a time to avoid configuration problems using *Hardware Installation* on Page 11.

2. Install PortVision DX.

   Comtrol recommends connecting the DeviceMaster LT to a PC or laptop running Windows and that you install PortVision DX for easy IP address configuration and firmware updates. See *PortVision DX Requirements* on Page 14 and refer to *Installing PortVision DX* on Page 15 to install PortVision DX.

3. Program the IP address.

   See *Configuring the Network Settings* on Page 19 for detailed configuration procedures.

4. If necessary, update SocketServer.

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

   a. Check the SocketServer version using *Checking the SocketServer Version* on Page 23 to determine the version on the DeviceMaster LT.

   b. If necessary, update SocketServer. See *Uploading SocketServer with PortVision DX* on Page 25.

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

5. Go to the appropriate overview or overviews for your installation:
   - NS-Link COM ports (or secure COM ports) - *NS-Link COM Port Driver Installation Overview* on Page 8
   - NS-Link tty ports - *NS-Link tty Port Installation Overview* on Page 8
   - TCP/IP socket ports - *TCP/IP Socket Port Installation Overview* on Page 9

NS-Link COM Port Driver Installation Overview

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

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

   See *Windows Installations* on Page 33 for an installation overview of the NS-Link driver for Windows operating systems.

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

   Note: *Although the download link displays win7 in the path, the driver supports multiple Windows operating systems (Page 14).*
3. Configure the COM ports using the *Comtrol Drivers Management Console*. See *Configuring the NS-Link Driver for Windows* on Page 38, which provides an overview of COM port configuration.
4. Configure device properties, you can refer to *Configuring COM Port Properties for Windows* on Page 42.
5. Optionally, you may need to configure one or more ports for socket mode. See *Socket Port Configuration* on Page 45 for information about configuring socket ports using the *Server Configuration* web page.
6. Connect the serial devices to the DeviceMaster LT. Refer to *Connecting Serial Devices* on Page 73 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 LT to run the NS-Link device driver for Linux operating systems.

1. After connecting the DeviceMaster LT, programming the IP address, and uploading the latest version of SocketServer, you are ready to install the driver.
2. Locate and unpackage the driver assembly http://downloads.comtrol.com/dev_mstr/rts/drivers/linux/.

   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 45 for information about configuring socket ports using the web interface (SocketServer/NS-Link).
4. Connect the serial devices to the DeviceMaster LT. Refer to *Connecting Serial Devices* on Page 73 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 LT socket ports.

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

   You can refer to the SocketServer help system or *Socket Port Configuration* on Page 45 for information for configuration procedures.
3. Connect the serial devices to the DeviceMaster LT. Refer to *Connecting Serial Devices* on Page 73 for cabling and connector information.

Locating Software and Documentation

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

- PortVision DX features a **Documentation** option that you can use to download and later, access documentation from within PortVision DX. See *Accessing DeviceMaster LT Documentation from PortVision DX* on Page 28 for more information.
- Check for and download the latest files using the links in the following table.

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

Software		Description/Documentation	File
Configuration Application	PortVision DX	Install on a Windows host to configure the IP address and upload SocketServer on the DeviceMaster LT.	⬇
SocketServer	SocketServer	This is the firmware that comes pre-installed on your DeviceMaster LT platform. You may need to upload the latest version of SocketServer before installing and configuring drivers or configuring sockets.	⬇
Device Driver	Linux	Install if you want tty ports. Refer to the **Readme** file compressed in the Linux driver assembly for driver configuration procedures.	⬇
	Windows Server 2008R2 through Windows 10	Install if you want COM ports. Refer to the *DeviceMaster Device Driver (NS-Link) User Guide*. for detailed information.	⬇

Software		Description/Documentation	File
Bootloader	Bootloader	The operating system that runs on the DeviceMaster LT hardware during the power on phase, which then loads SocketServer. Only update the Bootloader on your DeviceMaster LT if advised by Technical Support or the download site when checking for the latest SocketServer or device driver version.	🌐
This Guide	Any	You can check for the latest version of this *Guide*.	🌐

Hardware Installation

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

1. Place the DeviceMaster LT on a stable surface.

   Note: *Do not connect multiple units until you have changed the default IP address, see Initial Configuration on Page 13.*

2. Connect the DeviceMaster LT to the same Ethernet network segment as the host PC using either port labeled **10/100** using a standard Ethernet cable.
   The device is to be connect to Ethernet networks without routing outside the plant.

⚠ Caution

3. ***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 LT by connecting the AC power adapter to the DeviceMaster LT, the power cord to the power adapter, and plugging the power cord into a power source. See *External Power Supply Specifications* on Page 113 if you want to provide your own power supply.
   The device is intended to be used with a UL Listed power supply rated between 9 and 30 VDC, 400 mA minimum.

5. Verify that the **STAT** LED has completed the boot cycle and network connection for the DeviceMaster LT is functioning properly.
   Note: *The RX/TX LEDs cycle during a reboot.*

   - **STAT** (Status LED) - If the Status LED on the DeviceMaster LT is lit, it indicates the DeviceMaster LT has power and it has completed the boot cycle.
     The **STAT** 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.

   - Ethernet LEDs - The green LED indicates that a link has been established and the yellow LED indicates activity.

6. Go to *Initial Configuration* on Page 13 for default network settings and how to configure the DeviceMaster LT for use.

Initial Configuration

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

Optionally, you can use RedBoot to configure the network address, see *RedBoot Procedures* on Page 105.

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

- Install PortVision DX
- Configure the network address (Page 19)
- Check the SocketServer version on the DeviceMaster LT (Page 23)
- If necessary, download the latest version SocketServer and upload it into the DeviceMaster LT (Page 25)
- Organize how PortVision DX displays your Comtrol Ethernet attached products
- Access the latest documentation for your Comtrol Ethernet attached product

PortVision DX Overview

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

- DeviceMaster family
  - DM-2101, DM-2201, and DM-2304
  - DeviceMaster PRO
  - DeviceMaster RTS
  - DeviceMaster Serial Hub
  - DeviceMaster UP
- DeviceMaster LT
- IO-Link Master
- RocketLinx switches

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

PortVision DX Requirements

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

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

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

Configuring Security Settings and PortVision DX

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

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

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

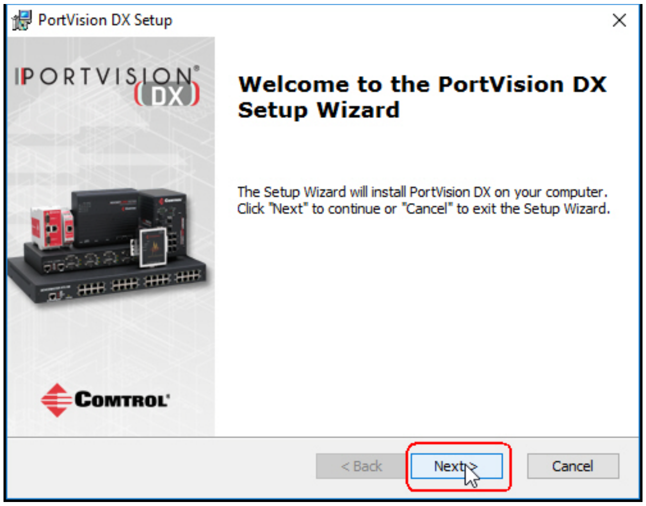
Installing PortVision DX

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

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

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

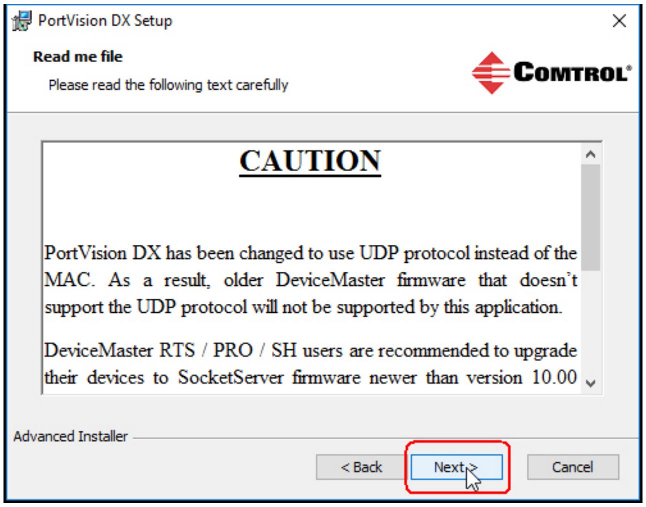
2. Execute the **PortVision_DX[*version*].msi** file.
3. Click **Next** on the *Welcome* screen.



Welcome to the PortVision DX Setup Wizard

The Setup Wizard will install PortVision DX on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

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



Read me file

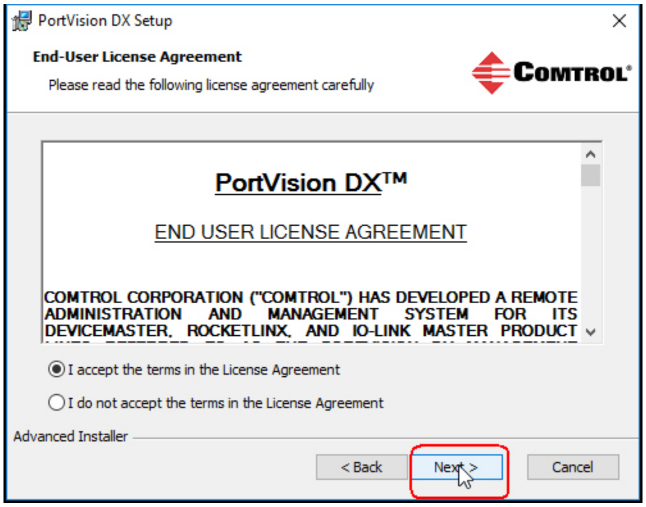
Please read the following text carefully

CAUTION

PortVision DX has been changed to use UDP protocol instead of the MAC. As a result, older DeviceMaster firmware that doesn't support the UDP protocol will not be supported by this application.

DeviceMaster RTS / PRO / SH users are recommended to upgrade their devices to SocketServer firmware newer than version 10.00

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



PortVision DX Setup

End-User License Agreement

Please read the following license agreement carefully

PortVision DX™

END USER LICENSE AGREEMENT

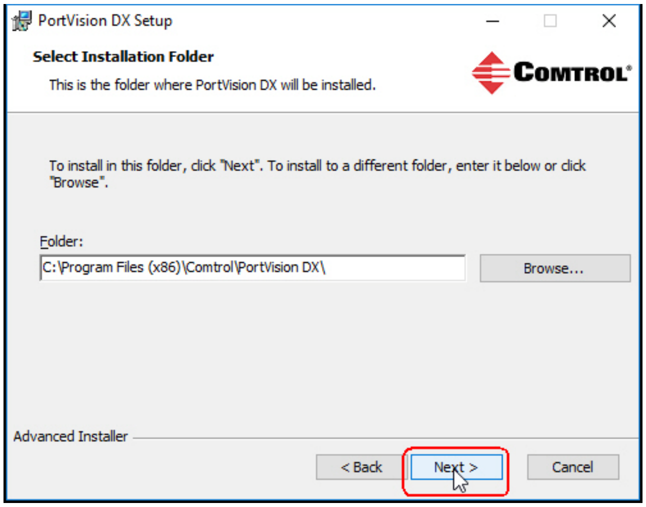
COMTROL CORPORATION ("COMTROL") HAS DEVELOPED A REMOTE ADMINISTRATION AND MANAGEMENT SYSTEM FOR ITS DEVICEMASTER, ROCKETLINX, AND IO-LINK MASTER PRODUCT

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

Advanced Installer

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



PortVision DX Setup

Select Installation Folder

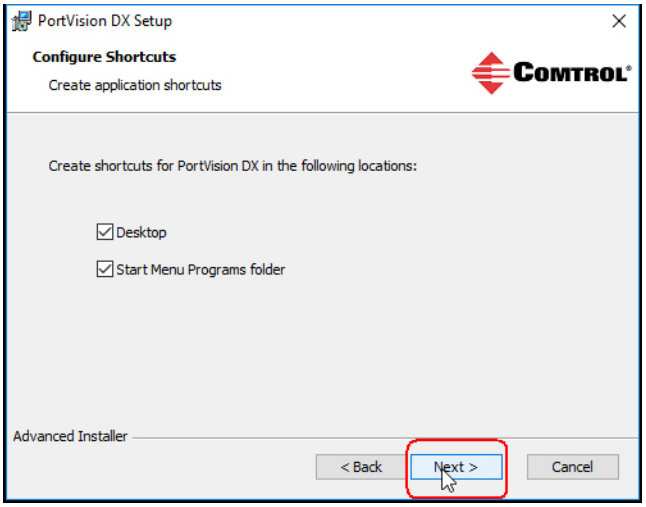
This is the folder where PortVision DX will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files (x86)\Comtrol\PortVision DX\

Advanced Installer

7. Click **Next** to configure the shortcuts.



PortVision DX Setup

Configure Shortcuts

Create application shortcuts

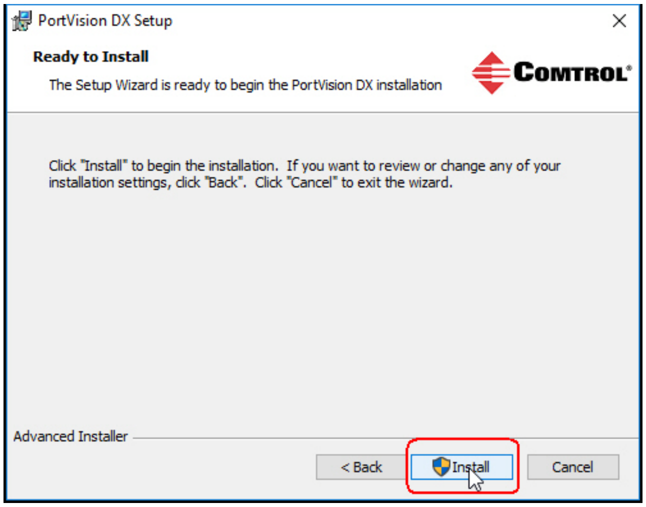
Create shortcuts for PortVision DX in the following locations:

☑ Desktop

☑ Start Menu Programs folder

Advanced Installer

8. Click **Install**.



PortVision DX Setup

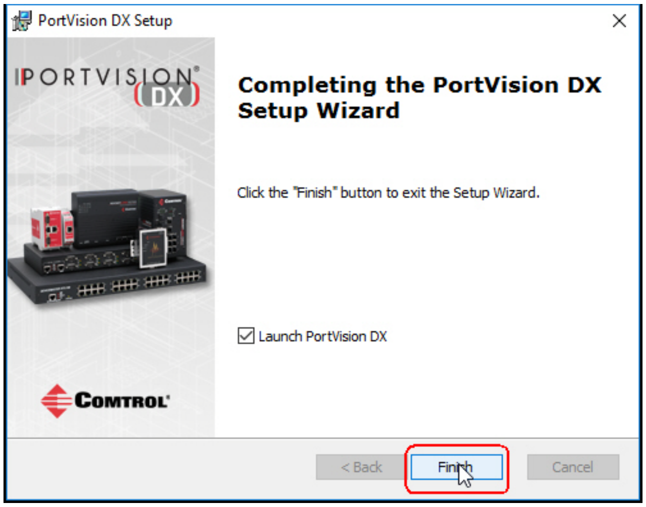
Ready to Install

The Setup Wizard is ready to begin the PortVision DX installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

9. Depending on the operating system, you may need to click **Yes** to the *Do you want to allow the following program to install software on this computer?* query.

10. Click **Launch PortVision DX** and **Finish** in the last installation screen.



PortVision DX Setup

Completing the PortVision DX Setup Wizard

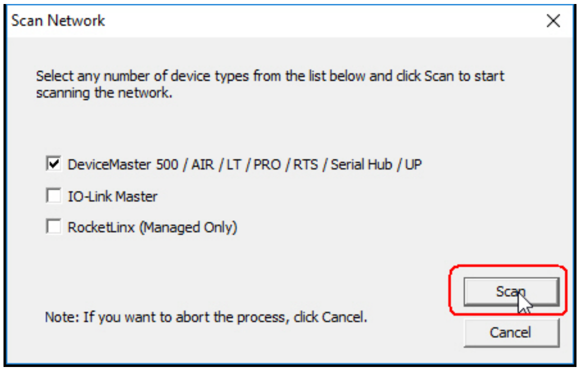
Click the "Finish" button to exit the Setup Wizard.

☑ Launch PortVision DX

11. Depending on the operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* query.

12. Select the Comtrol Ethernet attached products that you want to locate and then click **Scan**.

You can save time if you only scan for DeviceMasters.



Scan Network

Select any number of device types from the list below and click Scan to start scanning the network.

☑ DeviceMaster 500 / AIR / LT / PRO / RTS / Serial Hub / UP
□ IO-Link Master
□ RocketLinx (Managed Only)

Note: If you want to abort the process, click Cancel.

Note: *If the Comtrol Ethernet attached product is not on the local segment and it has been programmed with an IP address, it will be necessary to manually add the Comtrol Ethernet attached product to PortVision DX.*

13. Go to Step 6 in the next section, *Configuring the Network Settings*, to program the DeviceMaster LT network settings.

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

Configuring the Network Settings

Use the following procedure to change the default network settings on the DeviceMaster LT for your network.

Default Network Settings

IP address:
192.168.250.250

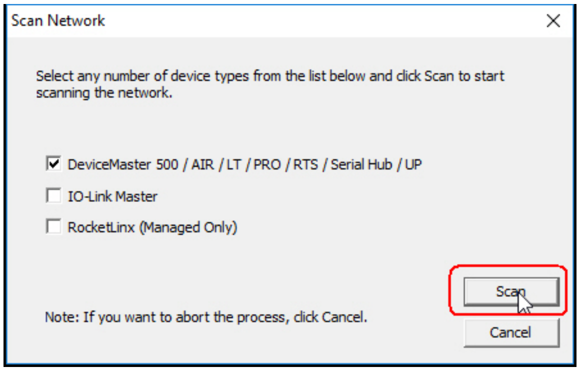
Subnet mask:
255.255.0.0

Gateway address:
192.168.250.1

Note: *Technical Support advises configuring one new DeviceMaster LT at a time to avoid device driver configuration problems. If you want to configure multiple DeviceMaster LTs using the* **Assign IP to Multiple Devices** *option, see Configuring Multiple DeviceMaster LTs Network Addresses on Page 79.*

The following procedure shows how to configure a single DeviceMaster LT connected to the same network segment as the Windows system. If the DeviceMaster LT is not on the same physical segment, you can add it manually using *Adding a New Device in PortVision DX* on Page 79.

1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 15).
2. Start PortVision DX using the **PortVision DX** desktop shortcut or from the **Start** button, click **All Programs > Comtrol > PortVision DX > PortVision DX**.
3. Depending on your operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* query.
4. Click the **Scan** button in the *Toolbar.*
5. Click **Scan** to locate the Comtrol Ethernet attached products including the DeviceMaster LT on the network.



Select any number of device types from the list below and click Scan to start scanning the network.

☑ DeviceMaster 500 / AIR / LT / PRO / RTS / Serial Hub / UP

☐ IO-Link Master

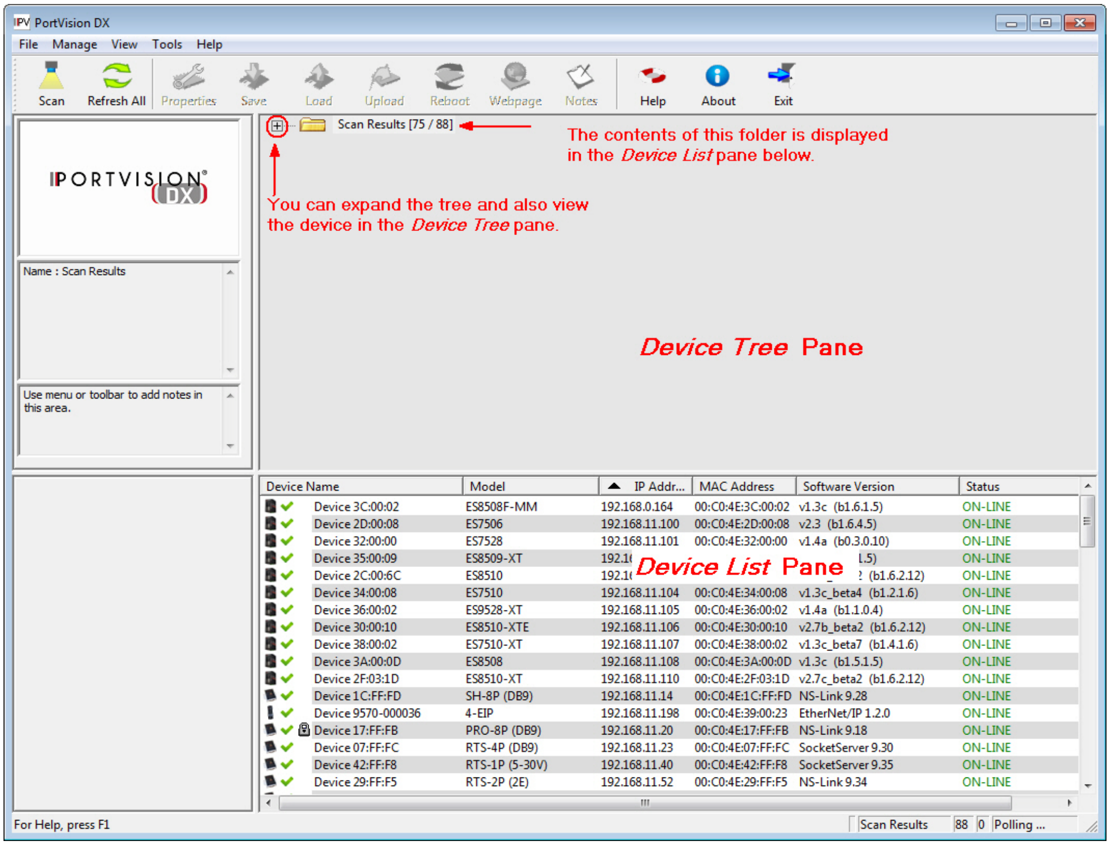
☐ RocketLinx (Managed Only)

Note: If you want to abort the process, click Cancel.

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

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

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



The contents of this folder is displayed in the *Device List* pane below.

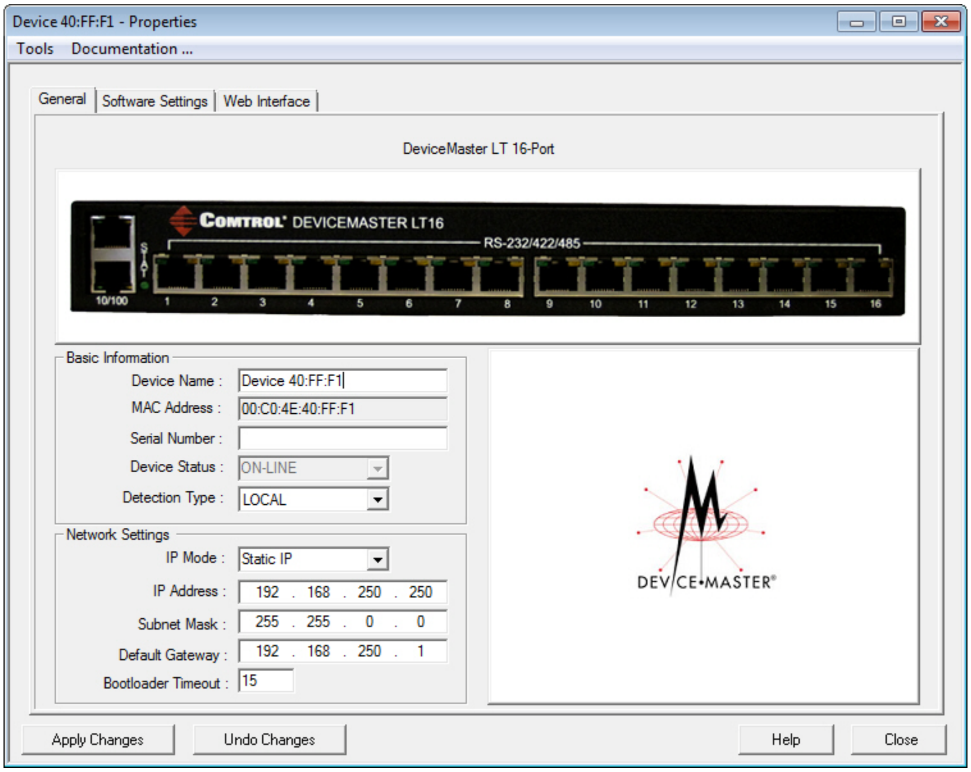
You can expand the tree and also view the device in the *Device Tree* pane.

Device Tree Pane

Device List Pane

Device Name	Model	IP Addr...	MAC Address	Software Version	Status
Device 3C:00:02	ES8508F-MM	192.168.0.164	00:C0:4E:3C:00:02	v1.3c (b1.6.1.5)	ON-LINE
Device 2D:00:08	ES7506	192.168.11.100	00:C0:4E:2D:00:08	v2.3 (b1.6.4.5)	ON-LINE
Device 32:00:00	ES7528	192.168.11.101	00:C0:4E:32:00:00	v1.4a (b0.3.0.10)	ON-LINE
Device 35:00:09	ES8509-XT	192.1		1.5)	ON-LINE
Device 2C:00:6C	ES8510	192.1		(b1.6.2.12)	ON-LINE
Device 34:00:08	ES7510	192.168.11.104	00:C0:4E:34:00:08	v1.3c_beta4 (b1.2.1.6)	ON-LINE
Device 36:00:02	ES9528-XT	192.168.11.105	00:C0:4E:36:00:02	v1.4a (b1.1.0.4)	ON-LINE
Device 30:00:10	ES8510-XTE	192.168.11.106	00:C0:4E:30:00:10	v2.7b_beta2 (b1.6.2.12)	ON-LINE
Device 38:00:02	ES7510-XT	192.168.11.107	00:C0:4E:38:00:02	v1.3c_beta7 (b1.4.1.6)	ON-LINE
Device 3A:00:0D	ES8508	192.168.11.108	00:C0:4E:3A:00:0D	v1.3c (b1.5.1.5)	ON-LINE
Device 2F:03:1D	ES8510-XT	192.168.11.110	00:C0:4E:2F:03:1D	v2.7c_beta2 (b1.6.2.12)	ON-LINE
Device 1C:FF:FD	SH-8P (DB9)	192.168.11.14	00:C0:4E:1C:FF:FD	NS-Link 9.28	ON-LINE
Device 9570-000036	4-EIP	192.168.11.198	00:C0:4E:39:00:23	EtherNet/IP 1.2.0	ON-LINE
Device 17:FF:FB	PRO-8P (DB9)	192.168.11.20	00:C0:4E:17:FF:FB	NS-Link 9.18	ON-LINE
Device 07:FF:FC	RTS-4P (DB9)	192.168.11.23	00:C0:4E:07:FF:FC	SocketServer 9.30	ON-LINE
Device 42:FF:F8	RTS-1P (5-30V)	192.168.11.40	00:C0:4E:42:FF:F8	SocketServer 9.35	ON-LINE
Device 29:FF:F5	RTS-2P (2E)	192.168.11.52	00:C0:4E:29:FF:F5	NS-Link 9.34	ON-LINE

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



DeviceMaster LT 16-Port

Basic Information

Device Name : Device 40:FF:F1

MAC Address : 00:C0:4E:40:FF:F1

Serial Number :

Device Status : ON-LINE

Detection Type : LOCAL

Network Settings

IP Mode : Static IP

IP Address : 192 . 168 . 250 . 250

Subnet Mask : 255 . 255 . 0 . 0

Default Gateway : 192 . 168 . 250 . 1

Bootloader Timeout : 15

Note: *The MAC address and Device Status fields are automatically populated and you cannot change those values.*

8. If necessary, you can change the **Detection Type**.
   - **REMOTE** means that the DeviceMaster LT is not connected to this segment of the network and it uses IP communications, not MAC communications.
   - **LOCAL** means that the DeviceMaster LT is on this local network segment and uses MAC communications. An IP address is not required but Technical support recommends using an IP address.
9. Change the DeviceMaster LT network properties as required for your site.
   - If you want to disable IP communications on the DeviceMaster LT, click **Disable IP**.
   - To use the DeviceMaster LT 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 LT in the DHCP server.
   - To program a static IP address, click **Static IP** and enter the appropriate values for your site.

   Note: *For additional information, open the PortVision DX Help system.*
10. Typically, the **Bootloader Timeout** value should be left to it's default value. In some situations, you may need to temporarily adjust the **Bootloader Timeout** to a higher value during a firmware update.

11. Click **Apply Changes** to update the network information on the DeviceMaster LT.

    Note: *If you are deploying multiple DeviceMaster LTs that share common values, you can save the configuration file and load that configuration onto other DeviceMaster LTs. See Using SocketServer Configuration Files on Page 81 for more information.*

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

Go to *Checking the SocketServer Version* on Page 23 to check the SocketServer version. You should update SocketServer firmware before any further configuration.

Checking the SocketServer Version

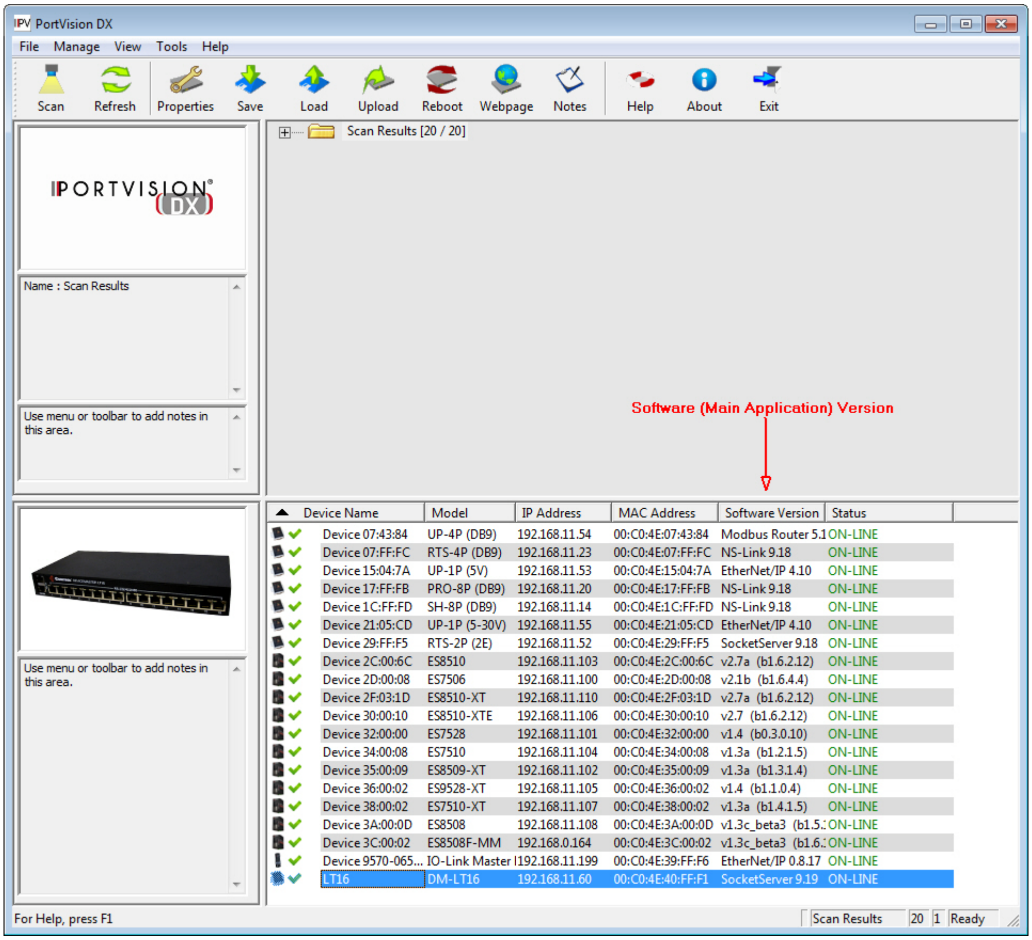
SocketServer refers to the web page that is integrated in the firmware that comes pre-installed on your DeviceMaster LT platform, which provides an interface to TCP/IP socket mode configuration and services. If you install an NS-Link device driver, an NS-Link version of SocketServer loads on the DeviceMaster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

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

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

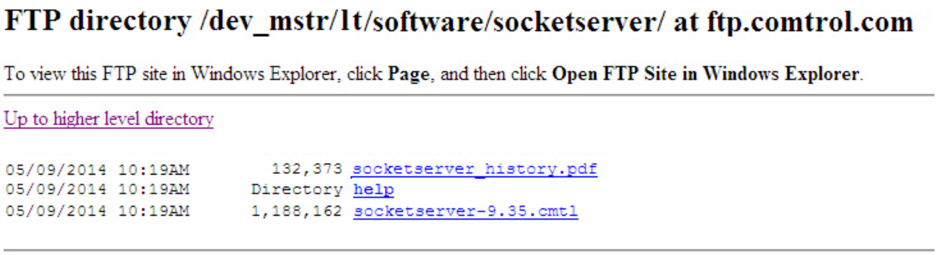
1. If necessary, open **PortVision DX > Comtrol > PortVision DX** or use the desktop shortcut and scan the network.

2. Check the SocketServer version number of the *Software Version* for the DeviceMaster LT.



Device Name	Model	IP Address	MAC Address	Software Version	Status
Device 07:43:84	UP-4P (DB9)	192.168.11.54	00:C0:4E:07:43:84	Modbus Router 5.1	ON-LINE
Device 07:FF:FC	RTS-4P (DB9)	192.168.11.23	00:C0:4E:07:FF:FC	NS-Link 9.18	ON-LINE
Device 15:04:7A	UP-1P (5V)	192.168.11.53	00:C0:4E:15:04:7A	EtherNet/IP 4.10	ON-LINE
Device 17:FF:FB	PRO-8P (DB9)	192.168.11.20	00:C0:4E:17:FF:FB	NS-Link 9.18	ON-LINE
Device 1C:FF:FD	SH-8P (DB9)	192.168.11.14	00:C0:4E:1C:FF:FD	NS-Link 9.18	ON-LINE
Device 21:05:CD	UP-1P (5-30V)	192.168.11.55	00:C0:4E:21:05:CD	EtherNet/IP 4.10	ON-LINE
Device 29:FF:F5	RTS-2P (2E)	192.168.11.52	00:C0:4E:29:FF:F5	SocketServer 9.18	ON-LINE
Device 2C:00:6C	ES8510	192.168.11.103	00:C0:4E:2C:00:6C	v2.7a (b1.6.2.12)	ON-LINE
Device 2D:00:08	ES7506	192.168.11.100	00:C0:4E:2D:00:08	v2.1b (b1.6.4.4)	ON-LINE
Device 2F:03:1D	ES8510-XT	192.168.11.110	00:C0:4E:2F:03:1D	v2.7a (b1.6.2.12)	ON-LINE
Device 30:00:10	ES8510-XTE	192.168.11.106	00:C0:4E:30:00:10	v2.7 (b1.6.2.12)	ON-LINE
Device 32:00:00	ES7528	192.168.11.101	00:C0:4E:32:00:00	v1.4 (b0.3.0.10)	ON-LINE
Device 34:00:08	ES7510	192.168.11.104	00:C0:4E:34:00:08	v1.3a (b1.2.1.5)	ON-LINE
Device 35:00:09	ES8509-XT	192.168.11.102	00:C0:4E:35:00:09	v1.3a (b1.3.1.4)	ON-LINE
Device 36:00:02	ES9528-XT	192.168.11.105	00:C0:4E:36:00:02	v1.4 (b1.1.0.4)	ON-LINE
Device 38:00:02	ES7510-XT	192.168.11.107	00:C0:4E:38:00:02	v1.3a (b1.4.1.5)	ON-LINE
Device 3A:00:0D	ES8508	192.168.11.108	00:C0:4E:3A:00:0D	v1.3c_beta3 (b1.5.:	ON-LINE
Device 3C:00:02	ES8508F-MM	192.168.0.164	00:C0:4E:3C:00:02	v1.3c_beta3 (b1.6.:	ON-LINE
Device 9570-065...	IO-Link Master I	192.168.11.199	00:C0:4E:39:FF:F6	EtherNet/IP 0.8.17	ON-LINE
LT16	DM-LT16	192.168.11.60	00:C0:4E:40:FF:F1	SocketServer 9.19	ON-LINE

3. Check the Comtrol ftp site to see if a later version is available by accessing the ftp subdirectory that contains the latest version of SocketServer: ftp://ftp.comtrol.com/dev_mstr/LT/software/socketserver.



FTP directory /dev_mstr/lt/software/socketserver/ at ftp.comtrol.com

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

Up to higher level directory

```
05/09/2014 10:19AM       132,373 socketserver_history.pdf
05/09/2014 10:19AM     Directory help
05/09/2014 10:19AM     1,188,162 socketserver-9.35.cmtl
```

4. If the version on the web site is later than the version on the DeviceMaster LT, download the file, and then go to *Uploading SocketServer with PortVision DX* on Page 25.

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

Uploading SocketServer with PortVision DX

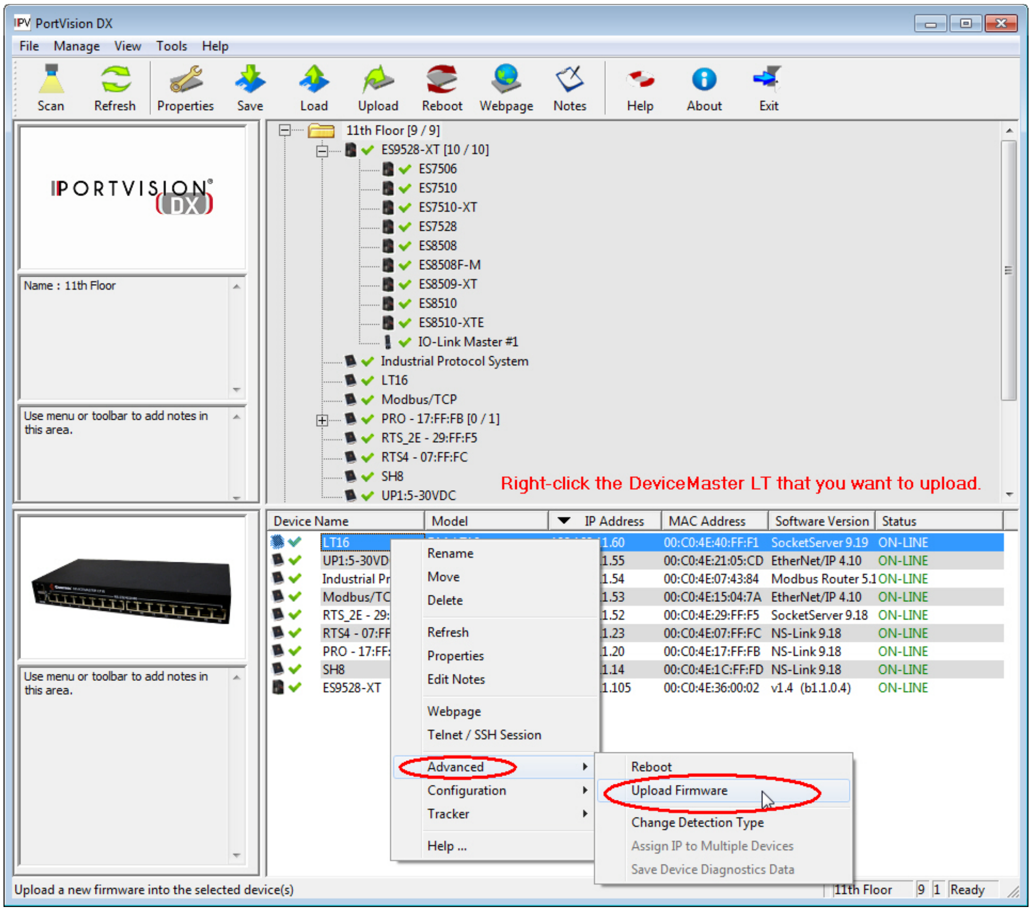
Use this section to upload a newer version of SocketServer on the DeviceMaster LT using PortVision DX. Technical Support recommends updating SocketServer before any further configuration to avoid configuration problems.

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

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

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

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

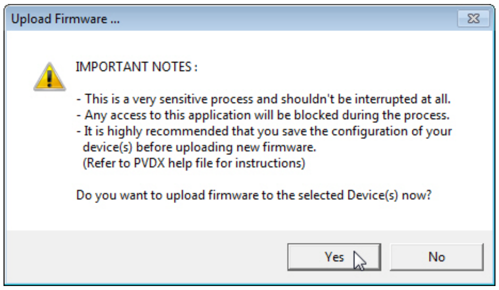


Right-click the DeviceMaster LT that you want to upload.

Device Name	Model	IP Address	MAC Address	Software Version	Status
LT16		1.60	00:C0:4E:40:FF:F1	SocketServer 9.19	ON-LINE
UP1:5-30VD		1.55	00:C0:4E:21:05:CD	EtherNet/IP 4.10	ON-LINE
Industrial Pr		1.54	00:C0:4E:07:43:84	Modbus Router 5.1	ON-LINE
Modbus/TC		1.53	00:C0:4E:15:04:7A	EtherNet/IP 4.10	ON-LINE
RTS_2E - 29:		1.52	00:C0:4E:29:FF:F5	SocketServer 9.18	ON-LINE
RTS4 - 07:FF		1.23	00:C0:4E:07:FF:FC	NS-Link 9.18	ON-LINE
PRO - 17:FF:		1.20	00:C0:4E:17:FF:FB	NS-Link 9.18	ON-LINE
SH8		1.14	00:C0:4E:1C:FF:FD	NS-Link 9.18	ON-LINE
ES9528-XT		1.105	00:C0:4E:36:00:02	v1.4 (b1.1.0.4)	ON-LINE

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

4. Click **Yes** to the *Upload Firmware* message that warns you that this is a sensitive process. It may take a few moments for the firmware to upload onto the DeviceMaster LT. The DeviceMaster LT reboots itself during the upload process.



IMPORTANT NOTES :

- This is a very sensitive process and shouldn't be interrupted at all.
- Any access to this application will be blocked during the process.
- It is highly recommended that you save the configuration of your device(s) before uploading new firmware. (Refer to PVDX help file for instructions)

Do you want to upload firmware to the selected Device(s) now?

5. Click **Ok** to the advisory message about waiting to use the device until the status reads **ON-LINE**. In the next polling cycle, PortVision DX updates the *Device List* pane and displays the new SocketServer version or right-click the DeviceMaster LT and click **Refresh**.
6. If the upload fails, reset the Bootloader timeout to 60 seconds and then repeat Steps 3 through 5. For procedures, see *Changing the Bootloader Timeout* on Page 89.

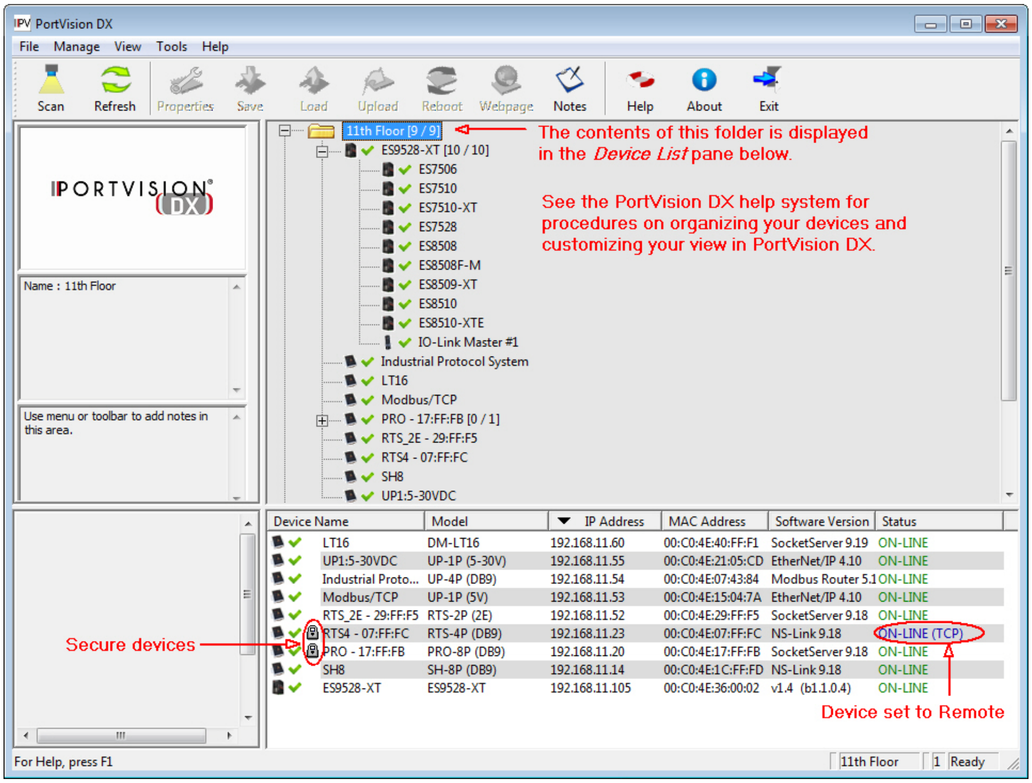
You are now ready to continue the installation and configuration process.

- *Device Driver (NS-Link) Installation* on Page 31
- *Socket Port Configuration* on Page 45

Customizing PortVision DX

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

The following illustrates how you can customize your view.



Name : 11th Floor

Use menu or toolbar to add notes in this area.

The contents of this folder is displayed in the *Device List* pane below.

See the PortVision DX help system for procedures on organizing your devices and customizing your view in PortVision DX.

Device Name	Model	IP Address	MAC Address	Software Version	Status
LT16	DM-LT16	192.168.11.60	00:C0:4E:40:FF:F1	SocketServer 9.19	ON-LINE
UP1:5-30VDC	UP-1P (5-30V)	192.168.11.55	00:C0:4E:21:05:CD	EtherNet/IP 4.10	ON-LINE
Industrial Proto...	UP-4P (DB9)	192.168.11.54	00:C0:4E:07:43:84	Modbus Router 5.1	ON-LINE
Modbus/TCP	UP-1P (5V)	192.168.11.53	00:C0:4E:15:04:7A	EtherNet/IP 4.10	ON-LINE
RTS_2E - 29:FF:F5	RTS-2P (2E)	192.168.11.52	00:C0:4E:29:FF:F5	SocketServer 9.18	ON-LINE
RTS4 - 07:FF:FC	RTS-4P (DB9)	192.168.11.23	00:C0:4E:07:FF:FC	NS-Link 9.18	ON-LINE (TCP)
PRO - 17:FF:FB	PRO-8P (DB9)	192.168.11.20	00:C0:4E:17:FF:FB	SocketServer 9.18	ON-LINE
SH8	SH-8P (DB9)	192.168.11.14	00:C0:4E:1C:FF:FD	NS-Link 9.18	ON-LINE
ES9528-XT	ES9528-XT	192.168.11.105	00:C0:4E:36:00:02	v1.4 (b1.1.0.4)	ON-LINE

Secure devices

Device set to Remote

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

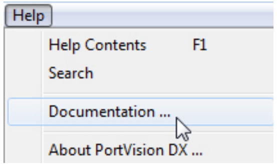
Accessing DeviceMaster LT Documentation from PortVision DX

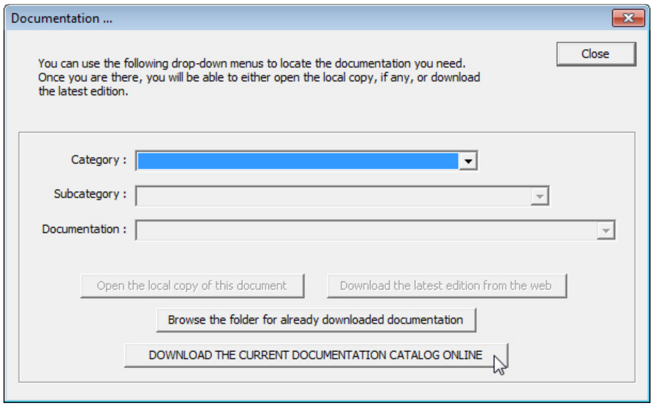
You can use this procedure in PortVision DX to download and open the previously downloaded documents for the DeviceMaster LT. You can also check to see if you have the latest version of the documentation using PortVision DX.

How to Download Documentation

Use this procedure to initially download a document or documents.

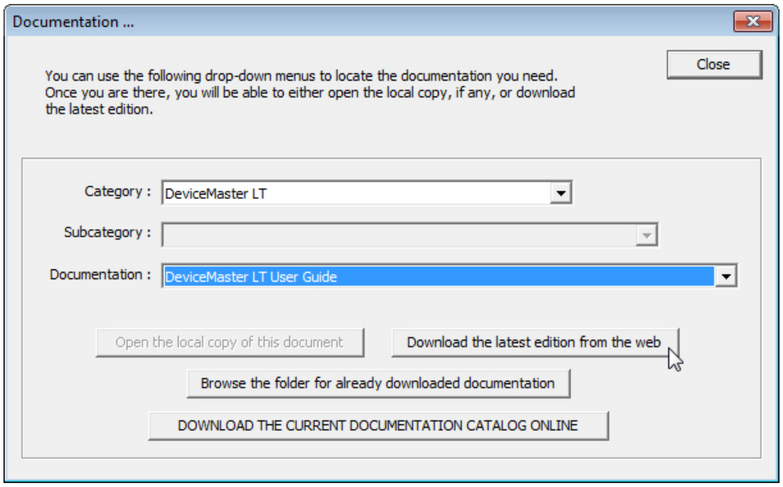
1. If necessary, open PortVision DX: **Start > Comtrol > PortVision DX** or use the desktop shortcut.
2. Click **Help > Documentation**.
3. Optionally, click the **DOWNLOAD THE CURRENT DOCUMENTATION CATALOG ONLINE** button to make sure that the latest documentation is available to PortVision DX.




Documentation ...
Close
Category :
Subcategory :
Documentation :
Open the local copy of this document
Download the latest edition from the web
Browse the folder for already downloaded documentation
DOWNLOAD THE CURRENT DOCUMENTATION CATALOG ONLINE

You can use the following drop-down menus to locate the documentation you need. Once you are there, you will be able to either open the local copy, if any, or download the latest edition.

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


Documentation ...
Close
Subcategory :
Open the local copy of this document
Download the latest edition from the web
Browse the folder for already downloaded documentation
DOWNLOAD THE CURRENT DOCUMENTATION CATALOG ONLINE

You can use the following drop-down menus to locate the documentation you need. Once you are there, you will be able to either open the local copy, if any, or download the latest edition.

Category : DeviceMaster LT

Documentation : DeviceMaster LT User Guide

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

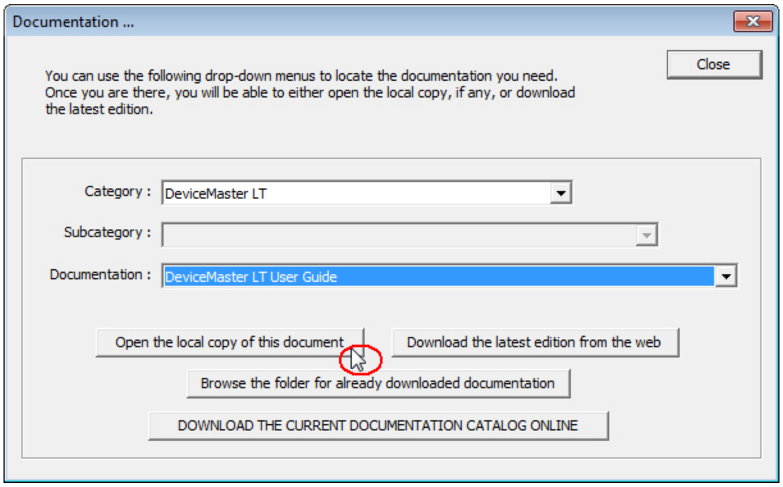
7. Click **Close** if you have downloaded all of the documents that you wanted.

How to Open Previously Downloaded Documents

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

Note: *Optionally, you can browse to the* **Program Files (x86) > Comtrol > PortVision DX > Docs** *subdirectory and open the document.*

1. If necessary, open PortVision DX: **Start > Comtrol > PortVision DX** or use the desktop shortcut.
2. Click **Help > Documentation**.
3. Click the **Open the local copy of the document** button to view the document.



Documentation ...

You can use the following drop-down menus to locate the documentation you need. Once you are there, you will be able to either open the local copy, if any, or download the latest edition.

Category : DeviceMaster LT

Subcategory :

Documentation : DeviceMaster LT User Guide

Close
Open the local copy of this document
Download the latest edition from the web
Browse the folder for already downloaded documentation
DOWNLOAD THE CURRENT DOCUMENTATION CATALOG ONLINE

Note: *If the document fails to open, it may be that your browser has been disabled. You can still access the document by clicking the* **Browse the folder for already downloaded documentation** *button and opening the document with your custom browser.*

4. Click **Close** in the *Documentation...* popup, unless you want to open or download other documents.

Device Driver (NS-Link) Installation

This section discusses the following topics:

- *Linux Installations* on Page 32
- *Windows Installations* on Page 33

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:

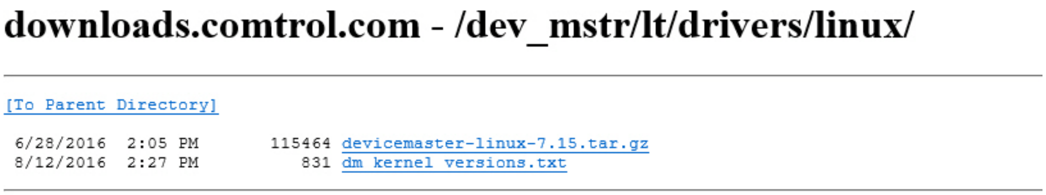
- The DeviceMaster LT is connected to the network and powered on (*Hardware Installation* on Page 11).
- The network information has been configured in the DeviceMaster LT (*Configuring the Network Settings* on Page 19).
- Checked to see if the latest version of SocketServer resides on the DeviceMaster LT (*Checking the SocketServer Version* on Page 23 using PortVision DX or you can open your browser, enter the DeviceMaster LT IP address to view the version on the *Server Status* page
- If necessary, uploaded the latest version of SocketServer (*Uploading SocketServer with PortVision DX* on Page 25.

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

After NS-Link driver installation and configuration, the same ports can be configured as TCP/IP sockets using an NS-Link version of the SocketServer web page (*Socket Port Configuration* on Page 45).

Linux Installations

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



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

```
[To Parent Directory]

 6/28/2016  2:05 PM       115464 devicemaster-linux-7.15.tar.gz
 8/12/2016  2:27 PM          831 dm kernel versions.txt
```

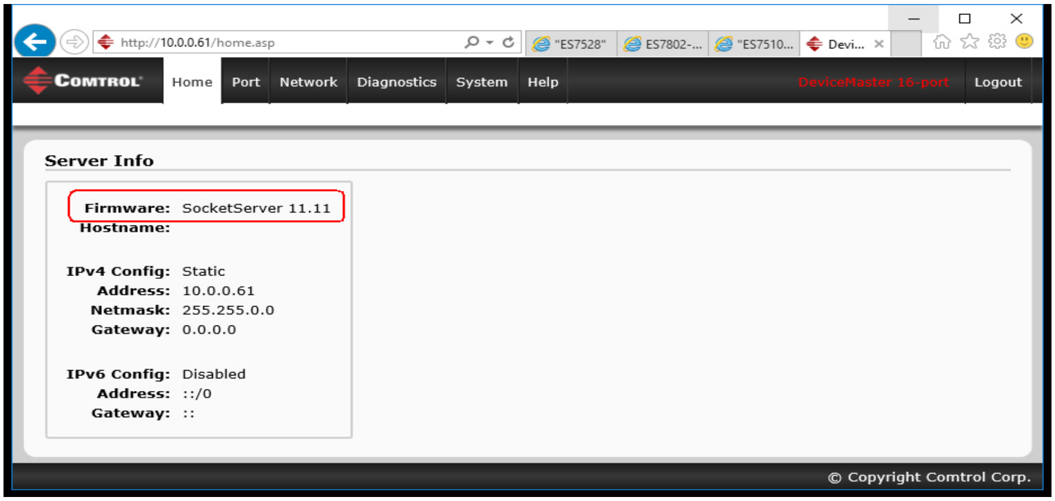
Refer to the **README** file packaged with the Linux driver for driver installation and configuration procedures.

Before you install the Linux NS-Link device driver:

1. Make sure that you have programmed an appropriate network address into the DeviceMaster LT.
2. Make sure that you verify that you have the latest version of SocketServer loaded on the DeviceMaster LT.

   If you do not want to install PortVision DX (Page 15) 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 LT.



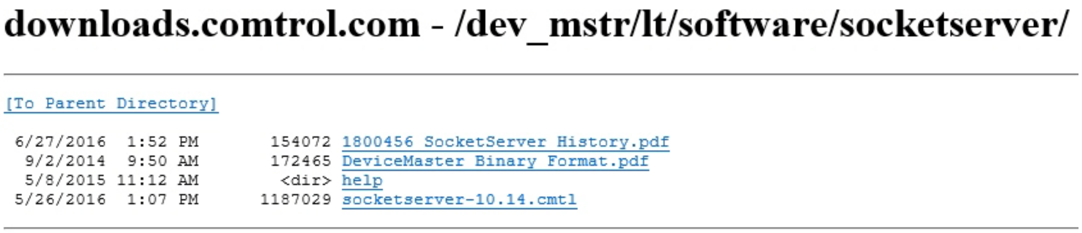
Server Info

Firmware: SocketServer 11.11
Hostname:

IPv4 Config: Static
Address: 10.0.0.61
Netmask: 255.255.0.0
Gateway: 0.0.0.0

IPv6 Config: Disabled
Address: ::/0
Gateway: ::

   b. Check the download site for the latest version: http://downloads.comtrol.com/dev_mstr/LT/software/SocketServer.



downloads.comtrol.com - /dev_mstr/lt/software/socketserver/

```
[To Parent Directory]

 6/27/2016  1:52 PM       154072 1800456 SocketServer History.pdf
  9/2/2014  9:50 AM       172465 DeviceMaster Binary Format.pdf
  5/8/2015 11:12 AM        <dir> help
 5/26/2016  1:07 PM      1187029 socketserver-10.14.cmtl
```

c. If necessary, download the latest version.

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

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

Windows Installations

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

Supported Operating Systems

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

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

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

Installation Overview for Windows

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

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

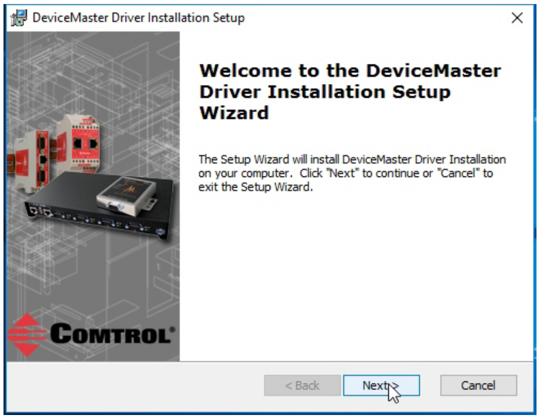
NS-Link for Windows Installation

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

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

   Note: *Although the download link displays win7 in the path, the driver supports the previously listed Windows operating systems.*

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

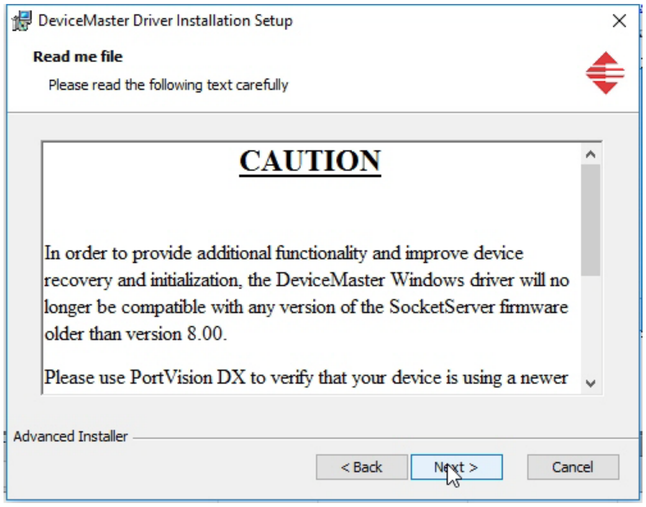


DeviceMaster Driver Installation Setup

Welcome to the DeviceMaster Driver Installation Setup Wizard

The Setup Wizard will install DeviceMaster Driver Installation on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

3. If included in this driver version, read the caution or notice:



DeviceMaster Driver Installation Setup

Read me file

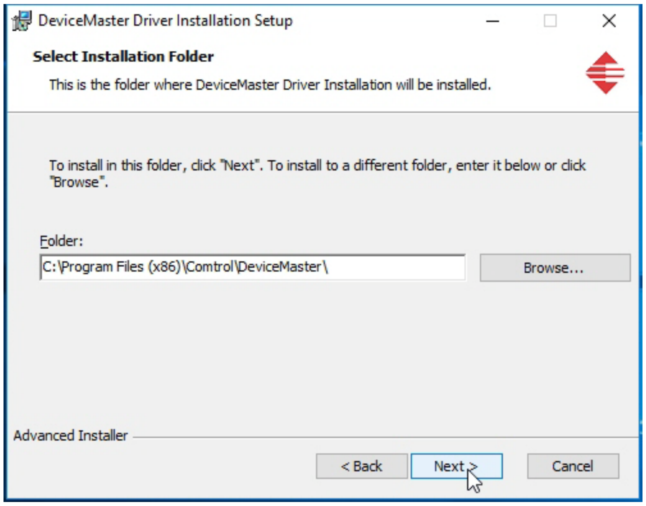
Please read the following text carefully

CAUTION

In order to provide additional functionality and improve device recovery and initialization, the DeviceMaster Windows driver will no longer be compatible with any version of the SocketServer firmware older than version 8.00.

Please use PortVision DX to verify that your device is using a newer

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



DeviceMaster Driver Installation Setup

Select Installation Folder

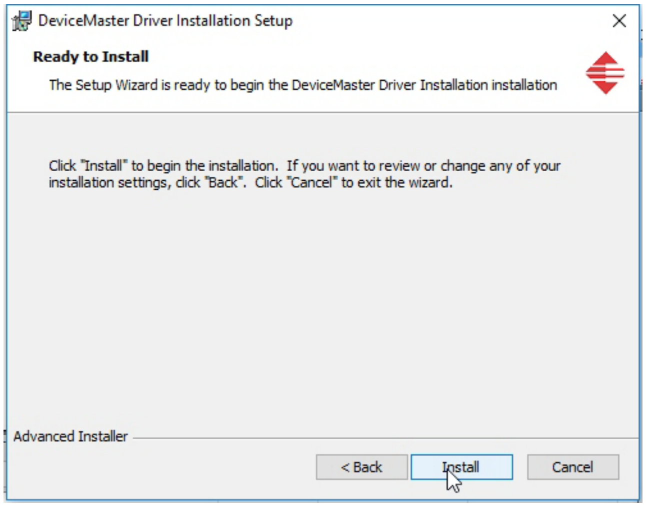
This is the folder where DeviceMaster Driver Installation will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder:

C:\Program Files (x86)\Comtrol\DeviceMaster\

5. Click **Install**



DeviceMaster Driver Installation Setup

Ready to Install

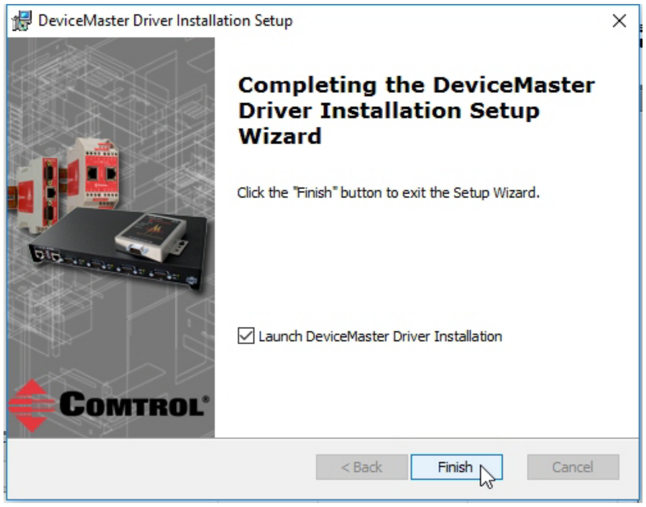
The Setup Wizard is ready to begin the DeviceMaster Driver Installation installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

6. Leave the **Launch DeviceMaster Driver Installation** box checked.

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

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



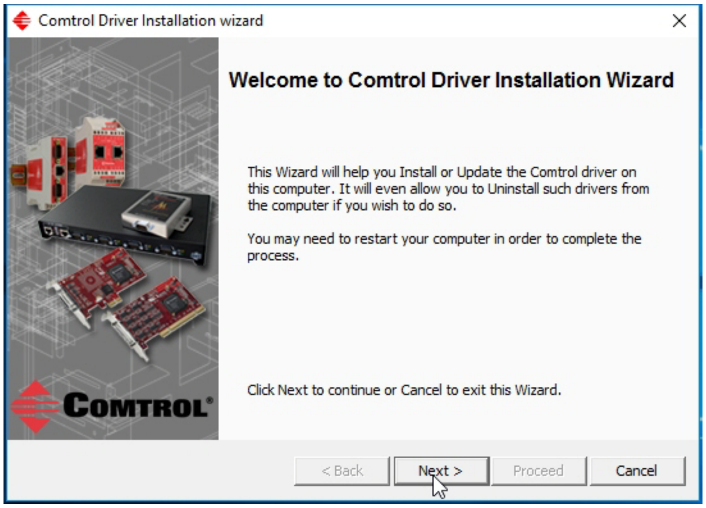
DeviceMaster Driver Installation Setup

Completing the DeviceMaster Driver Installation Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

☑ Launch DeviceMaster Driver Installation

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



Comtrol Driver Installation wizard

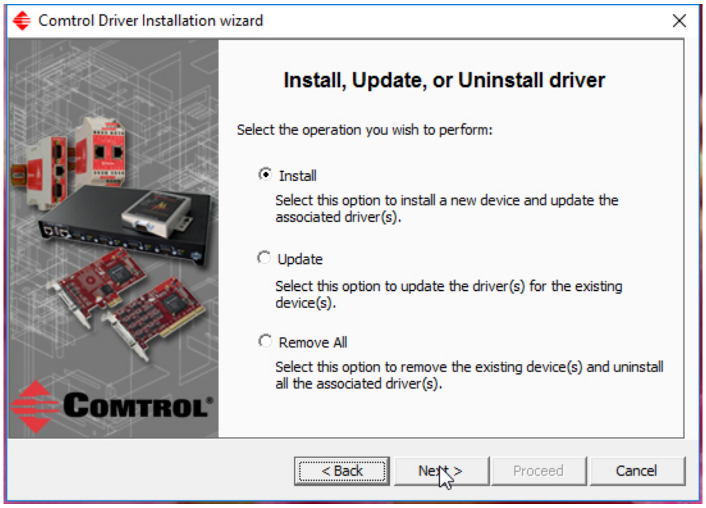
Welcome to Comtrol Driver Installation Wizard

This Wizard will help you Install or Update the Comtrol driver on this computer. It will even allow you to Uninstall such drivers from the computer if you wish to do so.

You may need to restart your computer in order to complete the process.

Click Next to continue or Cancel to exit this Wizard.

9. Click **Install** and **Next**.



Comtrol Driver Installation wizard

Install, Update, or Uninstall driver

Select the operation you wish to perform:

● Install

Select this option to install a new device and update the associated driver(s).

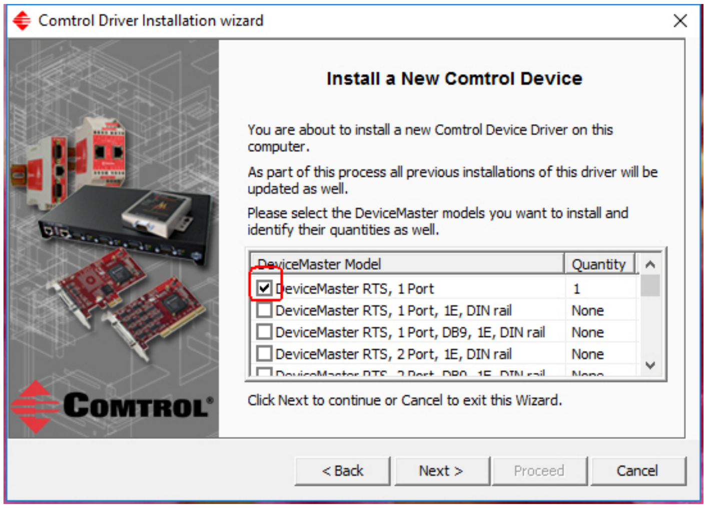
○ Update

Select this option to update the driver(s) for the existing device(s).

○ Remove All

Select this option to remove the existing device(s) and uninstall all the associated driver(s).

10. Select the DeviceMaster LT from the list.



Comtrol Driver Installation wizard

Install a New Comtrol Device

You are about to install a new Comtrol Device Driver on this computer.

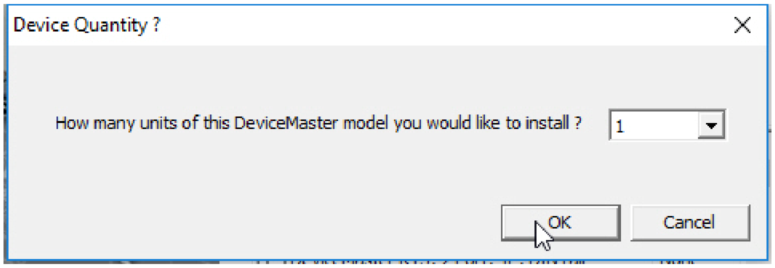
As part of this process all previous installations of this driver will be updated as well.

Please select the DeviceMaster models you want to install and identify their quantities as well.

DeviceMaster Model	Quantity
☑ DeviceMaster RTS, 1 Port	1
□ DeviceMaster RTS, 1 Port, 1E, DIN rail	None
□ DeviceMaster RTS, 1 Port, DB9, 1E, DIN rail	None
□ DeviceMaster RTS, 2 Port, 1E, DIN rail	None

Click Next to continue or Cancel to exit this Wizard.

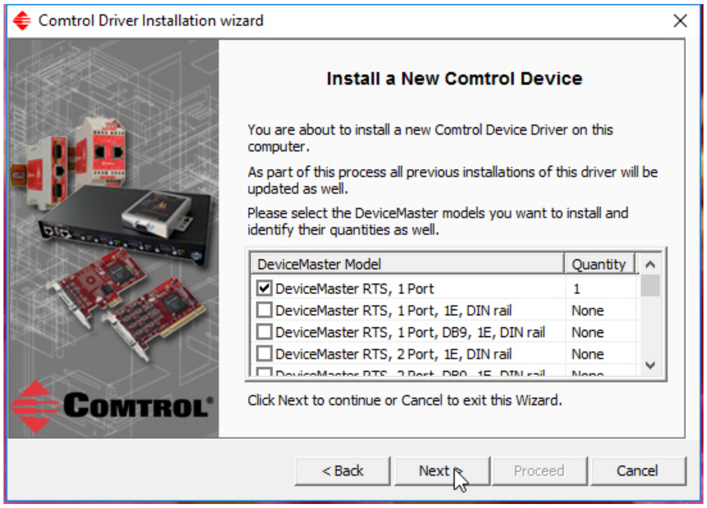
11. Enter the quantity of this DeviceMaster LT that you want to install and click **Ok**.



Device Quantity ?

How many units of this DeviceMaster model you would like to install ? 1

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



Comtrol Driver Installation wizard

Install a New Comtrol Device

You are about to install a new Comtrol Device Driver on this computer.

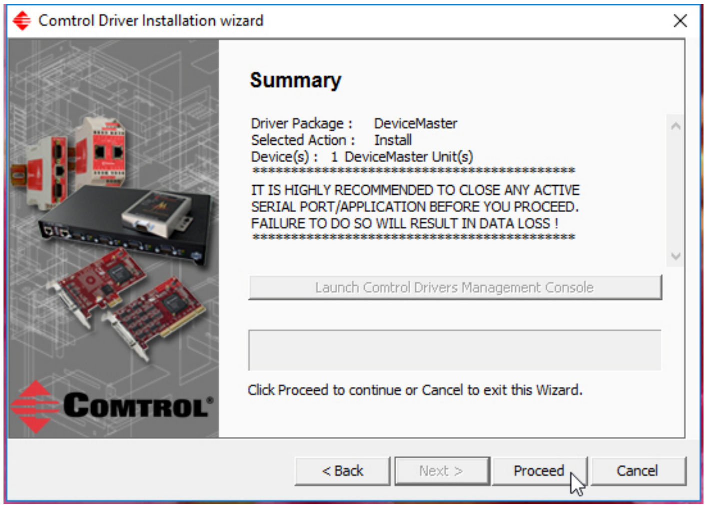
As part of this process all previous installations of this driver will be updated as well.

Please select the DeviceMaster models you want to install and identify their quantities as well.

DeviceMaster Model	Quantity
☑ DeviceMaster RTS, 1 Port	1
□ DeviceMaster RTS, 1 Port, 1E, DIN rail	None
□ DeviceMaster RTS, 1 Port, DB9, 1E, DIN rail	None
□ DeviceMaster RTS, 2 Port, 1E, DIN rail	None

Click Next to continue or Cancel to exit this Wizard.

13. Click **Proceed**.



Comtrol Driver Installation wizard

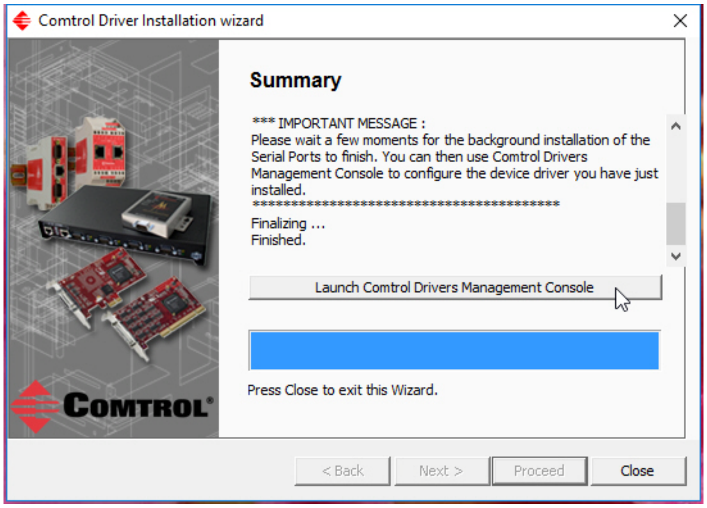
Summary

Driver Package : DeviceMaster
Selected Action : Install
Device(s) : 1 DeviceMaster Unit(s)
****
IT IS HIGHLY RECOMMENDED TO CLOSE ANY ACTIVE SERIAL PORT/APPLICATION BEFORE YOU PROCEED. FAILURE TO DO SO WILL RESULT IN DATA LOSS !
****

Click Proceed to continue or Cancel to exit this Wizard.

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

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



Comtrol Driver Installation wizard

Summary

*** IMPORTANT MESSAGE :
Please wait a few moments for the background installation of the Serial Ports to finish. You can then use Comtrol Drivers Management Console to configure the device driver you have just installed.
****
Finalizing ...
Finished.

Press Close to exit this Wizard.

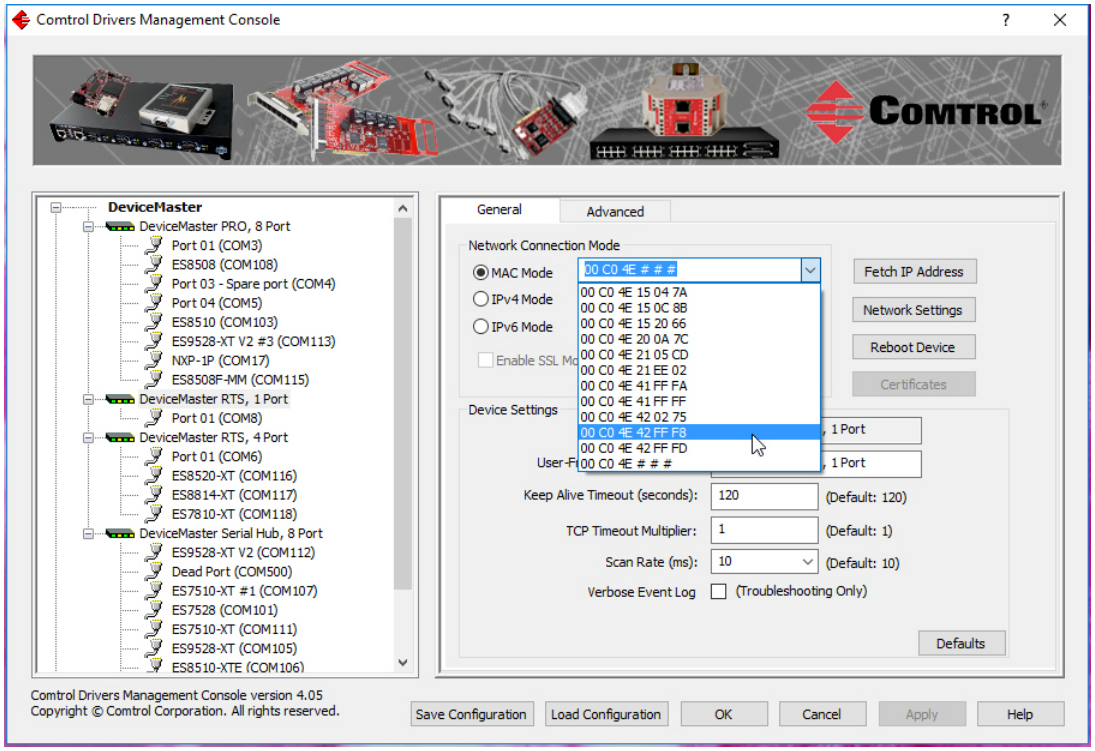
15. Go to the next subsection for NS-Link driver configuration procedures.

Configuring the NS-Link Driver for Windows

This subsection provides a configuration overview for the NS-Link driver. For detailed information or if the DeviceMaster LT 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 download site.

The DeviceMaster LT 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 *Comtrol Drivers Management Console* using the desktop shortcut or under the start menu **> Comtrol > DeviceMaster Driver Management Console**.
2. Highlight the *Device Name* of the DeviceMaster LT 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 LT. If you programmed the IP address using PortVision DX, the IP address displays in the **IP Mode** text box after you select the MAC address.



Network Connection Mode

● MAC Mode 00 C0 4E # # #

○ IPv4 Mode

○ IPv6 Mode

□ Enable SSL Mo

00 C0 4E 15 04 7A
00 C0 4E 15 0C 8B
00 C0 4E 15 20 66
00 C0 4E 20 0A 7C
00 C0 4E 21 05 CD
00 C0 4E 21 EE 02
00 C0 4E 41 FF FA
00 C0 4E 41 FF FF
00 C0 4E 42 02 75
00 C0 4E 42 FF F8
00 C0 4E 42 FF FD
00 C0 4E # # #

Device Settings

, 1 Port

User-F , 1 Port

Keep Alive Timeout (seconds): 120 (Default: 120)

TCP Timeout Multiplier: 1 (Default: 1)

Scan Rate (ms): 10 (Default: 10)

Verbose Event Log □ (Troubleshooting Only)

Comtrol Drivers Management Console version 4.05
Copyright © Comtrol Corporation. All rights reserved.

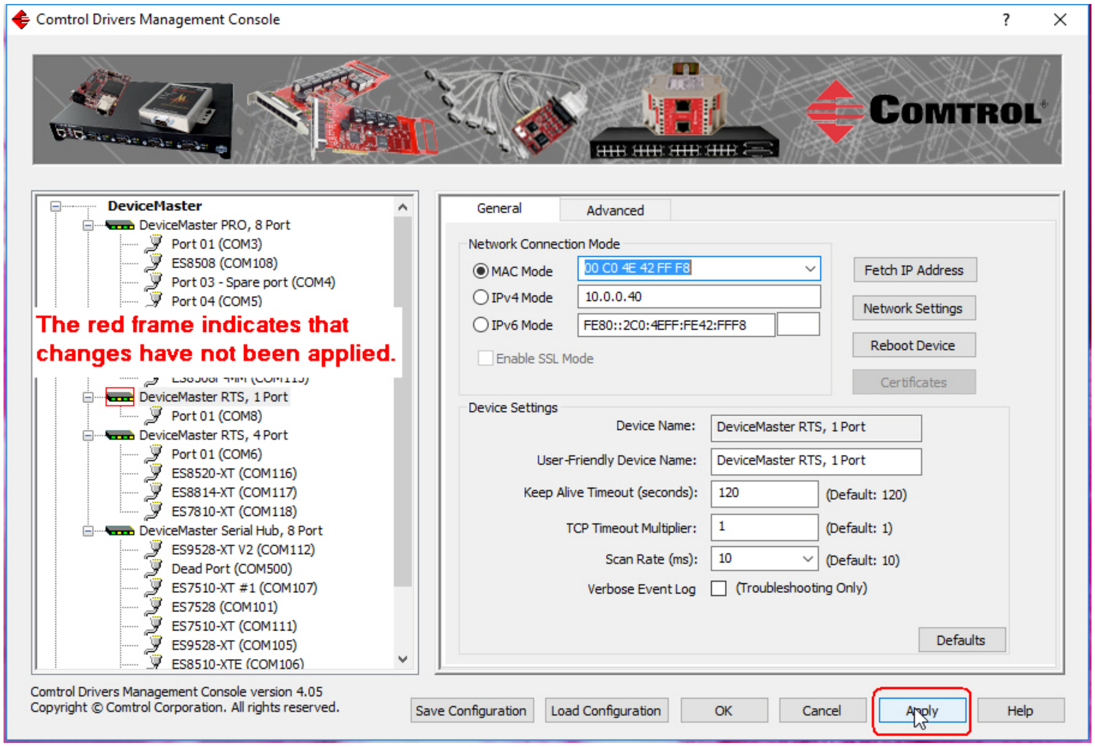
Note: *If you enter the MAC address, make sure that you use the correct format:* **00 C0 4E xx xx xx**. *A space must separate each pair of digits. The MAC address is located on a label on the DeviceMaster LT or you can view it using PortVision DX.*

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

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

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

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



Comtrol Drivers Management Console

- DeviceMaster
  - DeviceMaster PRO, 8 Port
    - Port 01 (COM3)
    - ES8508 (COM108)
    - Port 03 - Spare port (COM4)
    - Port 04 (COM5)
  - DeviceMaster RTS, 1 Port
    - Port 01 (COM8)
  - DeviceMaster RTS, 4 Port
    - Port 01 (COM6)
    - ES8520-XT (COM116)
    - ES8814-XT (COM117)
    - ES7810-XT (COM118)
  - DeviceMaster Serial Hub, 8 Port
    - ES9528-XT V2 (COM112)
    - Dead Port (COM500)
    - ES7510-XT #1 (COM107)
    - ES7528 (COM101)
    - ES7510-XT (COM111)
    - ES9528-XT (COM105)
    - ES8510-XTE (COM106)

The red frame indicates that changes have not been applied.

General | Advanced

Network Connection Mode

- ● MAC Mode: 00 C0 4E 42 FF F8
- ○ IPv4 Mode: 10.0.0.40
- ○ IPv6 Mode: FE80::2C0:4EFF:FE42:FFF8
- □ Enable SSL Mode

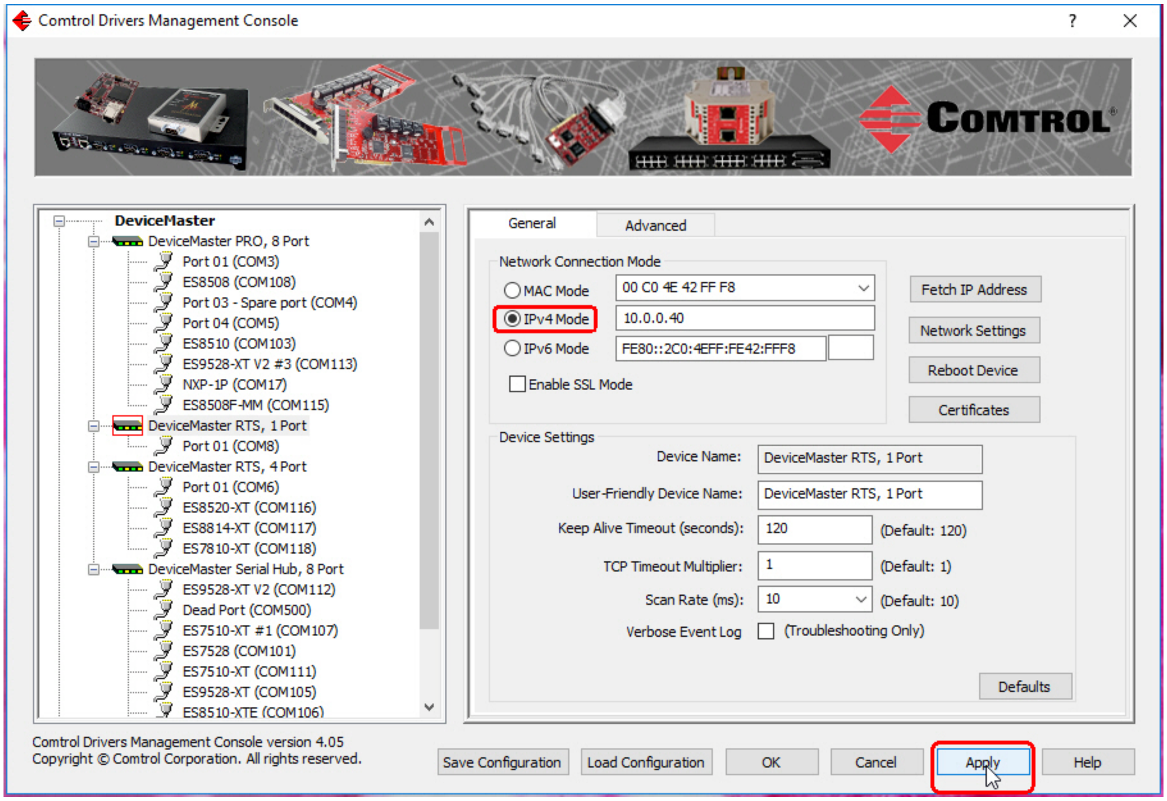
Device Settings

Device Name:	DeviceMaster RTS, 1 Port	
User-Friendly Device Name:	DeviceMaster RTS, 1 Port	
Keep Alive Timeout (seconds):	120	(Default: 120)
TCP Timeout Multiplier:	1	(Default: 1)
Scan Rate (ms):	10	(Default: 10)
Verbose Event Log	□ (Troubleshooting Only)	

Comtrol Drivers Management Console version 4.05
Copyright © Comtrol Corporation. All rights reserved.

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

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



Network Connection Mode

○ MAC Mode 00 C0 4E 42 FF F8

● IPv4 Mode 10.0.0.40

○ IPv6 Mode FE80::2C0:4EFF:FE42:FFF8

□ Enable SSL Mode

Device Settings

Device Name: DeviceMaster RTS, 1 Port

User-Friendly Device Name: DeviceMaster RTS, 1 Port

Keep Alive Timeout (seconds): 120 (Default: 120)

TCP Timeout Multiplier: 1 (Default: 1)

Scan Rate (ms): 10 (Default: 10)

Verbose Event Log □ (Troubleshooting Only)

Comtrol Drivers Management Console version 4.05
Copyright © Comtrol Corporation. All rights reserved.

6. Optionally, click the **Network Settings** button and click **Modify** to make any network settings changes for DHCP or MAC mode (Disable IP).

7. Optionally, click **Enable SSL Mode** if you want to configure secure COM ports.

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

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

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

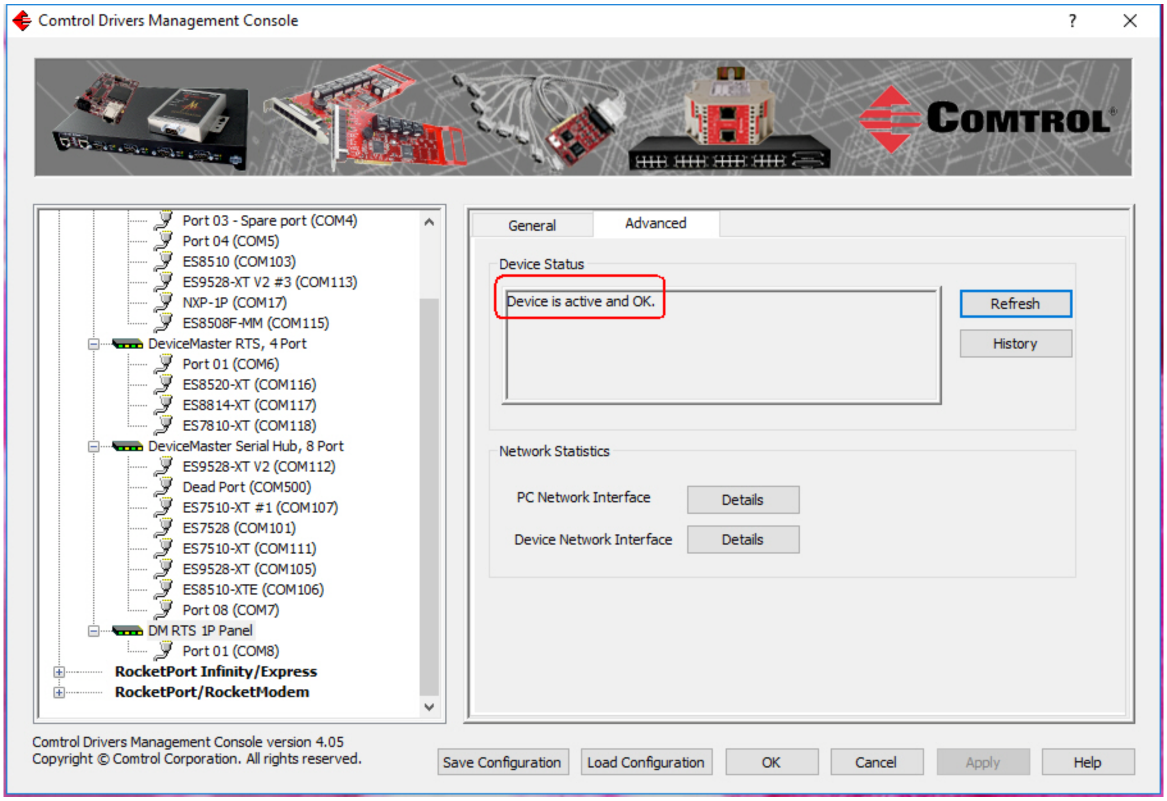
   In addition to encrypting the data streams, it is possible to configure the DeviceMaster LT so that only authorized client applications can connect using SSL/TLS.

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

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

8. If you are using a server certificate, click the **Certificates** button.
   a. Click the **Server Certificate** check box if you want to enter a **Server Certificate**.
   b. Enter the name in the **Server Certificate** text box.
   c. If you are using a client certificate, click the drop list and browse to the appropriate client certificate file.
   d. Click the **Ok** button to close the Certificates pop up window.
9. Configure the remainder of the device properties:
   a. If desired, change the **User-Friendly Device Name**.
   b. Optionally, set a different **Keep Alive Timeout** period. You can set the amount of time in seconds that this DeviceMaster LT waits until it closes this connection and frees all the ports associated with it.
   c. Optionally, set the **TCP Timeout Multiplier** value.
   d. Optionally, click a different **Scan Rate (ms)**.
   e. Optionally, click **Verbose Event Log** if you want to log additional DeviceMaster LT information into the event log.
   f. After making your changes, click **Apply** if you have additional configuration procedures or click **Ok** if you have completed configuring your DeviceMaster LT.

   Note: *You can refer to the help system if you need information about any of the options or features.*
10. Optionally, you can click the **Advanced** tab and verify that the *Device Status* message indicates that the DeviceMaster LT is active and *Ok*.



Device is active and OK.

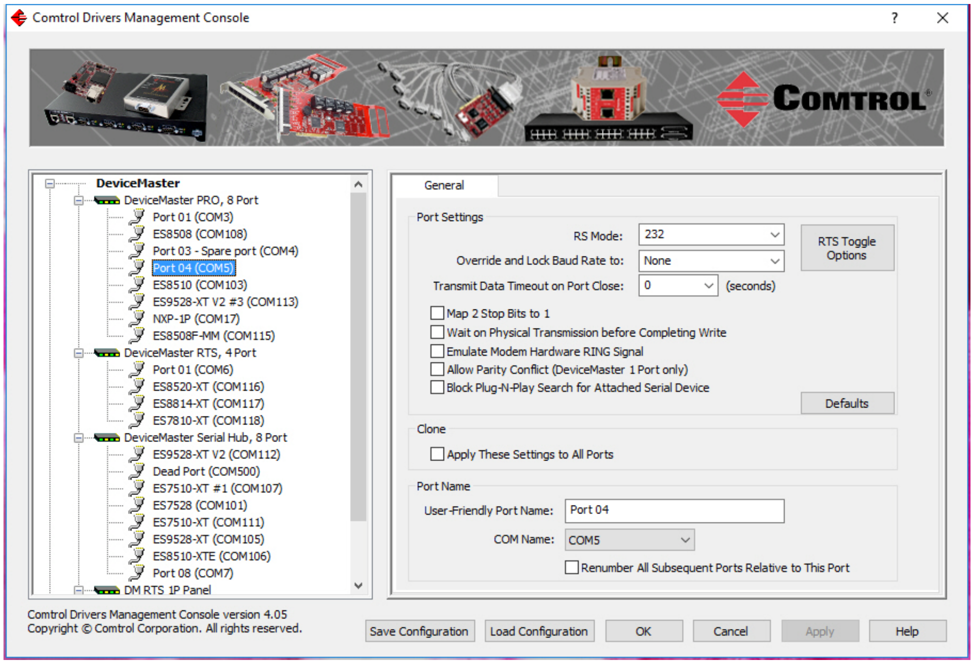
Comtrol Drivers Management Console version 4.05
Copyright © Comtrol Corporation. All rights reserved.

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

Configuring COM Port Properties for Windows

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

1. Highlight the first port you want to configure.



Comtrol Drivers Management Console

- DeviceMaster
  - DeviceMaster PRO, 8 Port
    - Port 01 (COM3)
    - ES8508 (COM108)
    - Port 03 - Spare port (COM4)
    - Port 04 (COM5)
    - ES8510 (COM103)
    - ES9528-XT V2 #3 (COM113)
    - NXP-1P (COM17)
    - ES8508F-MM (COM115)
  - DeviceMaster RTS, 4 Port
    - Port 01 (COM6)
    - ES8520-XT (COM116)
    - ES8814-XT (COM117)
    - ES7810-XT (COM118)
  - DeviceMaster Serial Hub, 8 Port
    - ES9528-XT V2 (COM112)
    - Dead Port (COM500)
    - ES7510-XT #1 (COM107)
    - ES7528 (COM101)
    - ES7510-XT (COM111)
    - ES9528-XT (COM105)
    - ES8510-XTE (COM106)
    - Port 08 (COM7)
  - DM RTS 1P Panel

General

Port Settings

RS Mode: 232

Override and Lock Baud Rate to: None

Transmit Data Timeout on Port Close: 0 (seconds)

□ Map 2 Stop Bits to 1

□ Wait on Physical Transmission before Completing Write

□ Emulate Modem Hardware RING Signal

□ Allow Parity Conflict (DeviceMaster 1 Port only)

□ Block Plug-N-Play Search for Attached Serial Device

Clone

□ Apply These Settings to All Ports

Port Name

User-Friendly Port Name: Port 04

COM Name: COM5

□ Renumber All Subsequent Ports Relative to This Port

Comtrol Drivers Management Console version 4.05
Copyright © Comtrol Corporation. All rights reserved.

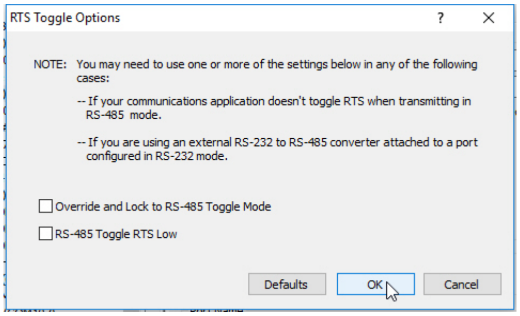
2. Complete the screen appropriately for the serial device that you plan on connecting to the port and click the **Ok** button.

   a. Select the appropriate communications mode.

   b. Enable the features that you want to use.

   c. Optionally, click the **RTS Toggle Options** button:

      - If your communications application does not toggle RTS when transmitting in RS-485 mode.
      - If you are using an external RS-232 to RS-485 converter, which is attached to a port that is configured for RS-232.



RTS Toggle Options

NOTE: You may need to use one or more of the settings below in any of the following cases:

-- If your communications application doesn't toggle RTS when transmitting in RS-485 mode.

-- If you are using an external RS-232 to RS-485 converter attached to a port configured in RS-232 mode.

□ Override and Lock to RS-485 Toggle Mode

□ RS-485 Toggle RTS Low

   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 LT to these characteristics.

4. Optionally, change the **User-Friendly Port Name**.

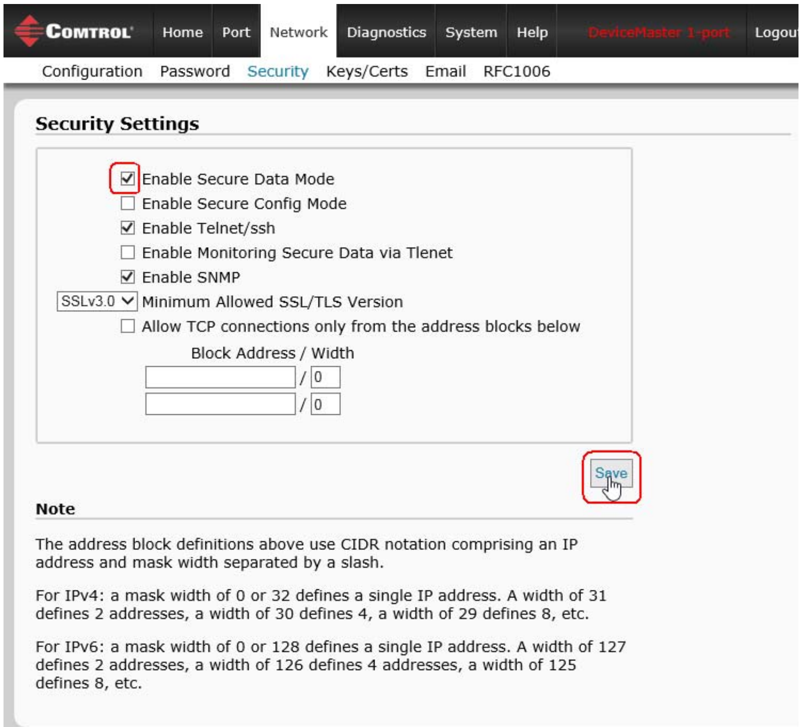
5. If desired, select a different **COM Name** (COM port number). The drop-down list displays (in use) next to COM port numbers that are already in use in this system. Do not duplicate COM port numbers as this will cause the ports to not function.
6. Click **Apply** to save these changes.

   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 95 to attach your serial device.
9. Optionally, you may need to configure one or more ports for socket mode (*Socket Port Configuration* on Page 45).

Enabling Secure Data Mode

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

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



Security Settings

☑ Enable Secure Data Mode
□ Enable Secure Config Mode
☑ Enable Telnet/ssh
□ Enable Monitoring Secure Data via Tlenet
☑ Enable SNMP
SSLv3.0 Minimum Allowed SSL/TLS Version
□ Allow TCP connections only from the address blocks below

Block Address / Width
/ 0
/ 0

Note

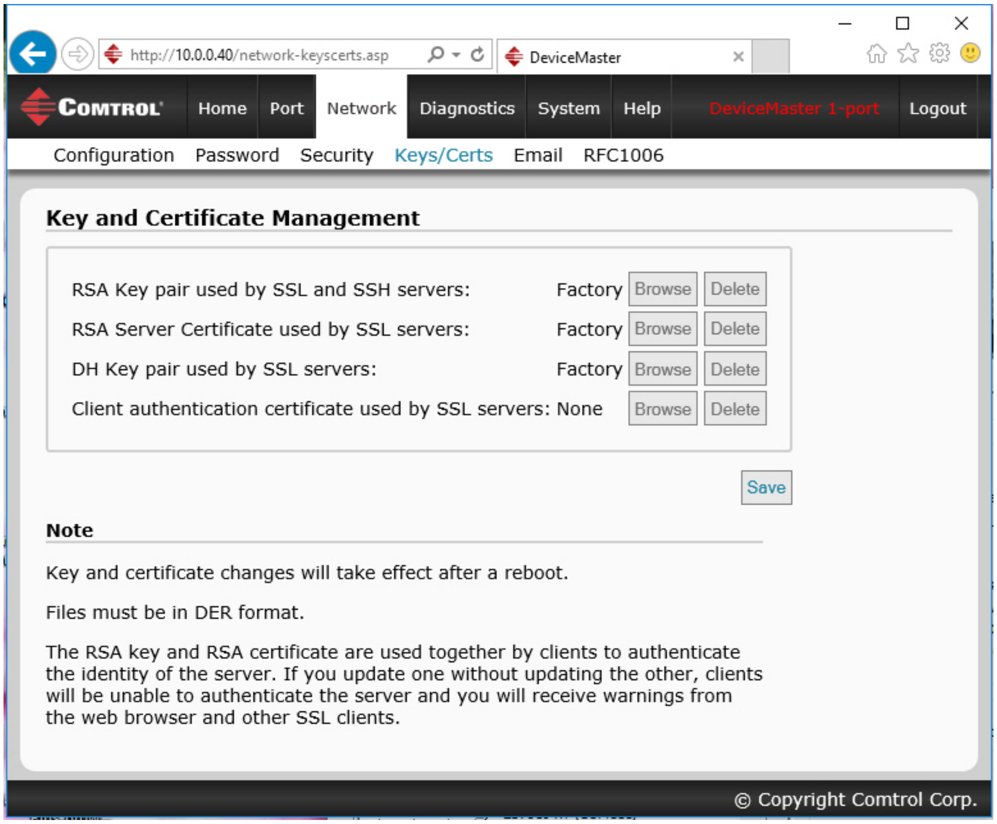
The address block definitions above use CIDR notation comprising an IP address and mask width separated by a slash.

For IPv4: a mask width of 0 or 32 defines a single IP address. A width of 31 defines 2 addresses, a width of 30 defines 4, a width of 29 defines 8, etc.

For IPv6: a mask width of 0 or 128 defines a single IP address. A width of 127 defines 2 addresses, a width of 126 defines 4 addresses, a width of 125 defines 8, etc.

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

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



Key and Certificate Management

RSA Key pair used by SSL and SSH servers:	Factory	Browse	Delete
RSA Server Certificate used by SSL servers:	Factory	Browse	Delete
DH Key pair used by SSL servers:	Factory	Browse	Delete
Client authentication certificate used by SSL servers:	None	Browse	Delete

Note

Key and certificate changes will take effect after a reboot.

Files must be in DER format.

The RSA key and RSA certificate are used together by clients to authenticate the identity of the server. If you update one without updating the other, clients will be unable to authenticate the server and you will receive warnings from the web browser and other SSL clients.

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

Socket Port Configuration

This section provides an overview of SocketServer and provides basic operating procedures. SocketServer and DeviceMaster LT security are discussed in detail in *DeviceMaster LT Security* on Page 49.

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

SocketServer Overview

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

The SocketServer home page (*Server Info*) provides basic information about the DeviceMaster LT including whether it is functioning in socket mode (SocketServer) or in NS-Link (driver). See *SocketServer Architecture* on Page 46 for more information about socket port support.

The following menus are available in the web interface:

- **Port**, which includes the following pages:
  - **Port Overview** of all of the serial port settings
  - **Port Configuration** for each port that includes Serial, TCP connection, and UDP connection configuration capabilities
- **Network**, which includes the following pages:
  - **Configuration** for general, IPv4 and IPv6 settings (after initial configuration)
  - **Password** to set a device password
  - **Security**, which is discussed in detail starting on Page 49
  - **Keys/Certs** to manage security keys and certificates
  - **Email** for notification services
  - **RFC1006** (ISO over TCP)
- **Diagnostics**, which include:
  - **System Log**
  - **Device Snapshot**
  - **Port Monitor**

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

Web Page Help System

The web page *Help* system is available separately for your convenience. The web page Help system contains detailed information and configuration procedures for each mode discussed in *SocketServer Architecture* on Page 46.

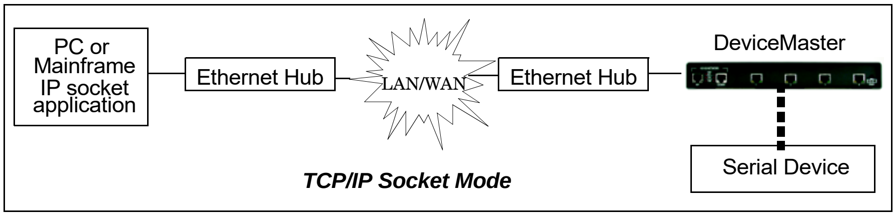
The *Help* system for the web page is available from: ftp://ftp.comtrol.com/dev_mstr/LT/software/socketserver/help/ssvr_help.zip.

To use the help system:

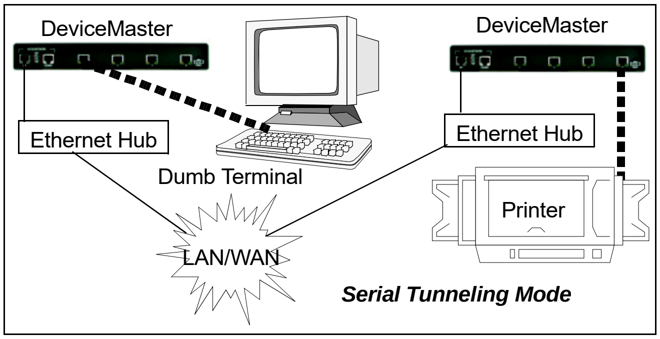
1. Unzip the files in a folder.
2. Open the **ssvr_help.htm** file.
3. Use your browser find function to locate the option or information for which are searching.

SocketServer Architecture

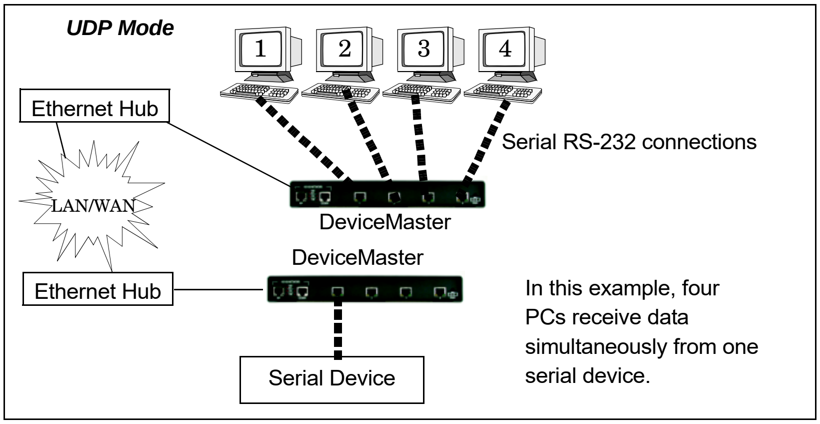
TCP/IP socket mode operation is used to connect serial devices with an application that supports TCP/IP socket communications addressing.



Serial tunneling mode is used to establish a socket connection between two DeviceMaster LTs 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.


UDP Mode
1
2
3
4
Ethernet Hub
Serial RS-232 connections
LAN/WAN
DeviceMaster
DeviceMaster
Ethernet Hub
Serial Device
In this example, four PCs receive data simultaneously from one serial device.

Accessing Socket Configuration

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

- *Web Browser*
- *PortVision DX*

Web Browser

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

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

   Note: *If you do not know the IP address, you can view and highlight the IP address in PortVision DX and click the* **Webpage** *button.*
3. If necessary, enter **admin** as the *username*, your password, and then click the **Login** button.
4. Click the **Port** menu.
5. Click the port number that you want to configure socket port settings (serial, TCP connection configuration, and UDP connection configuration).

Note: *Refer to the web page Help system, if you need information about configuring sockets or serial tunneling, which contains detailed configuration procedures and descriptions for all fields. See Web Page Help System on Page 45 for information about downloading the help file separately.*

6. After changing the appropriate settings for your environment, click **Save**.
7. Click the **Network** tab to access the following pages if you need to configure additional settings:
   - **Configuration** page to change the network settings.
   - **Password** page to configure a password for the DeviceMaster.
   - **Security** page to enable DeviceMaster LT security.
   - **Keys/Certs** page to configure security certificates and keys.
   - **Email** page to configure email notification services.
   - **RFC1006** page to configure RFC1006 settings.

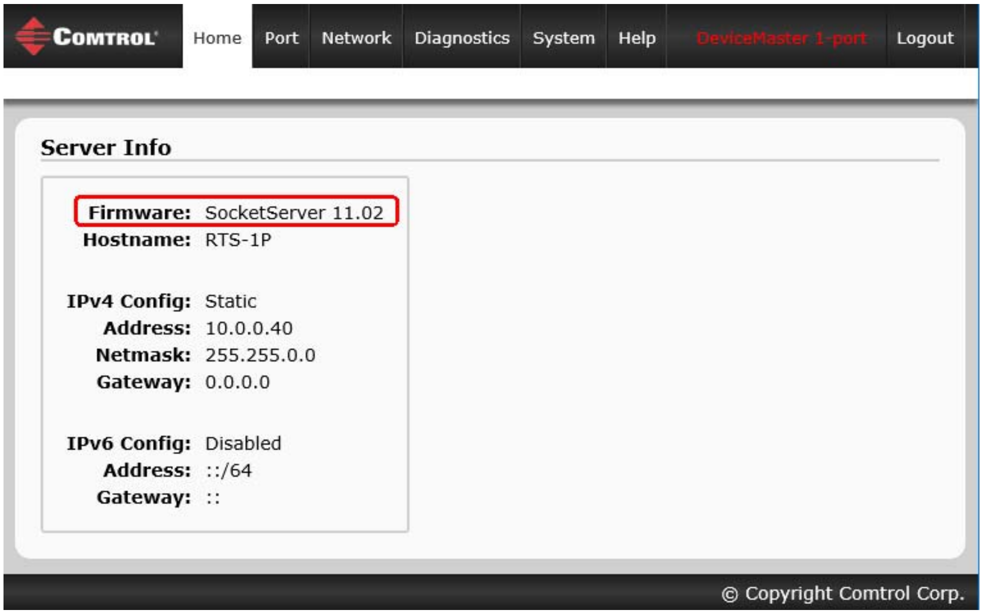
PortVision DX

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

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

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 Info

Firmware: SocketServer 11.02
Hostname: RTS-1P

IPv4 Config: Static
Address: 10.0.0.40
Netmask: 255.255.0.0
Gateway: 0.0.0.0

IPv6 Config: Disabled
Address: ::/64
Gateway: ::

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

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

DeviceMaster LT Security

This subsection provides a basic understanding of the DeviceMaster LT security options, and the repercussions of setting these options. See *Removing DeviceMaster LT Security Features* on Page 135 if you need to reset DeviceMaster LT security options. See *Returning the DeviceMaster LT to Factory Defaults* on Page 137 if you want to return the DeviceMaster LT 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) †	If configured with a CA certificate, the DeviceMaster LT requires all SSL/TLS clients to present an RSA identity certificate that has been signed by the configured CA certificate. As shipped, the DeviceMaster LT is not configured with a CA certificate and all SSL/TLS clients are allowed. 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. See *Key and Certificate Management* on Page 67 for more information. This section does not discuss the creation of CA Certificates.
Client Authentication	A process using paired keys and identity certificates to prevent unauthorized access to the DeviceMaster LT. Client authentication is discussed in *Client Authentication* on Page 59 and *Changing Keys and Certificates* on Page 71.
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. The DH (Diffie-Hellman) key exchange, also called exponential key exchange, is a method of digital encryption that uses numbers raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted, making the task of a would-be code breaker mathematically overwhelming. The most serious limitation of Diffie-Hellman (DH key) in its basic or *pure* 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. See *Certificates and Keys* on Page 59 and *Key and Certificate Management* on Page 67 for more information.

† *All DeviceMaster LT units are shipped from the factory with identical configurations. They all have the identical, self-signed, Comtrol Server RSA Certificates, Server RSA Keys, Server DH Keys, and no Client Authentication Certificates. For maximum data and access security, you should configure all DeviceMaster LT units with custom certificates and keys.*

Term or Issue	Explanation
Digital Certificate	A digital certificate is an electronic *credit card* that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys. See *Key and Certificate Management* on Page 67 for more information.
PKI (public key infrastructure)	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. The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message. Traditional cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This secret or private key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the public key infrastructure is the preferred approach on the Internet. (The private key system is sometimes known as symmetric cryptography and the public key system as asymmetric cryptography.) A public key infrastructure consists of: • A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key • A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor • One or more directories where the certificates (with their public keys) are held • A certificate management system For more information, see *SSL Authentication* on Page 58, *SSL Performance* on Page 60, *SSL Cipher Suites* on Page 61, and *DeviceMaster LT Supported Cipher Suites* on Page 61.

Term or Issue	Explanation
RSA Key Pair†	This is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption. RSA is widely used in electronic commerce protocols, and is believed to be sufficiently secure given sufficiently long keys and the use of up-to-date implementations. The system includes a communications channel coupled to at least one terminal having an encoding device, and to at least one terminal having a decoding device. • Public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures. • Private Key - One half of the *key pair* 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. Thus, if *User A* sends *User B* a message, *User A* can find out *User B's* public key (but not *User B's* private key) from a central administrator and encrypt a message to *User B* using *User B's* public key. When *User B* receives it, *User B* decrypts it with *User B's* private key. In addition to encrypting messages (which ensures privacy), *User B* can authenticate *User B* to *User A* (so that *User A* knows that it is really *User B* who sent the message) by using *User B's* private key to encrypt a digital certificate. See *Key and Certificate Management* on Page 67 for more information.
SSH (Secure Shell)	Secure Shell (SSH) allows data to be exchanged using a secure channel between two networked devices. Replaces telnet which has no security. SSH requires password authentication – even if the password is empty. See *SSH Server* on Page 57 for more information.
SSL (Secure Sockets Layer)	The Secure Sockets Layer (SSL) is the predecessor of (TLS) Transport Layer Security. SSL is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. See Pages 58 through 61 for detailed information about SSL. ***Note:*** *Two slightly different SSL protocols are supported by the DeviceMaster LT: SSLv3 and TLSv1.*

Term or Issue	Explanation
TLS (Transport Layer Security)	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). TLS and SSL are not interoperable. The TLS protocol does contain a mechanism that allows TLS implementation to back down to SSL 3.0.
Secure Data Mode	TCP connections that carry data to/from the DeviceMaster LT serial ports are encrypted using SSL or TLS security protocols. See *Security Modes* on Page 55 and *Configure/Enable Security Features Overview* on Page 63 for more information.
Secure Config Mode	Unencrypted access to administrative and diagnostic functions are disabled. See *Security Modes* on Page 55 and *Configure/Enable Security Features Overview* on Page 63 for more information.
Secure Monitor Data Mode via Telnet	Allows monitoring of a single serial port on the DeviceMaster LT while the port is configured for **Secure Data Mode**. For more information see, the **Enable Monitoring Secure Data via Telnet** option on Page 65.
Man in the Middle attack	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. 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.
How Public and Private Key Cryptography Works	In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority (CA). The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is never shared with anyone or sent across the Internet. You use the private key to decrypt text that has been encrypted with your public key by someone else (who can find out what your public key is from a public directory). Thus, if *User A* sends *User B* a message, *User A* can find out *User B's* public key (but not *User B's* private key) from a central administrator and encrypt a message to *User B* using *User B's* public key. When *User B* receives it, *User B* decrypts it with *User B's* private key. In addition to encrypting messages (which ensures privacy), *User B* can authenticate *User B* to *User A* (so *User A* knows that it is really *User B* who sent the message) by using *User B's* private key to encrypt a digital certificate. When *User A* receives it, *User A* can use *User B's* public key to decrypt it.

<table>
<tr><th>Term or Issue</th><th>Explanation</th></tr>
<tr><td><em>Who Provides the Infrastructure?</em></td><td>A number of products are offered that enable a company or group of companies to implement a PKI. The acceleration of e-commerce and business-to-business commerce over the Internet has increased the demand for PKI solutions. Related ideas are the virtual private network (VPN) and the IP Security (IPsec) standard. Among PKI leaders are:
• RSA, which has developed the main algorithms used by PKI vendors.
• 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.</td></tr>
<tr><td colspan="2">The following topic references are from: http://searchsecurity.techtarget.com/
• PKI (public key infrastructure)
• How Public/Private Key Cryptography Works
• Who Provides the Infrastructure
• Digital Certificate
• DH Key
• Man in the Middle attack
The RSA Key pair topic reference is from: http://en.wikipedia.org/wiki/RSA</td></tr>
</table>

TCP and UDP Socket Ports Used by the DeviceMaster LT

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

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 DX 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 LT. For example: A DeviceMaster LT 16- port would have Ports 8000 through 8015.
UDP 7000 - 7xxx	Incremented per serial port on the DeviceMaster LT. For example: A DeviceMaster LT 16- port would have Ports 7000 through 7015.

DeviceMaster LT Security Features

The following subsections provide information about DeviceMaster LT security features.

Security Modes

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

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

Security Comparison

This table displays addition information about security feature comparisons.

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

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

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

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

SSH Server

The DeviceMaster LT SSH server has the following characteristics:

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

SSL Overview

DeviceMaster LT 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 LT) 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.
- Several slightly different SSL protocols are supported by the DeviceMaster LT, SSLv3, TLSv1.0, TLS1.1, and TLS1.2.
- The DeviceMaster LT uses third-party MatrixSSL library from PeerSec Networks: http://www.peersec.com/matrixssl.html.

SSL Authentication

DeviceMaster LT 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 LT 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 LT proves its identity.

- The DeviceMaster LT (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 LT.
- The private key used to sign the certificate must also be uploaded to the DeviceMaster LT.

  Note: *Possession of that private key will allow eavesdroppers to decrypt all traffic to and from the DeviceMaster LT.*
- The corresponding public key can be used to verify the ID certificate but not to decrypt traffic.
- All DeviceMaster LT 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 LT firmware and use that private key to eavesdrop on traffic to/from any other DeviceMaster LT 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 LT 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 LT verifies the identity of clients (that is, web browsers and so forth).

- Clients can generally be configured to accept a particular unknown server certificate so that the user is not subsequently warned.
- The DeviceMaster LT (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 LT by SSL clients. This allows you to restrict access to the DeviceMaster LT to a limited set of clients which have been configured with corresponding ID certificates.
- DeviceMaster LT 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 LT.

Certificates and Keys

To control access to the DeviceMaster LT'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 LT 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 LT.
- 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 LT 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 LT 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 LT.

      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 LT uses during SSL/TLS handshaking to identify itself. It is used most frequently by SSL server code in the DeviceMaster LT when clients open connections to the DeviceMaster LT's secure web server or other secure TCP ports. If a DeviceMaster LT serial port configuration is set up to open (as a client), a TCP connection to another server device, the DeviceMaster LT 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 LT requires all SSL/TLS clients to present an RSA identity certificate that has been signed by the configured CA certificate. As shipped, the DeviceMaster LT is not configured with a CA certificate and all SSL/TLS clients are allowed.

SSL Performance

The DeviceMaster LT has these SSL performance characteristics:

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

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

Note: *These throughputs required 100% CPU usage, so other features such as the web server are very unresponsive at the throughputs shown above. To maintain a usable web interface, one would want to stay well below the maximum throughput/port numbers above.*

- The overhead required to set up an SSL connection is significant. The time required to open a connection to SocketServer varies depending on the public-key encryption scheme used for the initial handshaking. These are typical setup times for the three public-key encryption schemes for the DeviceMaster LT:
  - RSA 0.66 seconds
  - DHE 3.84 seconds
  - DHA 3.28 seconds
- Since there is a certain amount of overhead for each block of data sent/received on an SSL connection, the SocketServer polling rate and size of bocks that are written to the SocketServer also has a noticeable effect on CPU usage.

Writing larger blocks of data and a slower SocketServer polling rate will decrease CPU usage and allow somewhat higher throughputs.

SSL Cipher Suites

This subsection provides information about SSL cipher suites.

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

DeviceMaster LT Supported Cipher Suites

The DeviceMaster LT 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:

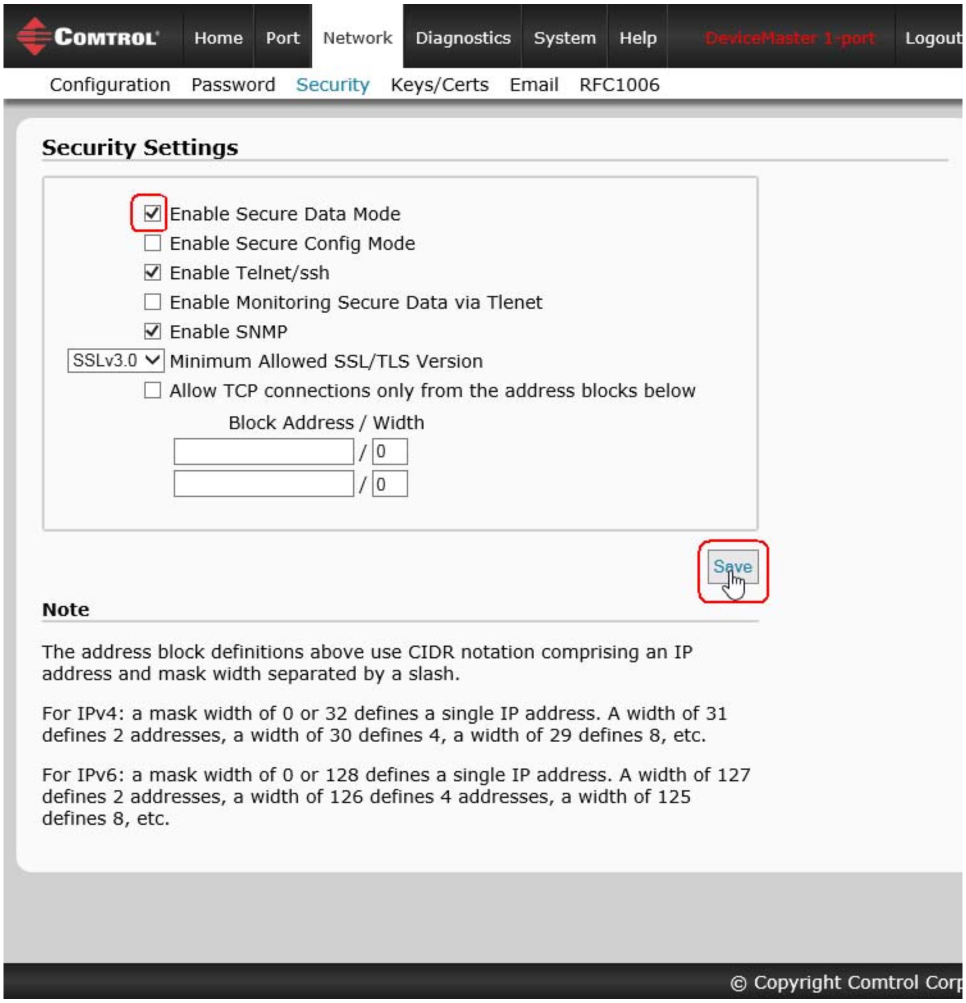
- Standard reference book is SSL and TLS by Eric Rescorla
- Wikipedia page on SSL/TLS provides a good overview: http://en.wikipedia.org/wiki/TLS
- **openssl** contains command-line tools to do the following. More information is available at: http://www.openssl.org/
    - Create/examine keys/certificates
    - 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 Overview

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

If you want secure COM ports, you must also **Enable SSL Mode** and enter any applicable server or client certificates in the NS-Link device driver for Windows. See *Device Driver (NS-Link) Installation* on Page 31.

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



Security Settings

☑ Enable Secure Data Mode
☐ Enable Secure Config Mode
☑ Enable Telnet/ssh
☐ Enable Monitoring Secure Data via Tlenet
☑ Enable SNMP
SSLv3.0 Minimum Allowed SSL/TLS Version
☐ Allow TCP connections only from the address blocks below

Block Address / Width
/ 0
/ 0

Note

The address block definitions above use CIDR notation comprising an IP address and mask width separated by a slash.

For IPv4: a mask width of 0 or 32 defines a single IP address. A width of 31 defines 2 addresses, a width of 30 defines 4, a width of 29 defines 8, etc.

For IPv6: a mask width of 0 or 128 defines a single IP address. A width of 127 defines 2 addresses, a width of 126 defines 4 addresses, a width of 125 defines 8, etc.

Security Option	Description
Enable Secure Data Mode	If **Secure Data Mode** is enabled TCP connections which carry data to/from the serial ports will be encrypted using SSL or TLS security protocols. This includes the following: • TCP connections to the per-serial-port TCP ports (default is 8000, 8001, 8002, and so forth) are encrypted using SSL/TLS. • TCP connections to TCP Port 4606 on which the DeviceMaster LT implements the Comtrol proprietary serial driver protocol are encrypted using SSL/TLS. • Since SSL/TLS can not be used for either UDP data streams or for the Comtrol proprietary MAC mode Ethernet driver protocol, both UDP and MAC mode serial data transport features are disabled. • In order to minimize possible security problems, e-mail and RFC1006 features are also disabled in *Secure Data* mode. In addition to encrypting the data streams, it is possible to configure the DeviceMaster LT so that only authorized client applications can connect using SSL/TLS. See the *Client Authentication* discussion on Page 59 for details.
Enable Secure Config Mode	If **Secure Config Mode** is enabled, unencrypted access to administrative and diagnostic functions is disabled. **Secure Config Mode** changes DeviceMaster LT behavior as follows: • Telnet access to administrative and diagnostic functions is disabled. SSH access is still allowed. • Unencrypted access to the web server via Port 80 (http:// URLs) is disabled. • 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 Comtrol proprietary TCP driver protocol on TCP Port 4606 are ignored. • Administrative commands that change configuration or operating state that are received using the Comtrol MAC mode proprietary Ethernet protocol number 0x11FE are ignored.

Security Option	Description
Enable Monitoring Secure Data via Telnet	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 LT for the change to go into affect. This option is disabled by default. The **Enable Monitoring Secure Data via Telnet** feature allows you to monitor serial data being sent/received on a serial port (either via NS-Link or SocketServer). The monitoring is done by telnetting to the DeviceMaster LT and using the following commands: • **monitor [-ac] portnumber** 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). Monitoring serial data through a telnet connection does generate extra network traffic and may have small effects on the timing of DeviceMaster LT operations when large amounts of data are being logged at high baud rates. See *Example 1* on Page 66 for more information. - The **-a** option enables displaying of ASCII representation of data in a column to the right the hex representation. See *Example 2* on Page 66. - 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 66. • **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. ***Note:*** *Optionally, you can use the Port Monitor function in the web interface. Click* **Diagnostics | Port Monitor**.
Enable Telnet/ssh	This option enables or disables the telnet security feature after you click **Save** and the DeviceMaster LT has been rebooted. *This option is enabled by default.*
Enable SNMP	This option enables or disables the SNMP security feature after you click **Save** and the DeviceMaster LT has been rebooted. *This option is enabled by default.*

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                        < abcABC123
> 61 62 63 41 42 43 31 32 33                        > abcABC123
< 61 62 63 41 42 43 31 32 33                        < abcABC123
> 61 62 63 41 42 43 31 32 33                        > abcABC123
< 61 62 63 41 42 43 31 32 33                        < abcABC123
```

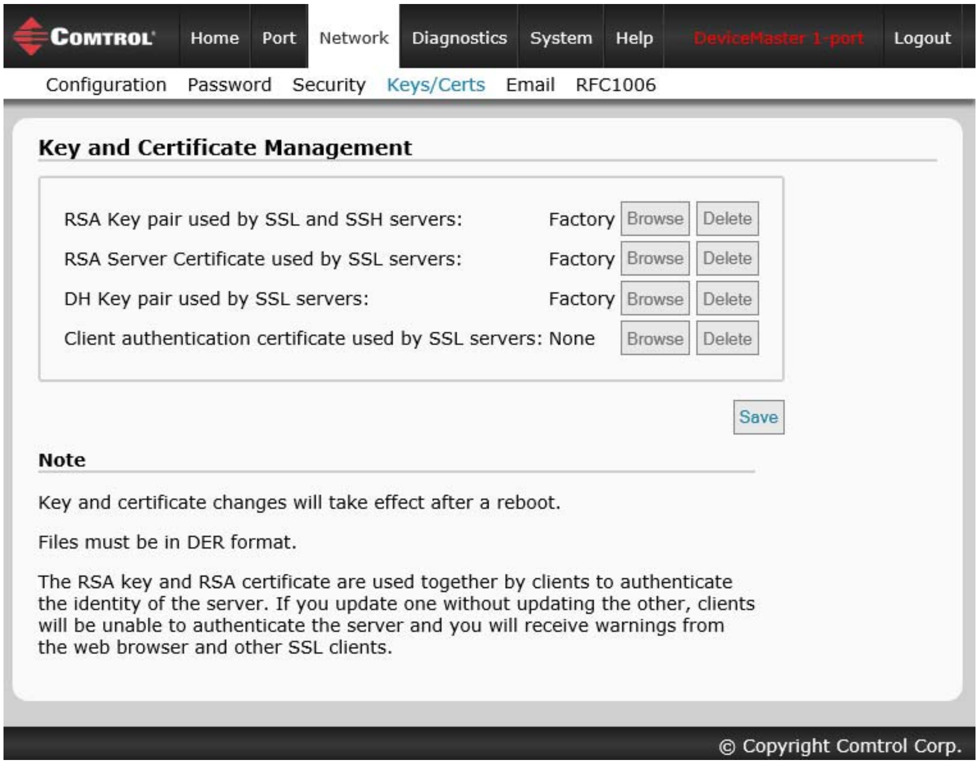
Example 3

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

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

Key and Certificate Management

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



Key and Certificate Management

RSA Key pair used by SSL and SSH servers: Factory

RSA Server Certificate used by SSL servers: Factory

DH Key pair used by SSL servers: Factory

Client authentication certificate used by SSL servers: None

Note

Key and certificate changes will take effect after a reboot.

Files must be in DER format.

The RSA key and RSA certificate are used together by clients to authenticate the identity of the server. If you update one without updating the other, clients will be unable to authenticate the server and you will receive warnings from the web browser and other SSL clients.

Key and Certificate Management Options	Description
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 &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;. 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.

<table>
<tr><th>Key and Certificate Management Options</th><th>Description</th></tr>
<tr><td>RSA Server Certificate used by SSL servers</td><td>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.</td></tr>
<tr><td>DH Key pair used by SSL servers</td><td>This is a private/public key pair that is used by some cipher suites to encrypt the SSL/TLS handshaking messages.
<b><i>Note:</i></b> <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></td></tr>
<tr><td>Client Authentication Certificate used by SSL servers</td><td>If configured with a CA certificate, the DeviceMaster requires all SSL/TLS clients to present an RSA identity certificate that has been signed by the configured CA certificate. As shipped, the DeviceMaster is not configured with a CA certificate and all SSL/TLS clients are allowed.
See <i>Client Authentication</i> on Page 59 for more detailed information</td></tr>
<tr><td colspan="2">• <i>All DeviceMaster LT units are shipped from the factory with identical configurations. They all have the identical, self-signed, Comtrol Server RSA Certificates, Server RSA Keys, Server DH Keys, and no Client Authentication Certificates.</i>
• <i>For maximum data and access security, you should configure all DeviceMaster LT units with custom certificates and keys.</i></td></tr>
</table>

Using a Web Browser to Set Security Features

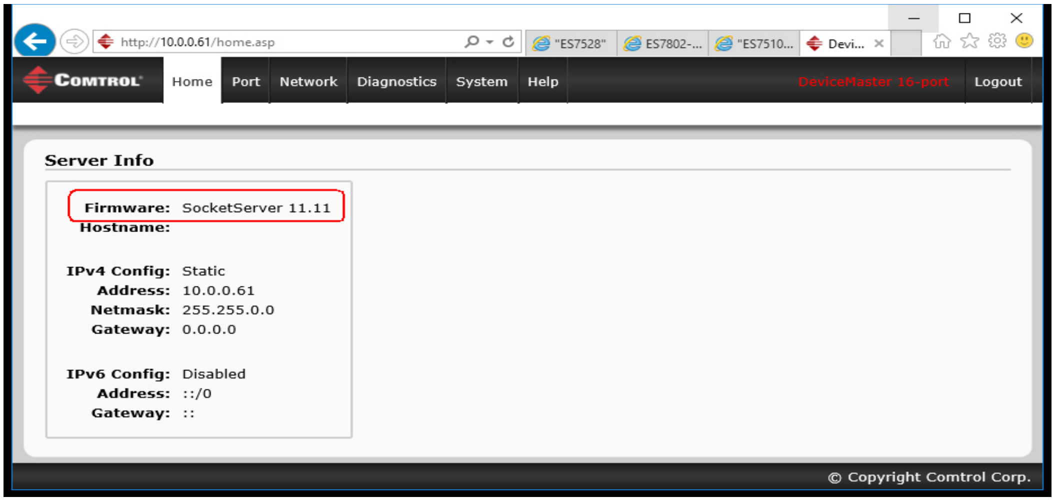
The follow procedures are discussed below:

- *Changing Security Configuration*
- *Changing Keys and Certificates* on Page 71

Changing Security Configuration

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

1. Enter the IP address of the DeviceMaster LT in the *Address* field of your web browser and press the **Enter** key.



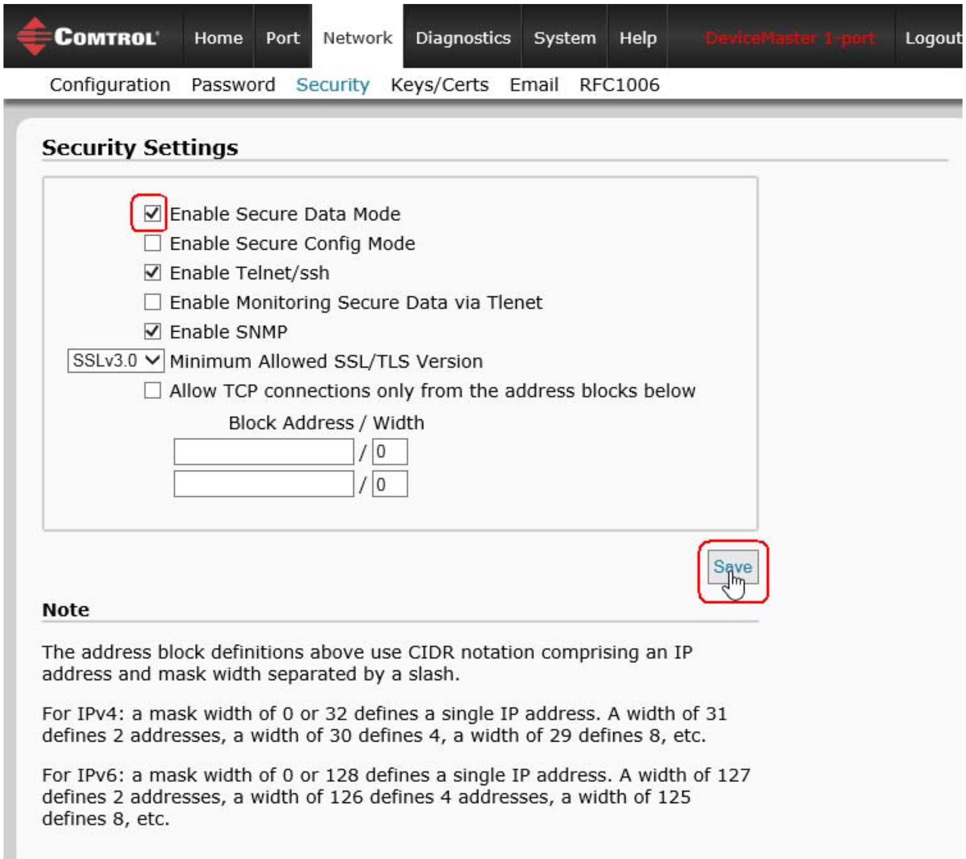
Server Info

```
  Firmware:  SocketServer 11.11
  Hostname:

IPv4 Config:  Static
    Address:  10.0.0.61
    Netmask:  255.255.0.0
    Gateway:  0.0.0.0

IPv6 Config:  Disabled
    Address:  ::/0
    Gateway:  ::
```

*The **Software** displays as NS-Link, if you have installed and configured a device driver.*

2. Click the **Network** menu.
3. Click the appropriate port number.

4. Click the appropriate check boxes to enable or disable security for your environment.



Security Settings

☑ Enable Secure Data Mode
□ Enable Secure Config Mode
☑ Enable Telnet/ssh
□ Enable Monitoring Secure Data via Tlenet
☑ Enable SNMP
SSLv3.0 Minimum Allowed SSL/TLS Version
□ Allow TCP connections only from the address blocks below

Block Address / Width
/ 0
/ 0

Note

The address block definitions above use CIDR notation comprising an IP address and mask width separated by a slash.

For IPv4: a mask width of 0 or 32 defines a single IP address. A width of 31 defines 2 addresses, a width of 30 defines 4, a width of 29 defines 8, etc.

For IPv6: a mask width of 0 or 128 defines a single IP address. A width of 127 defines 2 addresses, a width of 126 defines 4 addresses, a width of 125 defines 8, etc.

Refer to the help system or *Configure/Enable Security Features Overview* on Page 63 for detailed information.

5. After making changes, click **Save.**

Changing Keys and Certificates

Use the following steps to update security keys and certificates in the DeviceMaster LT. Refer to the help system or *Key and Certificate Management* subsection on Page 71 for detailed information.

1. If necessary, enter the IP address of the DeviceMaster LT in the *Address* field of your web browser and press the **Enter** key.
2. Click **Network | Keys/Certs**.
3. Click **Browse** to locate the key or certificate file, highlight the file, and click **Open**.
4. Click **Upload**.
5. Click **Save**, but changes will not take effect until the DeviceMaster LT is rebooted.

   Note: *The key or certificate notation changes from factory or none to* **User** *when the DeviceMaster LT is secure.*

   You can reboot the DeviceMaster LT by clicking **System | Reboot** or use the PortVision DX reboot optione.

Connecting Serial Devices

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

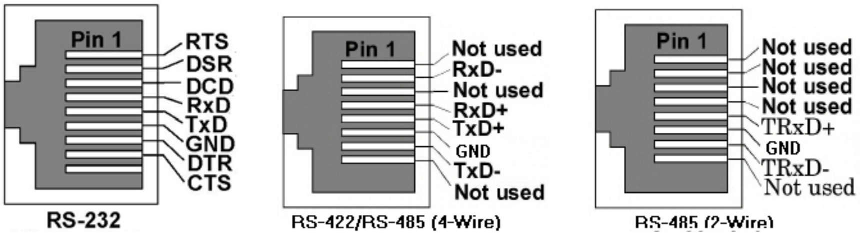
Use the appropriate subsection to connect asynchronous serial devices to the DeviceMaster LT ports.

This subsection provides the following information:

- Connector pin assignments (below)
- *RJ45 Null-Modem Cables (RS-232)* on Page 74
- *RJ45 Null-Modem Cables [RS-422/RS-485 (4-Wire)]* on Page 74
- *RJ45 Straight-Through Cables (RS-232/485)* on Page 74
- *RJ45 Loopback Plugs* on Page 75
- *RJ45 RS-485 Test Cable* on Page 75
- *Connecting RJ45 Devices* on Page 75

Connector Pin Out Assignments

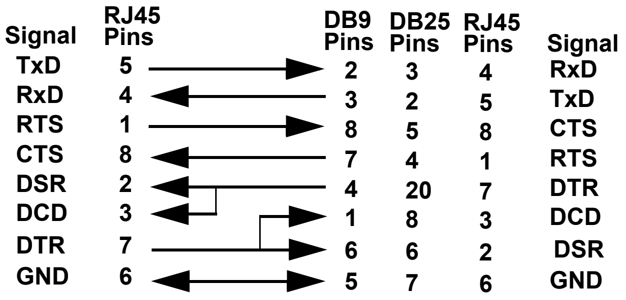
You can build your own null-modem or straight-through RJ45 serial cables if you are using the DB9 to RJ45 adapters using the following subsections.



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

RJ45 Null-Modem Cables (RS-232)

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

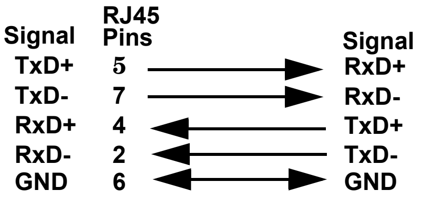


Signal	RJ45 Pins	DB9 Pins	DB25 Pins	RJ45 Pins	Signal
TxD	5	2	3	4	RxD
RxD	4	3	2	5	TxD
RTS	1	8	5	8	CTS
CTS	8	7	4	1	RTS
DSR	2	4	20	7	DTR
DCD	3	1	8	3	DCD
DTR	7	6	6	2	DSR
GND	6	5	7	6	GND

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/RS-485 (4-Wire)]

Use the following figure if you need to build an RS-422 or RS-485 (4-wire) null-modem RJ45 cable. A null-modem cable is required for connecting DTE devices.

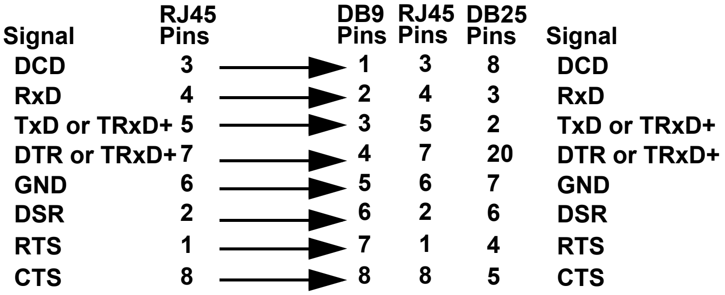


Signal	RJ45 Pins	Signal
TxD+	5	RxD+
TxD-	7	RxD-
RxD+	4	TxD+
RxD-	2	TxD-
GND	6	GND

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)

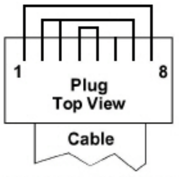
Use the following figure if you need to build an RS-232 or RS-485 straight-through cable. Straight-through cables are used to connect modems and other DCE devices. For example, a straight-through cable can be used to connect COM2 of one PC to COM2 to a modem.



Signal	RJ45 Pins	DB9 Pins	RJ45 Pins	DB25 Pins	Signal
DCD	3	1	3	8	DCD
RxD	4	2	4	3	RxD
TxD or TRxD+	5	3	5	2	TxD or TRxD+
DTR or TRxD+	7	4	7	20	DTR or TRxD+
GND	6	5	6	7	GND
DSR	2	6	2	6	DSR
RTS	1	7	1	4	RTS
CTS	8	8	8	5	CTS

RJ45 Loopback Plugs

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



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

- Pins 4 to 5
- Pins 1 to 8
- Pins 2 to 3 to 7

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. Refer to the documentation for the peripheral to determine the pinouts for the signals above.*

Signal	RJ45 Pins		Signal
TRxD-	7	◄──►	TRxD-
TRxD+	5	◄──►	TRxD+

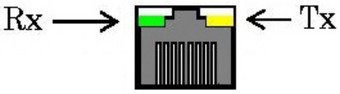
Connecting RJ45 Devices

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

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

   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 DeviceMaster LT LEDs indicate that the devices are communicating properly.

   The LED functions are displayed in the following table when the cable is attached properly to a serial device.

LED	Mode	Description	LED Status
RX (Green)	RS-232	No valid RS-232 device is connected	Always off
		Valid RS-232 device is connected but no data transmission is occurring	On
		Data being received	LED blinks
	RS-422/485	No data being received	Always off
		Data being received	LED blinks
	No mode	No mode selected	Always off
TX (Yellow)	RS-232/ 422/485	No data being transmitted	Always off
		Data being transmitted	LED blinks

3. You can refer to *DeviceMaster LT LEDs* on Page 134 for information about the remaining LEDs.

Note: *The RX/TX LEDs cycle during a reboot cycle.*

Managing the DeviceMaster LT

This section discusses the following DeviceMaster LT maintenance procedures:

- *Rebooting the DeviceMaster LT*
- *Uploading SocketServer to Multiple DeviceMaster LTs* on Page 78
- *Configuring Multiple DeviceMaster LTs Network Addresses* on Page 79

  Note: *You can configure the network addresses for multiple DeviceMaster LTs, configure common settings for the DeviceMaster LTs, and save the settings to a configuration file that you can use to load settings up to all or selected DeviceMaster LTs.*
- *Adding a New Device in PortVision DX* on Page 79
- *Using SocketServer Configuration Files* on Page 81
- *Using Driver Configuration Files* on Page 83
- *Changing the Bootloader Timeout* on Page 89, which discusses changing the Bootloader timeout
- *Managing Bootloader* on Page 91, which also discusses checking the Bootloader version and downloading the latest Bootloader
- *Checking the NS-Link Version* on Page 93
- *Accessing SocketServer Commands in Telnet/SSH Sessions (PortVision DX)* on Page 96
- *Accessing RedBoot Commands in Telnet/SSH Sessions (PortVision DX)* on Page 100

Note: *You can optionally refer to RedBoot Procedures on Page 105 if you want to perform procedures at the RedBoot level.*

Rebooting the DeviceMaster LT

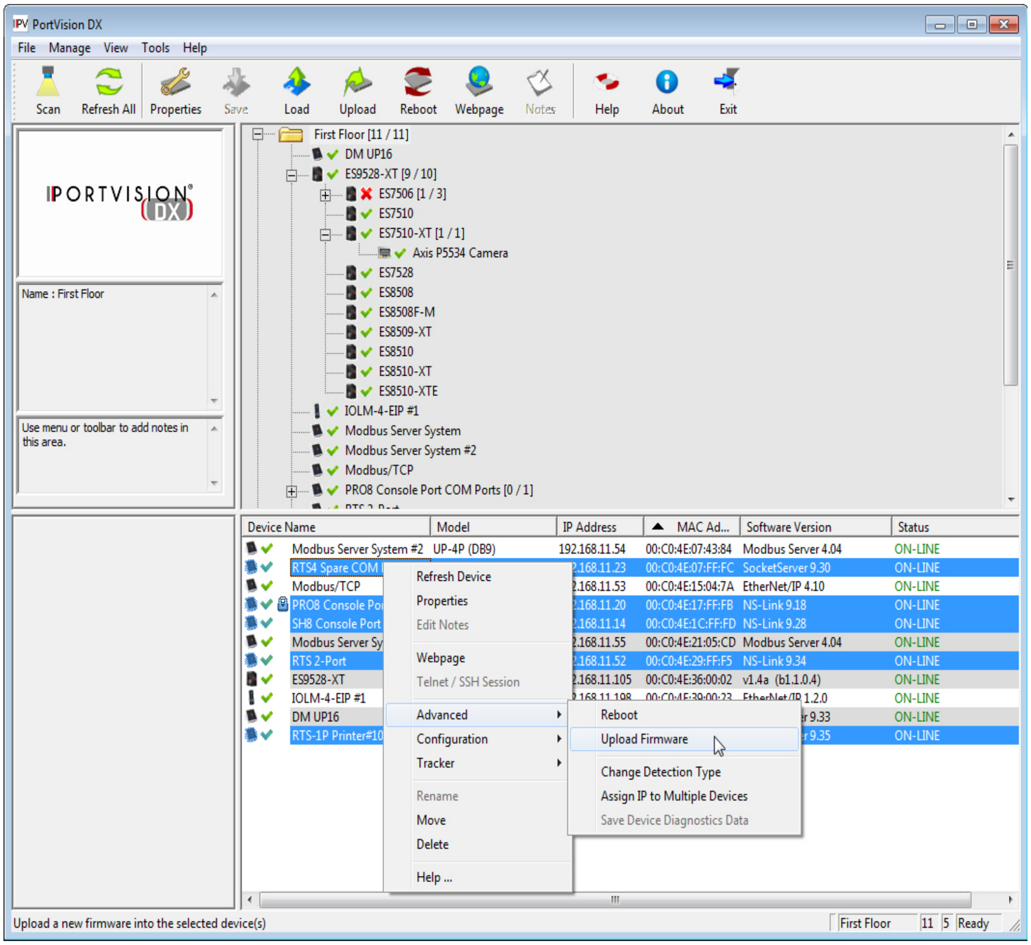
There are many ways to reboot the DeviceMaster LT.

Method	Procedure
PortVision DX	Right-click the DeviceMaster LT or DeviceMaster LTs in the *Device List* pane, click **Advanced >Reboot** and then **Yes**. ***Note:*** *If security has been enabled in the web page, you will need to reboot the DeviceMaster LT in the web page.*
Web page	**System | Reboot:** You have 10 seconds to Cancel before the DeviceMaster LT automatically reboots. Optionally, you can click **Reboot Now**.
Telnet	Type **reset**.

Uploading SocketServer to Multiple DeviceMaster LTs

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

1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 15) and **Scan** the network.
2. Shift-click the multiple DeviceMaster LTs on the **Main** screen that you want to update and use one of the following methods:
   - Click the **Upload** button.
   - Right-click and then click **Advanced > Upload Firmware**.
   - Click **Advanced >Upload Firmware** in the **Manage** menu.



Device Name	Model	IP Address	MAC Ad...	Software Version	Status
Modbus Server System #2	UP-4P (DB9)	192.168.11.54	00:C0:4E:07:43:84	Modbus Server 4.04	ON-LINE
RTS4 Spare COM		2.168.11.23	00:C0:4E:07:FF:FC	SocketServer 9.30	ON-LINE
Modbus/TCP		2.168.11.53	00:C0:4E:15:04:7A	EtherNet/IP 4.10	ON-LINE
PRO8 Console Po		2.168.11.20	00:C0:4E:17:FF:FB	NS-Link 9.18	ON-LINE
SH8 Console Port		2.168.11.14	00:C0:4E:1C:FF:FD	NS-Link 9.28	ON-LINE
Modbus Server Sy		2.168.11.55	00:C0:4E:21:05:CD	Modbus Server 4.04	ON-LINE
RTS 2-Port		2.168.11.52	00:C0:4E:29:FF:F5	NS-Link 9.34	ON-LINE
ES9528-XT		2.168.11.105	00:C0:4E:36:00:02	v1.4a (b1.1.0.4)	ON-LINE
IOLM-4-EIP #1		2.168.11.108	00:C0:4E:39:00:23	EtherNet/IP 1.2.0	ON-LINE
DM UP16				r 9.33	ON-LINE
RTS-1P Printer#10				r 9.35	ON-LINE

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

   It may take a few moments for the firmware to upload onto the DeviceMaster LT. The DeviceMaster LT reboots itself during the upload process.
4. Click **Ok** to the advisory message about waiting to use the device until the status reads **ON-LINE**.

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

Configuring Multiple DeviceMaster LTs Network Addresses

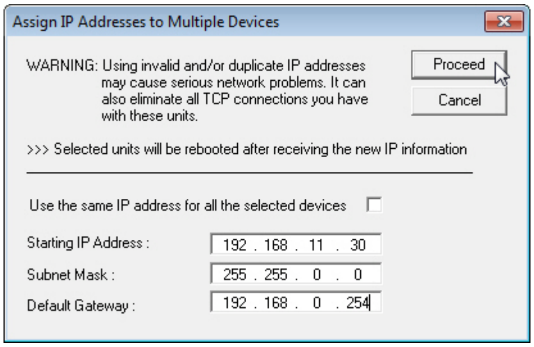
You can configure the network addresses for multiple DeviceMaster LTs using the **Assign IP to Multiple Devices** option.

In addition, you can also configure common settings for the DeviceMaster LT SocketServer or NS-Link web page and save the settings to a configuration file that you can load to all or selected DeviceMaster LTs. See *Using SocketServer Configuration Files* on Page 81 for more information.

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

1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 15) and **Scan** the network.
2. Shift-click the DeviceMaster LTs for which you want to program network information, right-click, and click **Advanced > Assign IP to Multiple Devices**.
3. Enter the starting IP address, subnet mask, IP Gateway and click **Proceed**.

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



Assign IP Addresses to Multiple Devices

WARNING: Using invalid and/or duplicate IP addresses may cause serious network problems. It can also eliminate all TCP connections you have with these units.

>>> 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 . 30

Subnet Mask : 255 . 255 . 0 . 0

Default Gateway : 192 . 168 . 0 . 254

Adding a New Device in PortVision DX

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

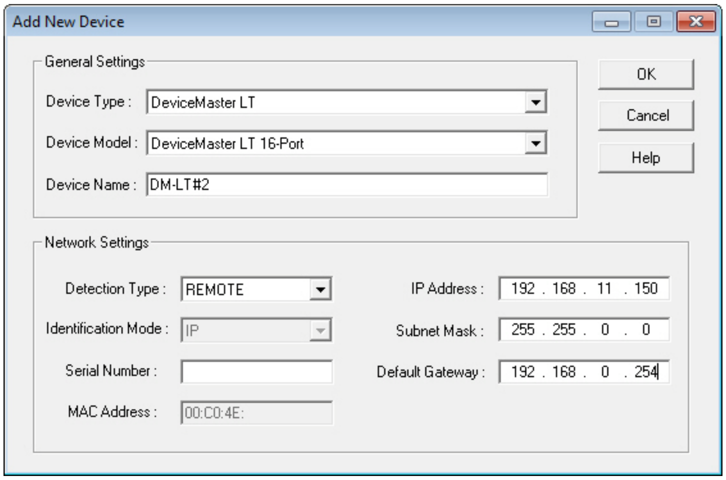
- Configure DeviceMaster LT units that are not on the local network (remote) using *Remote Using the IP Address* on Page 79.
- Pre-configure a DeviceMaster LT in PortVision DX (local) using *Local Using the IP Address or MAC Address* on Page 80.

Remote Using the IP Address

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

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

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



Add New Device

General Settings

Device Type : DeviceMaster LT

Device Model : DeviceMaster LT 16-Port

Device Name : DM-LT#2

Network Settings

Detection Type : REMOTE

Identification Mode : IP

Serial Number :

MAC Address : 00:C0:4E:

IP Address : 192 . 168 . 11 . 150

Subnet Mask : 255 . 255 . 0 . 0

Default Gateway : 192 . 168 . 0 . 254

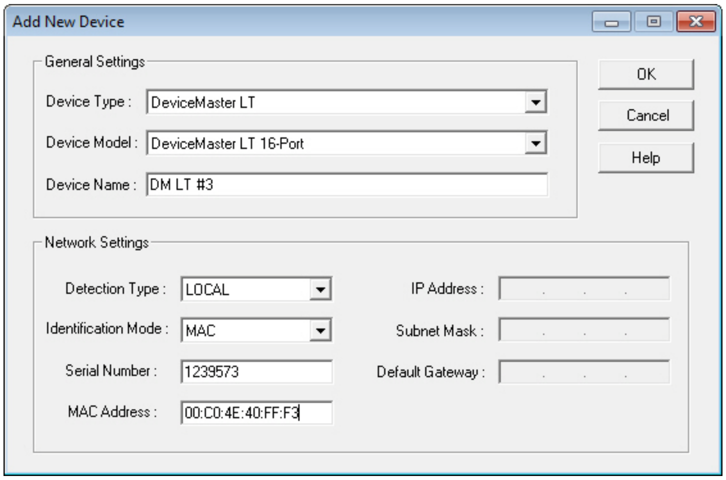
8. Click **Ok** to close the *Add New Device* window. It may take a few moments to save the DeviceMaster LT.

9. If necessary, click **Refresh** for the new DeviceMaster LT to display in the *Device Tree* or *Device List* panes. The DeviceMaster LT shows OFF-LINE if it is not attached to the network or if an incorrect IP address was entered.

Local Using the IP Address or MAC Address

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

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



Add New Device

General Settings

Device Type : DeviceMaster LT

Device Model : DeviceMaster LT 16-Port

Device Name : DM LT #3

Network Settings

Detection Type : LOCAL

Identification Mode : MAC

Serial Number : 1239573

MAC Address : 00:C0:4E:40:FF:F3

IP Address : . . .

Subnet Mask : . . .

Default Gateway : . . .

4. Select the appropriate model in the **Device Model** drop list.
5. Enter a friendly device name in the **Device Name** list box.

6. Select **LOCAL** for the *Detection Type*.
7. Enter the MAC address or network information.

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

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

Using SocketServer Configuration Files

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

- *PortVision DX - Saving a SocketServer Configuration File*
- *PortVision DX - Loading a SocketServer Configuration File* on Page 82
- *SocketServer - Saving Configuration Files* on Page 82
- *SocketServer - Loading Configuration Files* on Page 83

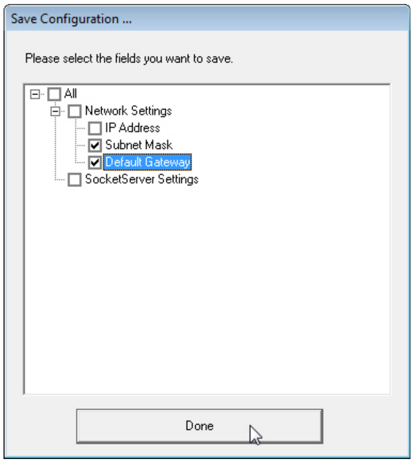
If you save a SocketServer configuration file using PortVision DX, you can choose what settings you want to save or load.

You may want to program the network settings in multiple DeviceMaster LTs using *Configuring Multiple DeviceMaster LTs Network Addresses* on Page 79.

PortVision DX - Saving a SocketServer Configuration File

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

Note: *Optionally, you can save a configuration file by accessing the* **Software Settings** *tab in the* **Properties** *screen and then clicking the* **Save Settings to a File** *button.*



Save Configuration ...

Please select the fields you want to save.

□ All
□ Network Settings
□ IP Address
☑ Subnet Mask
☑ Default Gateway
□ SocketServer Settings

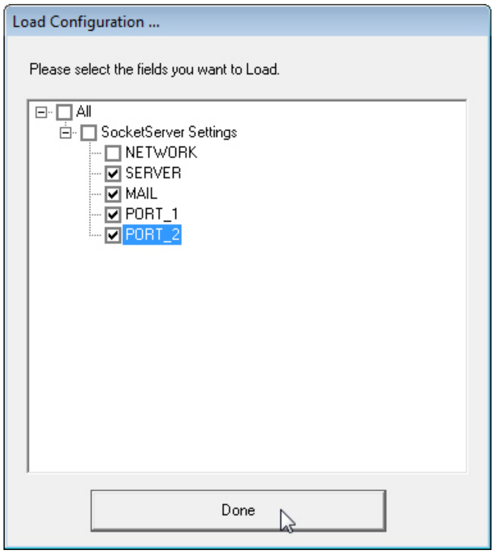
1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 15) and **Scan** the network.
2. Highlight the DeviceMaster LT in the *Device List* pane that you want to save its configuration and use one of the following methods:
   - Click the **Save** button.
   - Right-click and then click **Configuration > Save**.
3. Browse to the location you want to save the file, enter a file name, and click **Save**.
4. Click the **All** check box or click only the properties that you want saved for each property page in the configuration file and click **Done**.
5. Click **Ok** to close the *Save Configuration Completed* message.

PortVision DX - Loading a SocketServer Configuration File

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

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

1. Highlight the device or devices in the *Device List* pane that you want to load and use one of the following methods:
   - Click the **Load** button
   - Right-click and then click **Configuration > Load**
2. Click **Yes** to the warning that it will take 25 seconds per device and it may also reboot the devices.
3. Browse to the location of the configuration file, click the file name (**.dc**) and then **Open**.
4. Click the **All** check box or click only the properties that you want to load for each property page in the configuration file and then click **Done**.



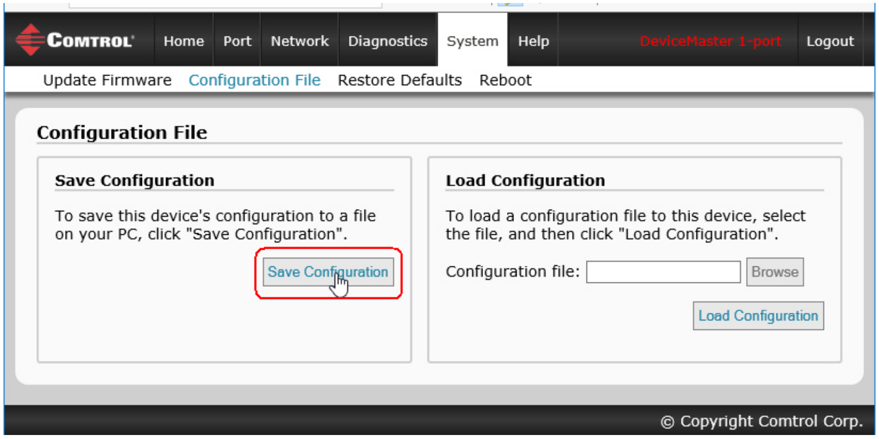
Note: *If you click* **All**, *every selected DeviceMaster LTs will be programmed with the same IP address.*

5. Close the *Load Configuration* popup message.

SocketServer - Saving Configuration Files

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

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



Configuration File

Save Configuration

To save this device's configuration to a file on your PC, click "Save Configuration".

Load Configuration

To load a configuration file to this device, select the file, and then click "Load Configuration".

Configuration file:

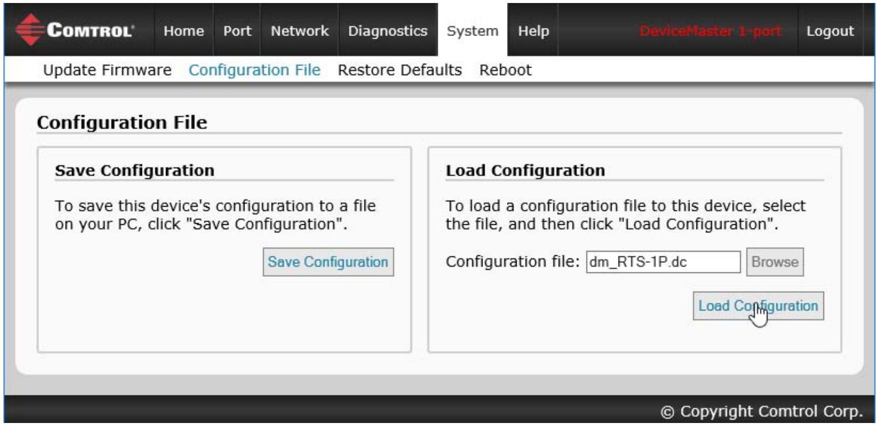
4. Save the configuration file to an appropriate location.

SocketServer - Loading Configuration Files

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

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

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


COMTROL
Home
Port
Network
Diagnostics
System
Help
DeviceMaster 1-port
Logout
Update Firmware
Configuration File
Restore Defaults
Reboot
Configuration File
Save Configuration
To save this device's configuration to a file on your PC, click "Save Configuration".
Save Configuration
Load Configuration
To load a configuration file to this device, select the file, and then click "Load Configuration".
Configuration file: dm_RTS-1P.dc
Browse
Load Configuration
© Copyright Comtrol Corp.

Using Driver Configuration Files

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

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

Saving Driver Configuration Files

You must save the driver configuration file in portions:

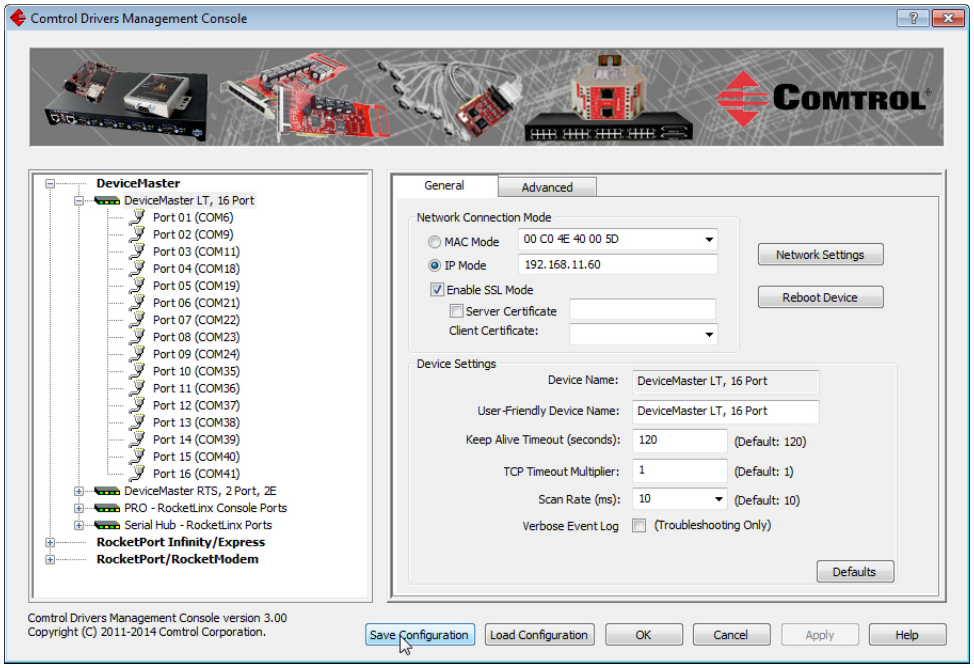
- Device-level configuration parameters.
- Port configuration parameters. You must upload each port's configuration parameters separately.

Saving Device-Level Configuration

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

1. If necessary, open the *Comtrol Drivers Management Console* using one of these methods:
   - ***Windows Control Panel;*** go to your *Control Panel* and click the **Comtrol Drivers Management Console**.
   - ***Shortcut***; located under **Start> Program Files> Comtrol> DeviceMaster LT> Comtrol Drivers Management Console**.
2. Depending on your operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* User Account Control message.

3. Highlight the DeviceMaster LT for which you want to save the driver configuration.
4. Click **Save Configuration**.



Network Connection Mode

○ MAC Mode: 00 C0 4E 40 00 5D

● IP Mode: 192.168.11.60

☑ Enable SSL Mode

□ Server Certificate

Client Certificate:

Device Settings

Device Name: DeviceMaster LT, 16 Port

User-Friendly Device Name: DeviceMaster LT, 16 Port

Keep Alive Timeout (seconds): 120 (Default: 120)

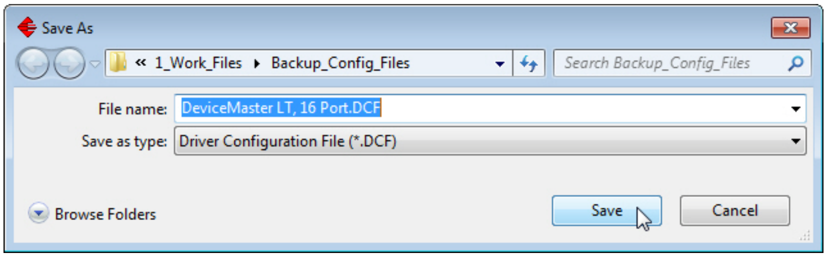
TCP Timeout Multiplier: 1 (Default: 1)

Scan Rate (ms): 10 (Default: 10)

Verbose Event Log □ (Troubleshooting Only)

Comtrol Drivers Management Console version 3.00
Copyright (C) 2011-2014 Comtrol Corporation.

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


Save As
« 1_Work_Files ▸ Backup_Config_Files
Search Backup_Config_Files
Browse Folders
Save
Cancel

File name: DeviceMaster LT, 16 Port.DCF

Save as type: Driver Configuration File (*.DCF)

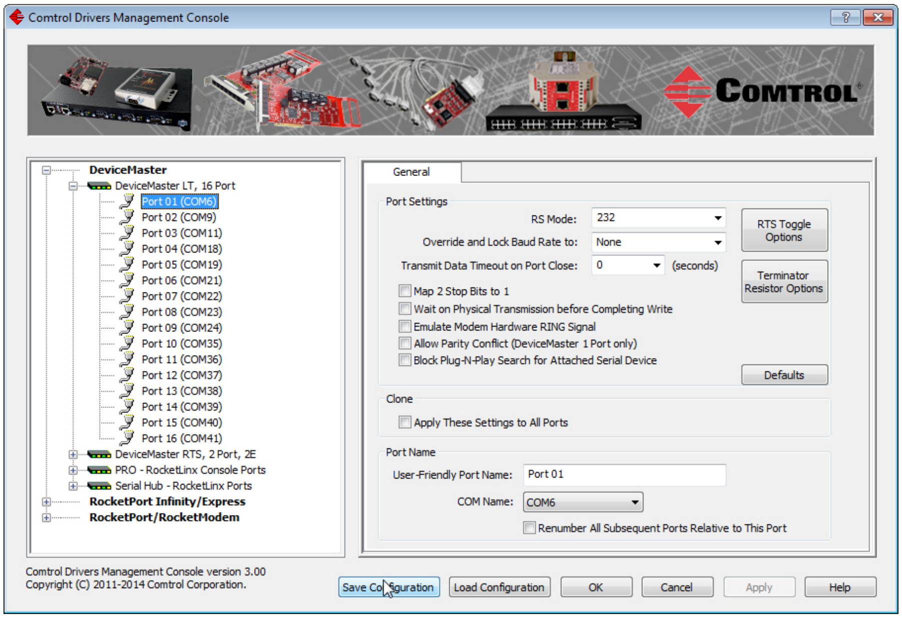
6. Repeat the previous steps for each DeviceMaster LT for which you want to save the driver configuration.

Saving Port-Level Configuration

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

1. If necessary, open the *Comtrol Drivers Management Console* using one of these methods:
   - ***Windows Control Panel;*** go to your *Control Panel* and click the **Comtrol Drivers Management Console**.
   - ***Shortcut***; located under **Start> Program Files> Comtrol> DeviceMaster LT> Comtrol Drivers Management Console**.
2. Depending on your operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* User Account Control message.
3. Highlight the DeviceMaster LT for which you want to save the port-level configuration.

4. Highlight the port for which you want to save port configuration.



Comtrol Drivers Management Console

- DeviceMaster
  - DeviceMaster LT, 16 Port
    - Port 01 (COM6)
    - Port 02 (COM9)
    - Port 03 (COM11)
    - Port 04 (COM18)
    - Port 05 (COM19)
    - Port 06 (COM21)
    - Port 07 (COM22)
    - Port 08 (COM23)
    - Port 09 (COM24)
    - Port 10 (COM35)
    - Port 11 (COM36)
    - Port 12 (COM37)
    - Port 13 (COM38)
    - Port 14 (COM39)
    - Port 15 (COM40)
    - Port 16 (COM41)
  - DeviceMaster RTS, 2 Port, 2E
  - PRO - RocketLinx Console Ports
  - Serial Hub - RocketLinx Ports
- RocketPort Infinity/Express
- RocketPort/RocketModem

General

Port Settings

RS Mode: 232

Override and Lock Baud Rate to: None

Transmit Data Timeout on Port Close: 0 (seconds)

□ Map 2 Stop Bits to 1

□ Wait on Physical Transmission before Completing Write

□ Emulate Modem Hardware RING Signal

□ Allow Parity Conflict (DeviceMaster 1 Port only)

□ Block Plug-N-Play Search for Attached Serial Device

Clone

□ Apply These Settings to All Ports

Port Name

User-Friendly Port Name: Port 01

COM Name: COM6

□ Renumber All Subsequent Ports Relative to This Port

Comtrol Drivers Management Console version 3.00
Copyright (C) 2011-2014 Comtrol Corporation.

5. Click **Save Configuration.**

6. Repeat this process for each port for which you want to save the configuration settings.

Loading Driver Configuration Files

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

The driver configuration file uploads in portions:

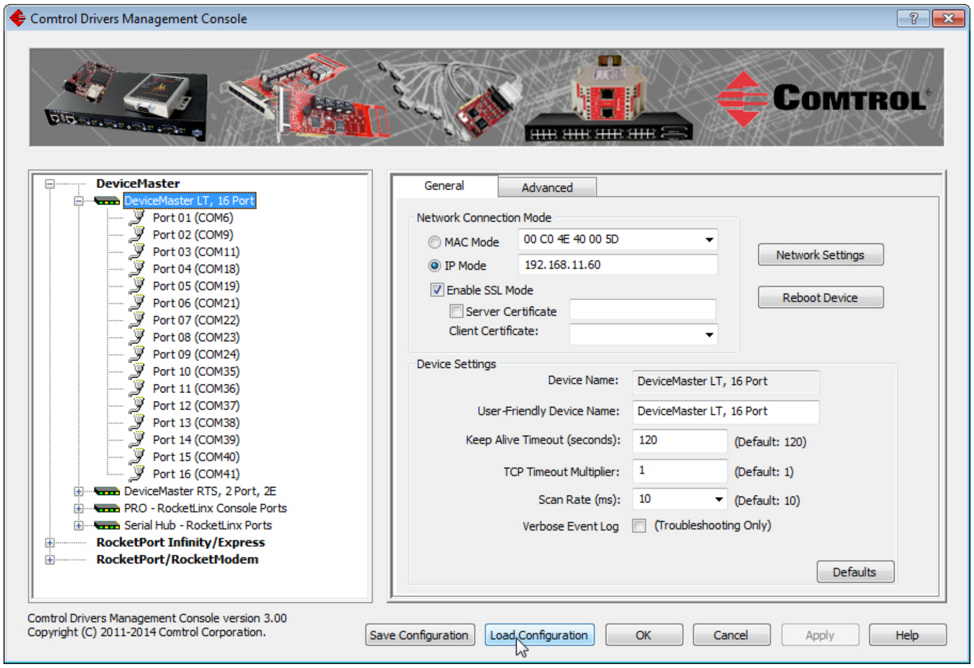
- Device-level configuration parameters.
- Port configuration parameters. You must upload each port's configuration parameters separately.

Loading Device Configuration

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

1. If necessary, open the *Comtrol Drivers Management Console* using one of these methods:
   - ***Windows Control Panel;*** go to your *Control Panel* and click on the **Comtrol Drivers Management Console**.
   - ***Shortcut***; located under **Start> Program Files> Comtrol> DeviceMaster LT> Comtrol Drivers Management Console**.
2. Depending on your operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* User Account Control message.

3. In the left pane, highlight the DeviceMaster LT for which you want to load the device-level settings from the configuration file.



Comtrol Drivers Management Console

- DeviceMaster
  - DeviceMaster LT, 16 Port
    - Port 01 (COM6)
    - Port 02 (COM9)
    - Port 03 (COM11)
    - Port 04 (COM18)
    - Port 05 (COM19)
    - Port 06 (COM21)
    - Port 07 (COM22)
    - Port 08 (COM23)
    - Port 09 (COM24)
    - Port 10 (COM35)
    - Port 11 (COM36)
    - Port 12 (COM37)
    - Port 13 (COM38)
    - Port 14 (COM39)
    - Port 15 (COM40)
    - Port 16 (COM41)
  - DeviceMaster RTS, 2 Port, 2E
  - PRO - RocketLinx Console Ports
  - Serial Hub - RocketLinx Ports
- RocketPort Infinity/Express
- RocketPort/RocketModem

General | Advanced

Network Connection Mode

○ MAC Mode: 00 C0 4E 40 00 5D

● IP Mode: 192.168.11.60

☑ Enable SSL Mode

□ Server Certificate

Client Certificate:

Device Settings

Device Name: DeviceMaster LT, 16 Port

User-Friendly Device Name: DeviceMaster LT, 16 Port

Keep Alive Timeout (seconds): 120 (Default: 120)

TCP Timeout Multiplier: 1 (Default: 1)

Scan Rate (ms): 10 (Default: 10)

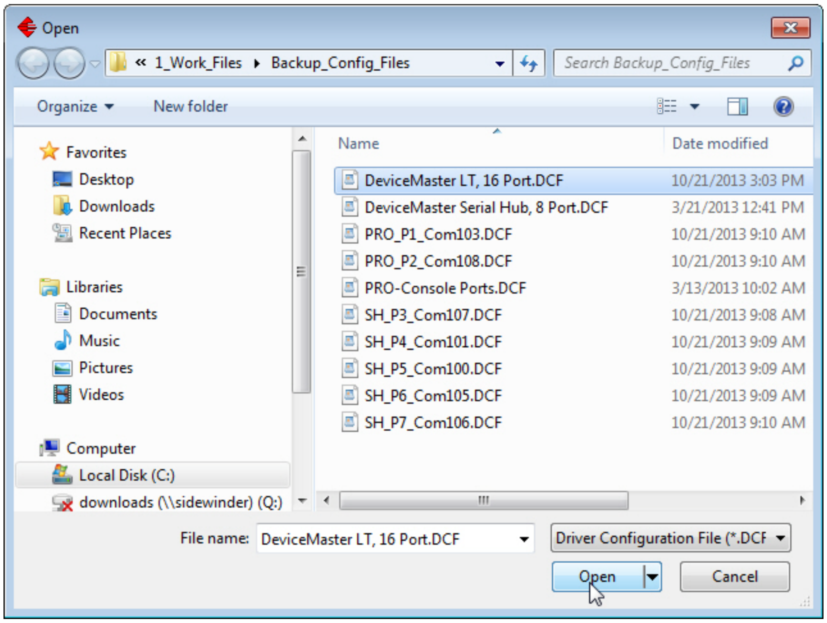
Verbose Event Log □ (Troubleshooting Only)

Comtrol Drivers Management Console version 3.00
Copyright (C) 2011-2014 Comtrol Corporation.

4. Click **Load Configuration**.

5. Browse to the location of the configuration file that you want to load.

6. Highlight the configuration file and click **Open**. The configuration file loads in a few moments.



Open

« 1_Work_Files ▸ Backup_Config_Files

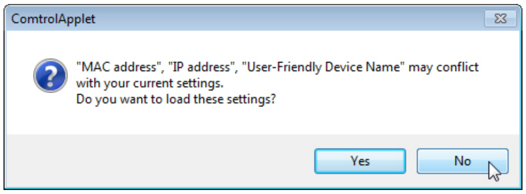
Name	Date modified
DeviceMaster LT, 16 Port.DCF	10/21/2013 3:03 PM
DeviceMaster Serial Hub, 8 Port.DCF	3/21/2013 12:41 PM
PRO_P1_Com103.DCF	10/21/2013 9:10 AM
PRO_P2_Com108.DCF	10/21/2013 9:10 AM
PRO-Console Ports.DCF	3/13/2013 10:02 AM
SH_P3_Com107.DCF	10/21/2013 9:08 AM
SH_P4_Com101.DCF	10/21/2013 9:09 AM
SH_P5_Com100.DCF	10/21/2013 9:09 AM
SH_P6_Com105.DCF	10/21/2013 9:09 AM
SH_P7_Com106.DCF	10/21/2013 9:10 AM

File name: DeviceMaster LT, 16 Port.DCF

Driver Configuration File (*.DCF

7. Make the appropriate choice for your situation:
   - Click **No** to the *ComtrolApplet* message, if you are using the file to set up multiple DeviceMaster LTs with the same device-level settings.
   - Click **Yes** to the *ComtrolApplet* message, if you are using the file to restore a specific DeviceMaster LT. For example, you needed to remove and then

re-install the DeviceMaster LT NS-Link device driver.



"MAC address", "IP address", "User-Friendly Device Name" may conflict with your current settings.
Do you want to load these settings?

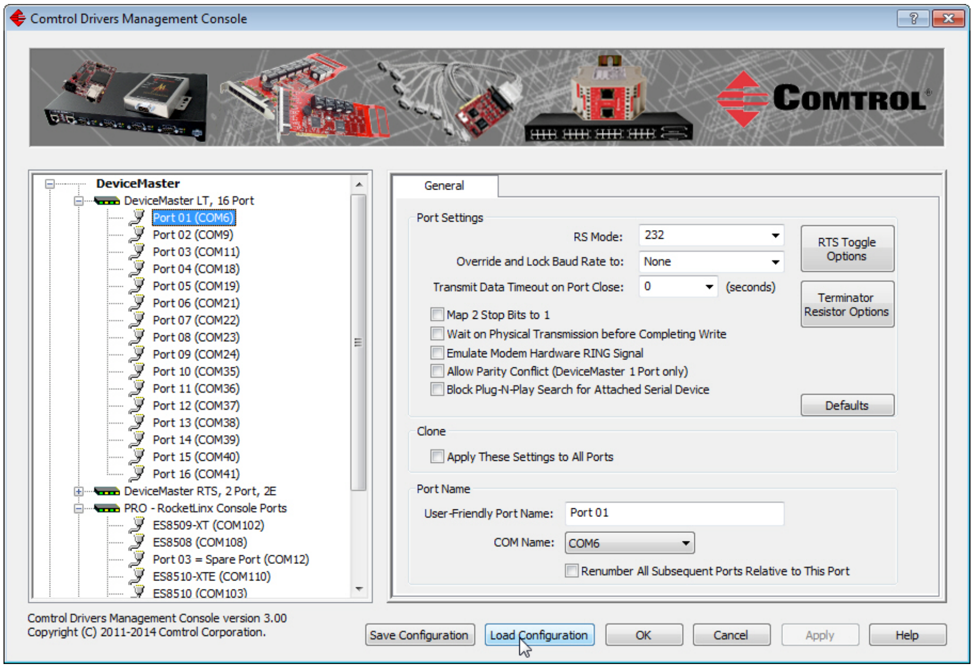
8. Click **Apply** so that the configuration is saved on the DeviceMaster LT.
9. Go to the next procedure if you want to restore port settings from a configuration file.

Loading Port Configuration

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

Note: *Device driver configuration files must be for the same model with the same port density*

1. If necessary, open the *Comtrol Drivers Management Console* using one of these methods:
   - ***Windows Control Panel;*** go to your *Control Panel* and click on the **Comtrol Drivers Management Console**.
   - ***Shortcut***; located under **Start> Program Files> Comtrol> DeviceMaster LT> Comtrol Drivers Management Console**.
2. Depending on your operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* User Account Control message.
3. In the left pane, highlight the port for which you want to load the port-level settings from the configuration file.



Port Settings

RS Mode: 232

Override and Lock Baud Rate to: None

Transmit Data Timeout on Port Close: 0 (seconds)

□ Map 2 Stop Bits to 1
□ Wait on Physical Transmission before Completing Write
□ Emulate Modem Hardware RING Signal
□ Allow Parity Conflict (DeviceMaster 1 Port only)
□ Block Plug-N-Play Search for Attached Serial Device

Clone

□ Apply These Settings to All Ports

Port Name

User-Friendly Port Name: Port 01

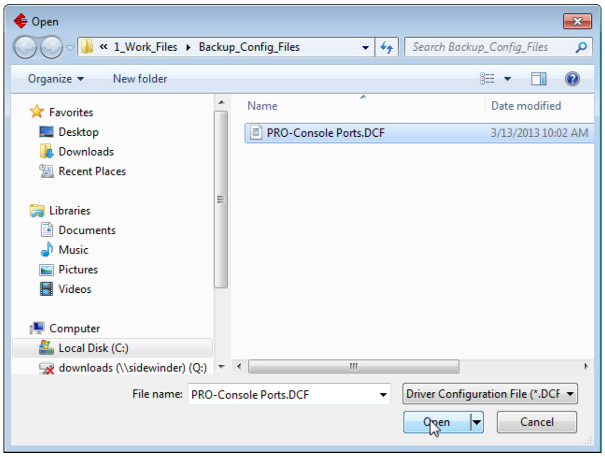
COM Name: COM6

□ Renumber All Subsequent Ports Relative to This Port

Comtrol Drivers Management Console version 3.00
Copyright (C) 2011-2014 Comtrol Corporation.

4. Click **Load Configuration**.
5. Browse to the location of the configuration file that you want to load.

6. Highlight the configuration file and click **Open**. The configuration file loads in a few moments.



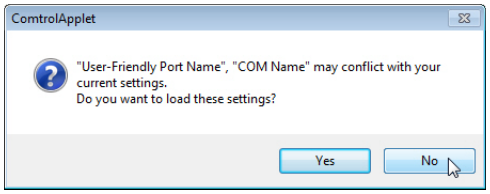
Open

« 1_Work_Files ▸ Backup_Config_Files

File name: PRO-Console Ports.DCF

Driver Configuration File (*.DCF

7. Make the appropriate choice for your situation:
   - Click **No** to the *ComtrolApplet* message, if you are using the file to set up multiple DeviceMaster LTs with the same port-level settings.
   - Click **Yes** to the *ComtrolApplet* message, if you are using the file to restore a specific DeviceMaster LT. For example, you needed to remove and then re-install the DeviceMaster LT NS-Link device driver.



ComtrolApplet

"User-Friendly Port Name", "COM Name" may conflict with your current settings.
Do you want to load these settings?

8. Click **Apply** so that the configuration is saved on the DeviceMaster LT.

9. Repeat Steps 3 through 8 for each port that you want to restore.

Changing the Bootloader Timeout

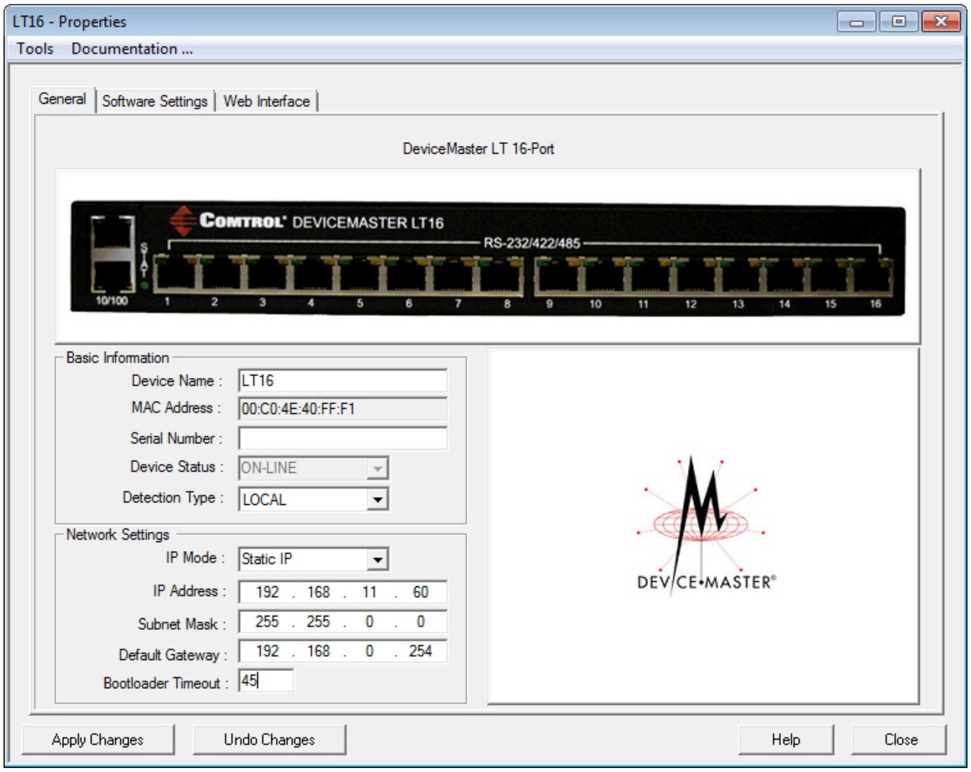
If SocketServer fails during the upload process, you should change the **Bootloader timeout** value to 45 seconds.

Note: *The DeviceMaster LT 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 19.*

PortVision DX - Changing Bootloader Timeout

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

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



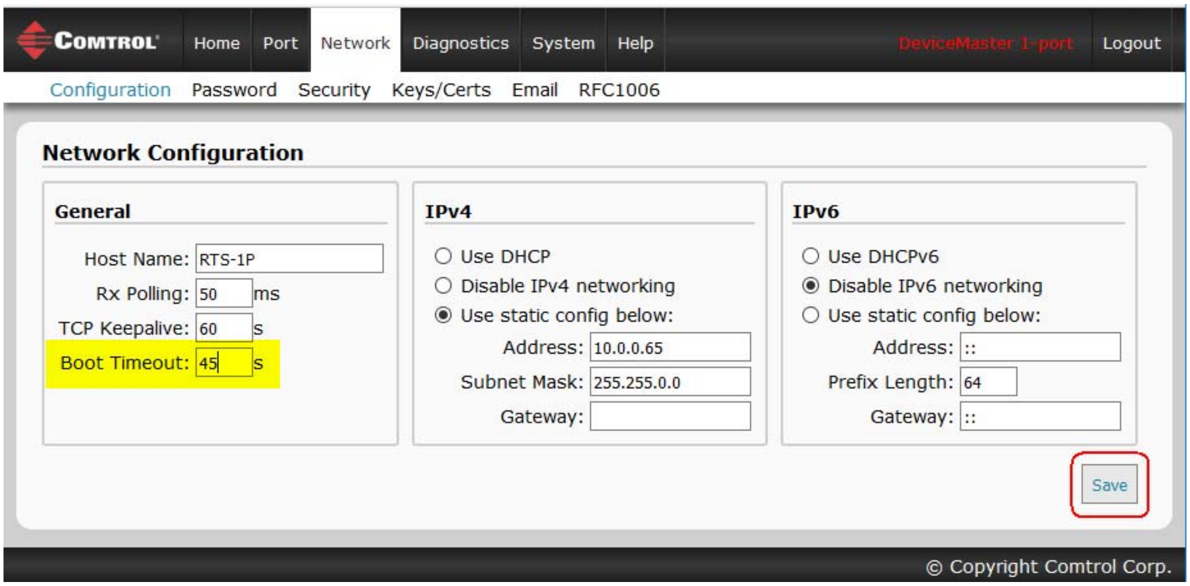
Device Name : LT16
MAC Address : 00:C0:4E:40:FF:F1
Serial Number :
Device Status : ON-LINE
Detection Type : LOCAL
IP Mode : Static IP
IP Address : 192 . 168 . 11 . 60
Subnet Mask : 255 . 255 . 0 . 0
Default Gateway : 192 . 168 . 0 . 254
Bootloader Timeout : 45

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

SocketServer - Changing Bootloader Timeout

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

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



Network Configuration

General

Host Name: RTS-1P
Rx Polling: 50 ms
TCP Keepalive: 60 s
Boot Timeout: 45 s

IPv4

○ Use DHCP
○ Disable IPv4 networking
● Use static config below:
Address: 10.0.0.65
Subnet Mask: 255.255.0.0
Gateway:

IPv6

○ Use DHCPv6
● Disable IPv6 networking
○ Use static config below:
Address: ::
Prefix Length: 64
Gateway: ::

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

Managing Bootloader

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

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

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

- **PortVision DX** is the easiest way to check the Bootloader version and upload the latest version.
- Optionally, RedBoot can be used to check the Bootloader version and update the Bootloader. See *RedBoot Procedures* on Page 105 for procedures.

Checking the Bootloader Version

The following procedure uses PortVision DX to check the Bootloader version. Optionally, you can use RedBoot, see *Determining the Bootloader Version* on Page 109.

1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 15) and **Scan** the network.
2. Right-click the DeviceMaster LT in the *Device List* pane and click **Advanced > Reboot**.
3. Click **Yes** to the *Confirm Reboot* query.
4. Right-click the DeviceMaster LT in the *Device List* pane, click **Refresh.** You may need to do this several times until you catch the reboot cycle in the *Device List* pane. The Bootloader version is briefly displayed during the reboot cycle before SocketServer loads.
5. Check the Comtrol web site to see if a later version is available.
6. Go to the next subsection if you need upload a new version of Bootloader.

Uploading Bootloader

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

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

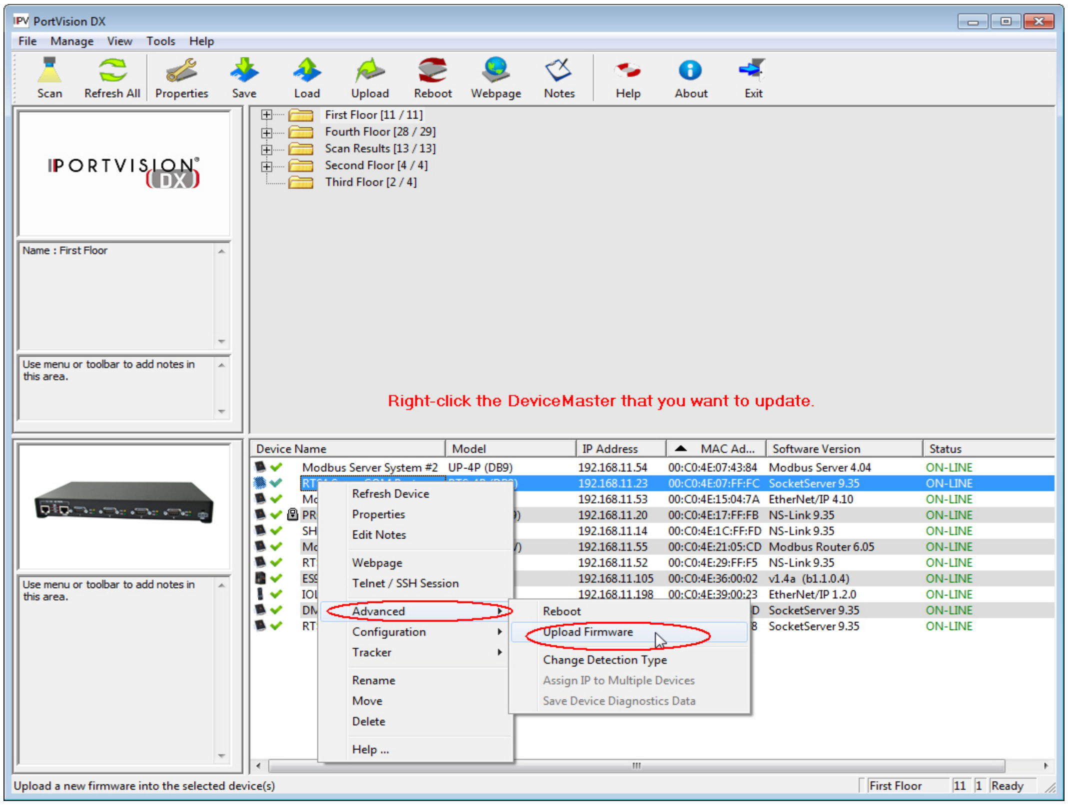
⚠ Caution

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

If you are not successful uploading SocketServerinto the DeviceMaster LT, do not upload Bootloader.

1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 15) and **Scan** the network.
2. If necessary, check the Bootloader version (*Checking the Bootloader Version*) and download the latest version.

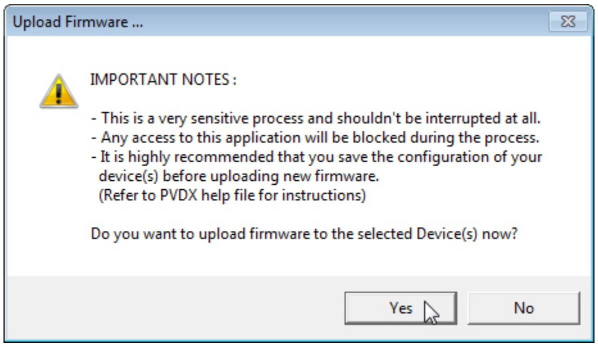
3. Right-click the DeviceMaster LT for which you want to update, click **Advanced > Upload Firmware**, browse to the Bootloader **.cmtl** file, and then click **Open**.



Right-click the DeviceMaster that you want to update.

Device Name	Model	IP Address	MAC Ad...	Software Version	Status
Modbus Server System #2	UP-4P (DB9)	192.168.11.54	00:C0:4E:07:43:84	Modbus Server 4.04	ON-LINE
RT	)	192.168.11.23	00:C0:4E:07:FF:FC	SocketServer 9.35	ON-LINE
Mc		192.168.11.53	00:C0:4E:15:04:7A	EtherNet/IP 4.10	ON-LINE
PR	9)	192.168.11.20	00:C0:4E:17:FF:FB	NS-Link 9.35	ON-LINE
SH		192.168.11.14	00:C0:4E:1C:FF:FD	NS-Link 9.35	ON-LINE
Mc	/)	192.168.11.55	00:C0:4E:21:05:CD	Modbus Router 6.05	ON-LINE
RT		192.168.11.52	00:C0:4E:29:FF:F5	NS-Link 9.35	ON-LINE
ES		192.168.11.105	00:C0:4E:36:00:02	v1.4a (b1.1.0.4)	ON-LINE
IOL		192.168.11.198	00:C0:4E:39:00:23	EtherNet/IP 1.2.0	ON-LINE
DM			D	SocketServer 9.35	ON-LINE
RT			8	SocketServer 9.35	ON-LINE

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



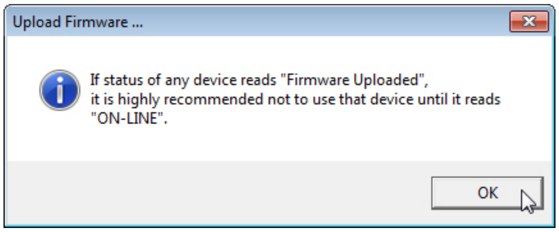
IMPORTANT NOTES :

- This is a very sensitive process and shouldn't be interrupted at all.
- Any access to this application will be blocked during the process.
- It is highly recommended that you save the configuration of your device(s) before uploading new firmware. (Refer to PVDX help file for instructions)

Do you want to upload firmware to the selected Device(s) now?

5. Click **Ok** to the second *Upload Firmware* message.

6. Right-click the DeviceMaster LT and click **Refresh** until the Bootloader version displays in the *Device List* pane and verify that the new version loaded.

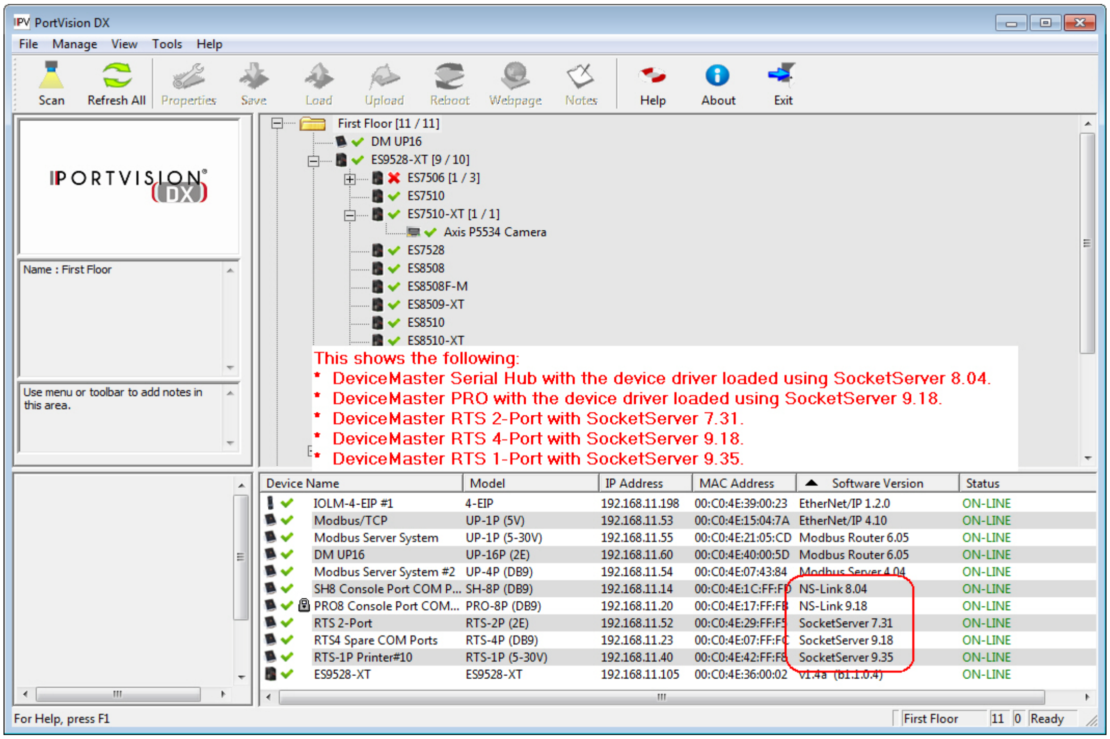


If status of any device reads "Firmware Uploaded", it is highly recommended not to use that device until it reads "ON-LINE".

Checking the NS-Link Version

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

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



This shows the following:
- DeviceMaster Serial Hub with the device driver loaded using SocketServer 8.04.
- DeviceMaster PRO with the device driver loaded using SocketServer 9.18.
- DeviceMaster RTS 2-Port with SocketServer 7.31.
- DeviceMaster RTS 4-Port with SocketServer 9.18.
- DeviceMaster RTS 1-Port with SocketServer 9.35.

Device Name	Model	IP Address	MAC Address	▲ Software Version	Status
IOLM-4-EIP #1	4-EIP	192.168.11.198	00:C0:4E:39:00:23	EtherNet/IP 1.2.0	ON-LINE
Modbus/TCP	UP-1P (5V)	192.168.11.53	00:C0:4E:15:04:7A	EtherNet/IP 4.10	ON-LINE
Modbus Server System	UP-1P (5-30V)	192.168.11.55	00:C0:4E:21:05:CD	Modbus Router 6.05	ON-LINE
DM UP16	UP-16P (2E)	192.168.11.60	00:C0:4E:40:00:5D	Modbus Router 6.05	ON-LINE
Modbus Server System #2	UP-4P (DB9)	192.168.11.54	00:C0:4E:07:43:84	Modbus Server 4.04	ON-LINE
SH8 Console Port COM P...	SH-8P (DB9)	192.168.11.14	00:C0:4E:1C:FF:FD	NS-Link 8.04	ON-LINE
PRO8 Console Port COM...	PRO-8P (DB9)	192.168.11.20	00:C0:4E:17:FF:FB	NS-Link 9.18	ON-LINE
RTS 2-Port	RTS-2P (2E)	192.168.11.52	00:C0:4E:29:FF:F5	SocketServer 7.31	ON-LINE
RTS4 Spare COM Ports	RTS-4P (DB9)	192.168.11.23	00:C0:4E:07:FF:FC	SocketServer 9.18	ON-LINE
RTS-1P Printer#10	RTS-1P (5-30V)	192.168.11.40	00:C0:4E:42:FF:F8	SocketServer 9.35	ON-LINE
ES9528-XT	ES9528-XT	192.168.11.105	00:C0:4E:36:00:02	v1.4a (b1.1.0.4)	ON-LINE

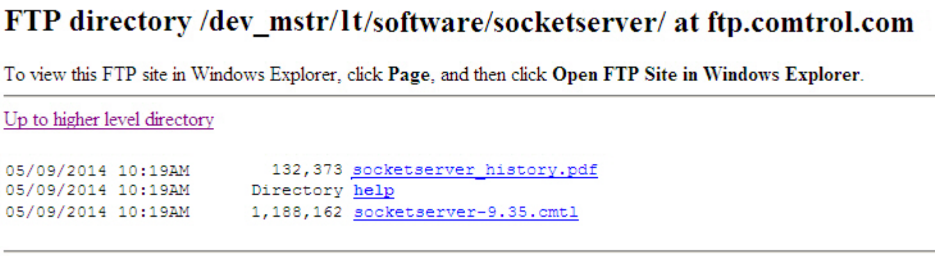
The *Device List* pane displays the NS-Link (SocketServer) version.

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

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

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

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



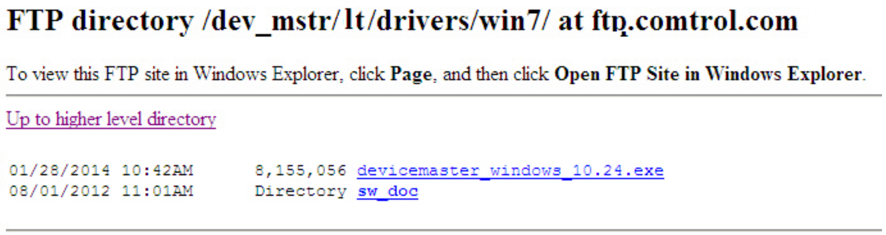
FTP directory /dev_mstr/lt/software/socketserver/ at ftp.comtrol.com

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

Up to higher level directory

```
05/09/2014 10:19AM        132,373 socketserver_history.pdf
05/09/2014 10:19AM      Directory help
05/09/2014 10:19AM      1,188,162 socketserver-9.35.cmtl
```

5. If a higher version of SocketServer is available and you want to update the DeviceMaster LT with the latest software:
   a. Update SocketServer using *Uploading SocketServer with PortVision DX* on Page 25.
   b. Download the latest driver from ftp://ftp.comtrol.com/dev_mstr/LT/drivers/win7.



FTP directory /dev_mstr/lt/drivers/win7/ at ftp.comtrol.com

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

Up to higher level directory

```
01/28/2014 10:42AM      8,155,056 devicemaster_windows_10.24.exe
08/01/2012 11:01AM      Directory sw_doc
```

   c. Update to the latest driver using the *DeviceMaster LT Device Driver (NS-Link) User Guide,* which can be downloaded using *Locating Software and Documentation* on Page 9.

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.

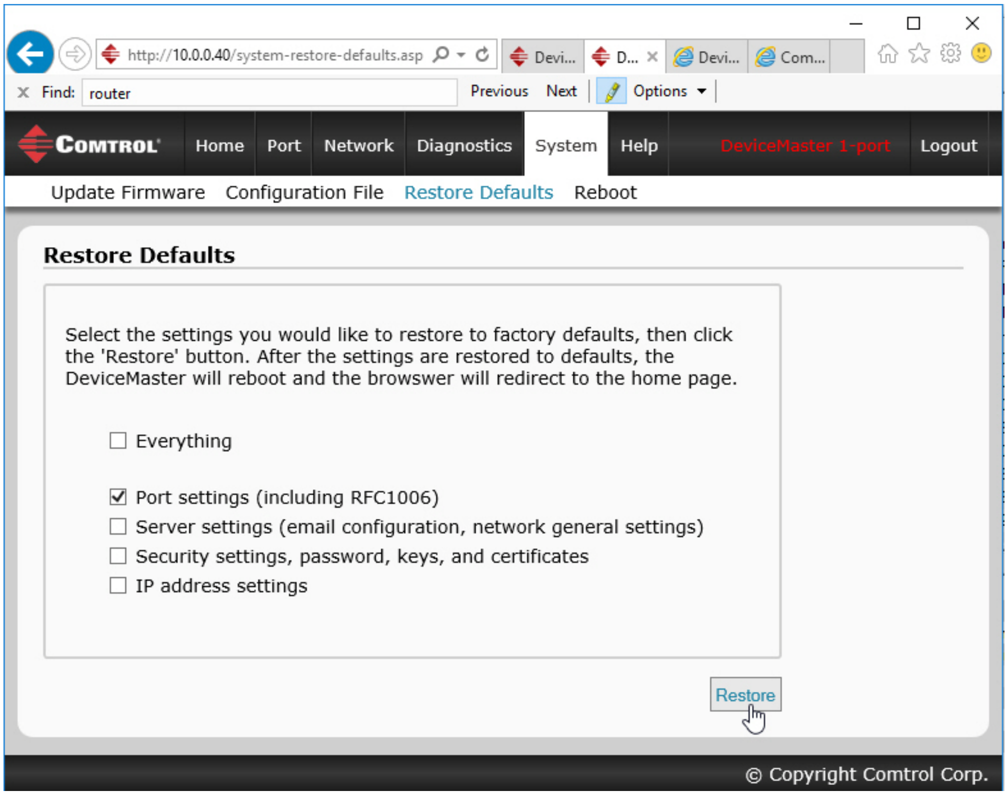
1. Open the *Comtrol Drivers Management Console* using **Start > Comtrol > DeviceMaster Management Console** or under *Control Panel*, **Comtrol Drivers Management Console**.
2. Highlight the first port that you want reset to default values.
3. Click the **Defaults** button (and if appropriate, **Clone**).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

If necessary, you can reset DeviceMaster LT 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 LT web page (*Accessing Socket Configuration* on Page 47).
2. Click **System | Restore Defaults**.
3. Click the **Port Settings (including RFC1006)** option and then click **Restore**.



Restore Defaults

Select the settings you would like to restore to factory defaults, then click the 'Restore' button. After the settings are restored to defaults, the DeviceMaster will reboot and the browswer will redirect to the home page.

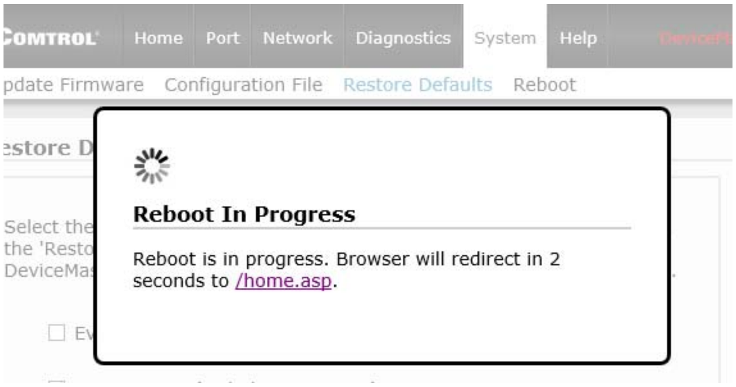
☐ Everything

☑ Port settings (including RFC1006)
☐ Server settings (email configuration, network general settings)
☐ Security settings, password, keys, and certificates
☐ IP address settings

Restore

© Copyright Comtrol Corp.

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



Reboot In Progress

Reboot is in progress. Browser will redirect in 2 seconds to /home.asp.

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

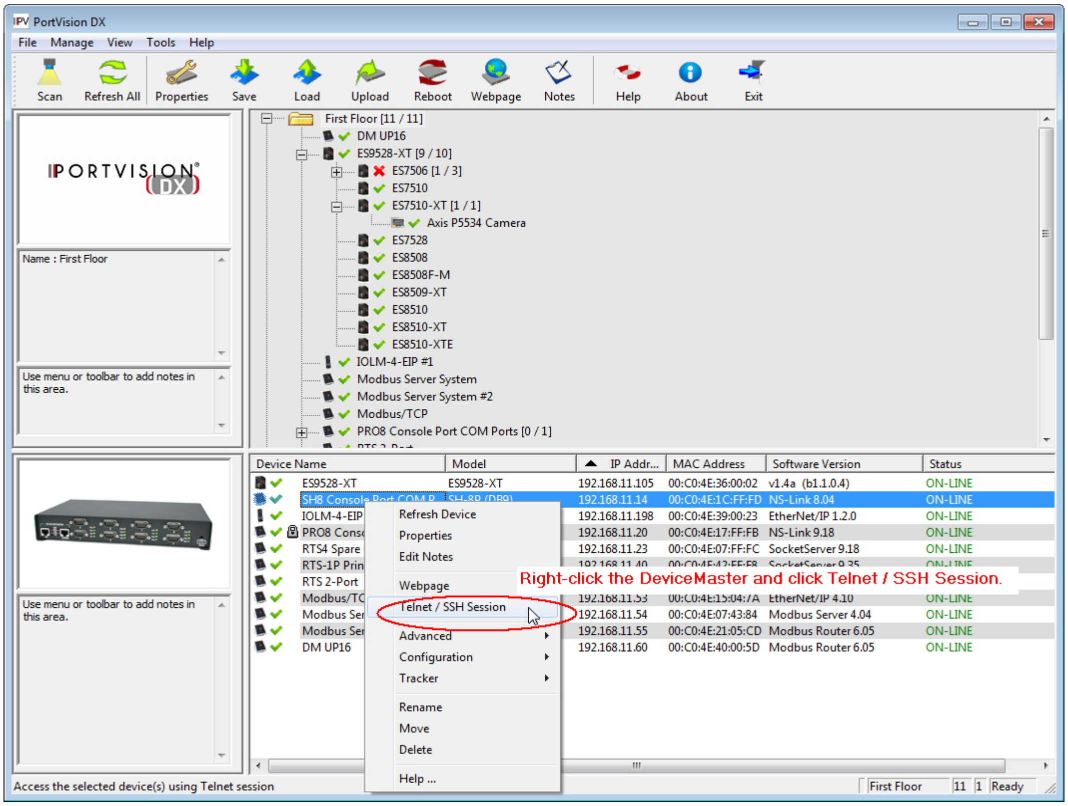
You can open a Telnet or SSH session using PortVision DX. Use the appropriate procedure for your site:

- *Telnet Session* (below)
- *SSH Session* on Page 98

Telnet Session

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

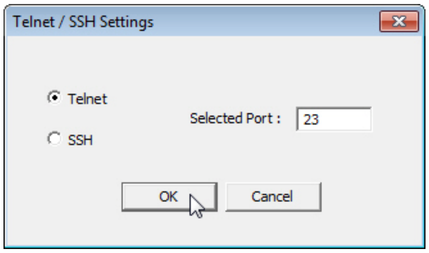
1. In PortVision DX, PortVision DX, right-click the DeviceMaster LT in the *Device List* pane for which you want to open a telnet session, and click **Telnet/ SSH Session**.



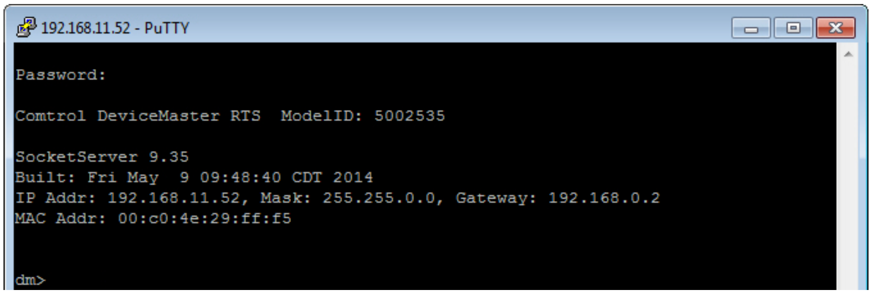
Device Name	Model	IP Addr...	MAC Address	Software Version	Status
ES9528-XT	ES9528-XT	192.168.11.105	00:C0:4E:36:00:02	v1.4a (b1.1.0.4)	ON-LINE
SH8 Console Port COM P	SH-8P (DB9)	192.168.11.14	00:C0:4E:1C:FF:FD	NS-Link 8.04	ON-LINE
IOLM-4-EIP		192.168.11.198	00:C0:4E:39:00:23	EtherNet/IP 1.2.0	ON-LINE
PRO8 Conso		192.168.11.20	00:C0:4E:17:FF:FB	NS-Link 9.18	ON-LINE
RTS4 Spare		192.168.11.23	00:C0:4E:07:FF:FC	SocketServer 9.18	ON-LINE
RTS-1P Prin		192.168.11.40	00:C0:4E:42:FF:F8	SocketServer 9.35	ON-LINE
RTS 2-Port					
Modbus/TC		192.168.11.53	00:C0:4E:15:04:7A	EtherNet/IP 4.10	ON-LINE
Modbus Ser		192.168.11.54	00:C0:4E:07:43:84	Modbus Server 4.04	ON-LINE
Modbus Ser		192.168.11.55	00:C0:4E:21:05:CD	Modbus Router 6.05	ON-LINE
DM UP16		192.168.11.60	00:C0:4E:40:00:5D	Modbus Router 6.05	ON-LINE

Right-click the DeviceMaster and click Telnet / SSH Session.

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

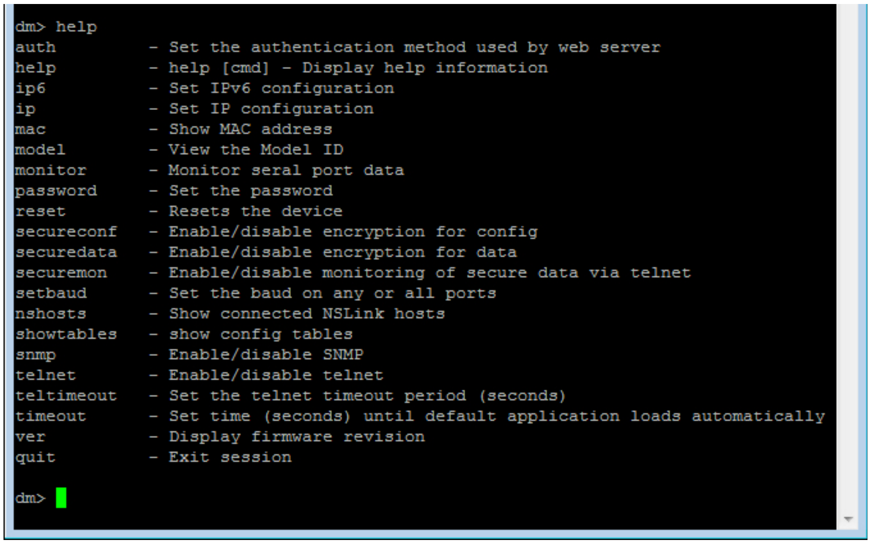


3. If necessary, enter the password and press **Enter**. If a password has not been set, press **Enter**.



```
Password:

Comtrol DeviceMaster RTS  ModelID: 5002535

SocketServer 9.35
Built: Fri May  9 09:48:40 CDT 2014
IP Addr: 192.168.11.52, Mask: 255.255.0.0, Gateway: 192.168.0.2
MAC Addr: 00:c0:4e:29:ff:f5


dm>
```

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

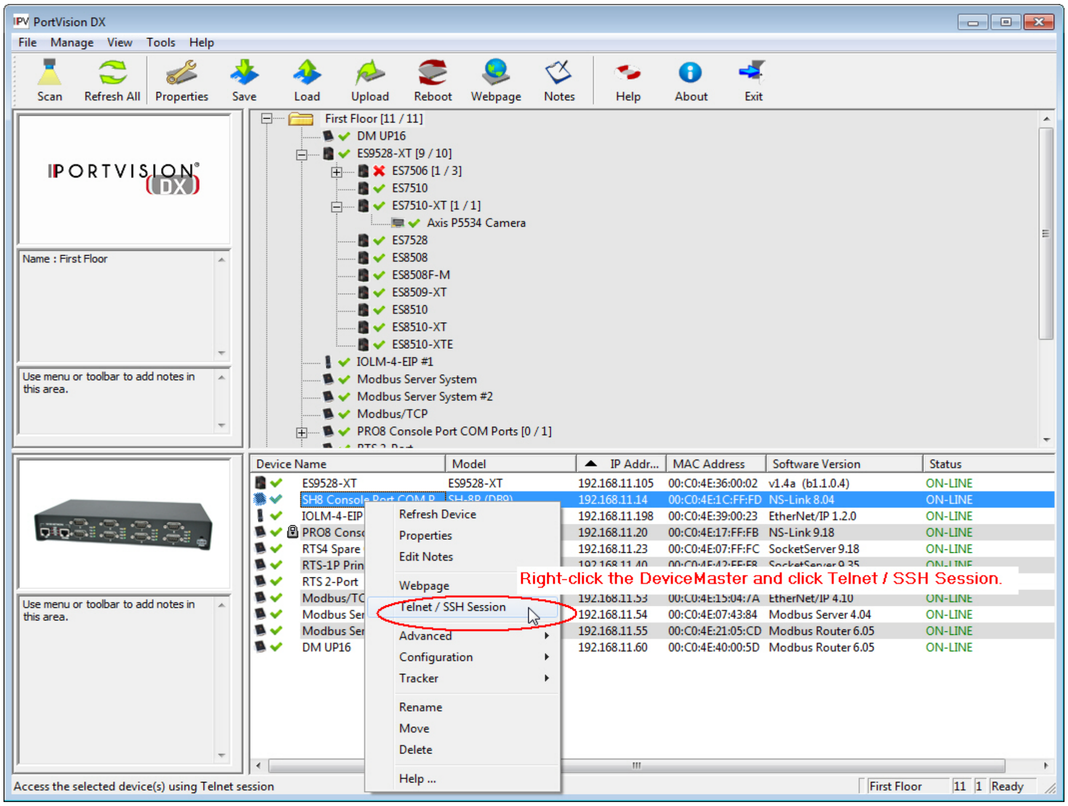


```
dm> help
auth          - Set the authentication method used by web server
help          - help [cmd] - Display help information
ip6           - Set IPv6 configuration
ip            - Set IP configuration
mac           - Show MAC address
model         - View the Model ID
monitor       - Monitor seral port data
password      - Set the password
reset         - Resets the device
secureconf    - Enable/disable encryption for config
securedata    - Enable/disable encryption for data
securemon     - Enable/disable monitoring of secure data via telnet
setbaud       - Set the baud on any or all ports
nshosts       - Show connected NSLink hosts
showtables    - show config tables
snmp          - Enable/disable SNMP
telnet        - Enable/disable telnet
teltimeout    - Set the telnet timeout period (seconds)
timeout       - Set time (seconds) until default application loads automatically
ver           - Display firmware revision
quit          - Exit session

dm>
```

SSH Session

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

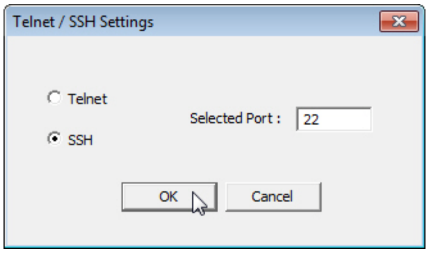
1. In PortVision DX, PortVision DX, right-click the DeviceMaster LT in the *Device List* pane for which you want to open an SSH session, and click **Telnet/ SSH Session**.



Device Name	Model	IP Addr...	MAC Address	Software Version	Status
ES9528-XT	ES9528-XT	192.168.11.105	00:C0:4E:36:00:02	v1.4a (b1.1.0.4)	ON-LINE
SH8 Console Port COM P...	SH-8P (DB9)	192.168.11.14	00:C0:4E:1C:FF:FD	NS-Link 8.04	ON-LINE
IOLM-4-EIP		192.168.11.198	00:C0:4E:39:00:23	EtherNet/IP 1.2.0	ON-LINE
PRO8 Consc...		192.168.11.20	00:C0:4E:17:FF:FB	NS-Link 9.18	ON-LINE
RTS4 Spare		192.168.11.23	00:C0:4E:07:FF:FC	SocketServer 9.18	ON-LINE
RTS-1P Prin...		192.168.11.40	00:C0:4E:42:FF:F8	SocketServer 9.35	ON-LINE
RTS 2-Port					
Modbus/TC...		192.168.11.53	00:C0:4E:15:04:7A	EtherNet/IP 4.10	ON-LINE
Modbus Ser...		192.168.11.54	00:C0:4E:07:43:84	Modbus Server 4.04	ON-LINE
Modbus Ser...		192.168.11.55	00:C0:4E:21:05:CD	Modbus Router 6.05	ON-LINE
DM UP16		192.168.11.60	00:C0:4E:40:00:5D	Modbus Router 6.05	ON-LINE

Right-click the DeviceMaster and click Telnet / SSH Session.

2. Click **SSH** and leave the port number at the default.

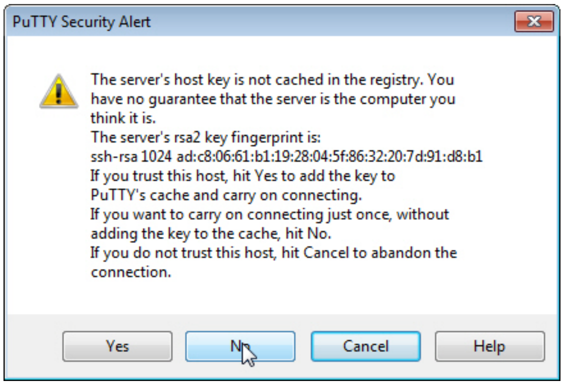


○ Telnet

● SSH

Selected Port : 22

3. If necessary (depending on the operating system), respond to the security notification.



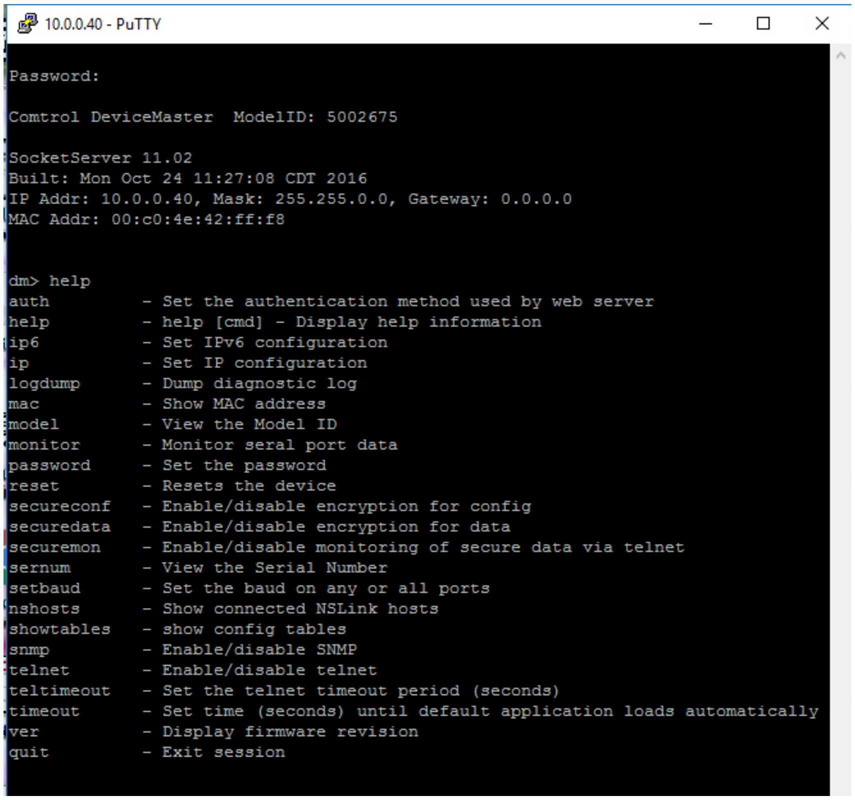
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 ad:c8:06:61:b1:19:28:04:5f:86:32:20:7d:91:d8:b1
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.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

4. Press **Enter**.

   ***Note:** The DeviceMaster LT does not have a user name.*

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

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



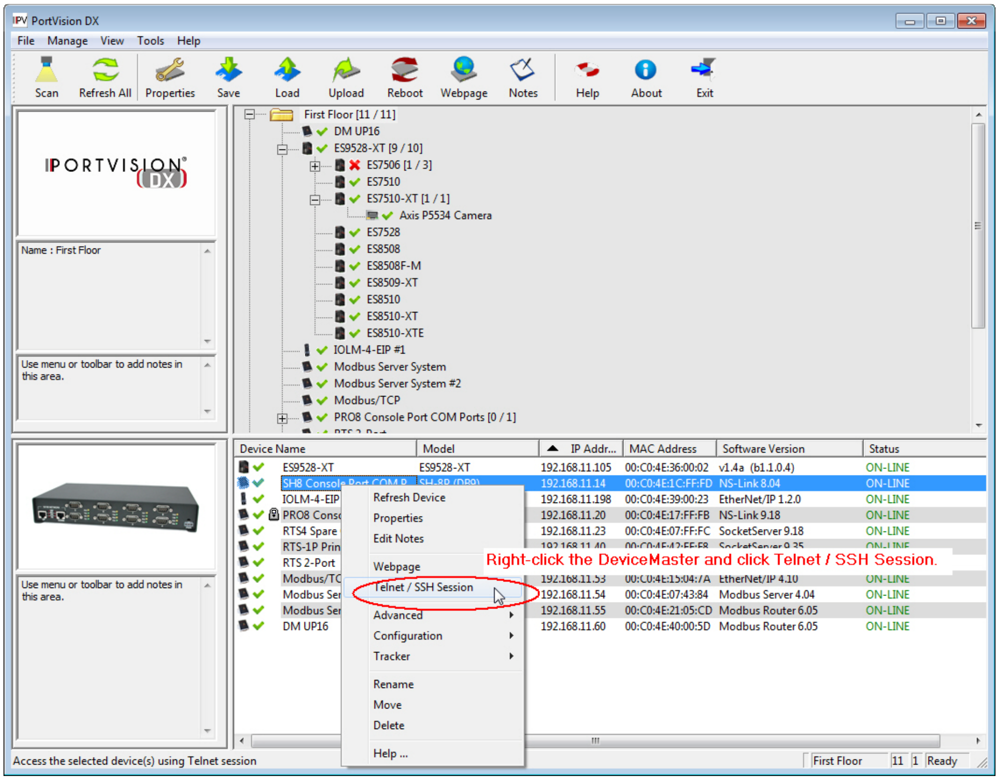
```
Password:

Comtrol DeviceMaster  ModelID: 5002675

SocketServer 11.02
Built: Mon Oct 24 11:27:08 CDT 2016
IP Addr: 10.0.0.40, Mask: 255.255.0.0, Gateway: 0.0.0.0
MAC Addr: 00:c0:4e:42:ff:f8


dm> help
auth         - Set the authentication method used by web server
help         - help [cmd] - Display help information
ip6          - Set IPv6 configuration
ip           - Set IP configuration
logdump      - Dump diagnostic log
mac          - Show MAC address
model        - View the Model ID
monitor      - Monitor seral port data
password     - Set the password
reset        - Resets the device
secureconf   - Enable/disable encryption for config
securedata   - Enable/disable encryption for data
securemon    - Enable/disable monitoring of secure data via telnet
sernum       - View the Serial Number
setbaud      - Set the baud on any or all ports
nshosts      - Show connected NSLink hosts
showtables   - show config tables
snmp         - Enable/disable SNMP
telnet       - Enable/disable telnet
teltimeout   - Set the telnet timeout period (seconds)
timeout      - Set time (seconds) until default application loads automatically
ver          - Display firmware revision
quit         - Exit session
```

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

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

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

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

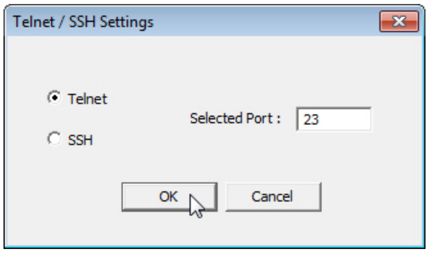


Device Name	Model	IP Addr...	MAC Address	Software Version	Status
ES9528-XT	ES9528-XT	192.168.11.105	00:C0:4E:36:00:02	v1.4a (b1.1.0.4)	ON-LINE
SH8 Console Port COM P	SH-8P (DB9)	192.168.11.14	00:C0:4E:1C:FF:FD	NS-Link 8.04	ON-LINE
IOLM-4-EIP		192.168.11.198	00:C0:4E:39:00:23	EtherNet/IP 1.2.0	ON-LINE
PRO8 Conso		192.168.11.20	00:C0:4E:17:FF:FB	NS-Link 9.18	ON-LINE
RTS4 Spare		192.168.11.23	00:C0:4E:07:FF:FC	SocketServer 9.18	ON-LINE
RTS-1P Prin		192.168.11.40	00:C0:4E:42:FF:F8	SocketServer 9.35	ON-LINE
RTS 2-Port					
Modbus/TC		192.168.11.53	00:C0:4E:15:04:7A	EtherNet/IP 4.10	ON-LINE
Modbus Ser		192.168.11.54	00:C0:4E:07:43:84	Modbus Server 4.04	ON-LINE
Modbus Ser		192.168.11.55	00:C0:4E:21:05:CD	Modbus Router 6.05	ON-LINE
DM UP16		192.168.11.60	00:C0:4E:40:00:5D	Modbus Router 6.05	ON-LINE

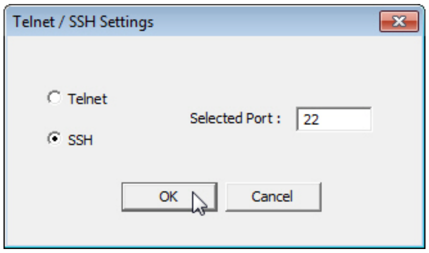
Right-click the DeviceMaster and click Telnet / SSH Session.

Access the selected device(s) using Telnet session

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

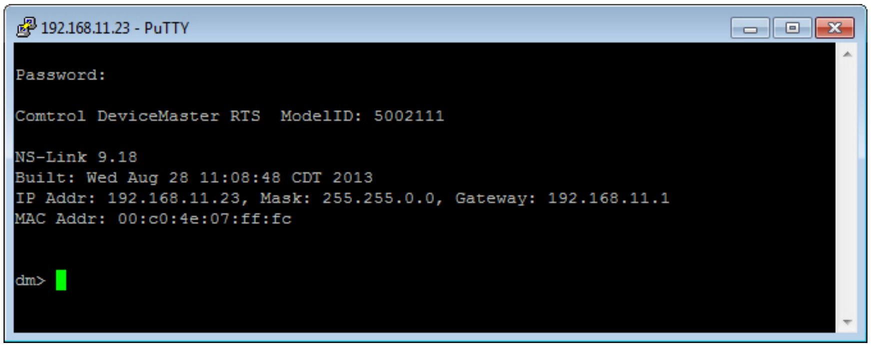


● Telnet
○ SSH
Selected Port : 23



○ Telnet
● SSH
Selected Port : 22

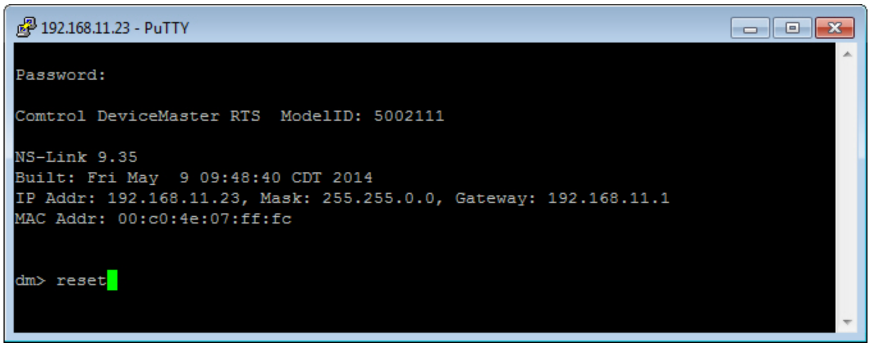
3. If necessary, enter the password and press **Enter**. If a password has not been set, press **Enter**. If using an SSH session, press **Enter** to the **login** as prompt.



```
Password:

Comtrol DeviceMaster RTS  ModelID: 5002111

NS-Link 9.18
Built: Wed Aug 28 11:08:48 CDT 2013
IP Addr: 192.168.11.23, Mask: 255.255.0.0, Gateway: 192.168.11.1
MAC Addr: 00:c0:4e:07:ff:fc


dm>
```

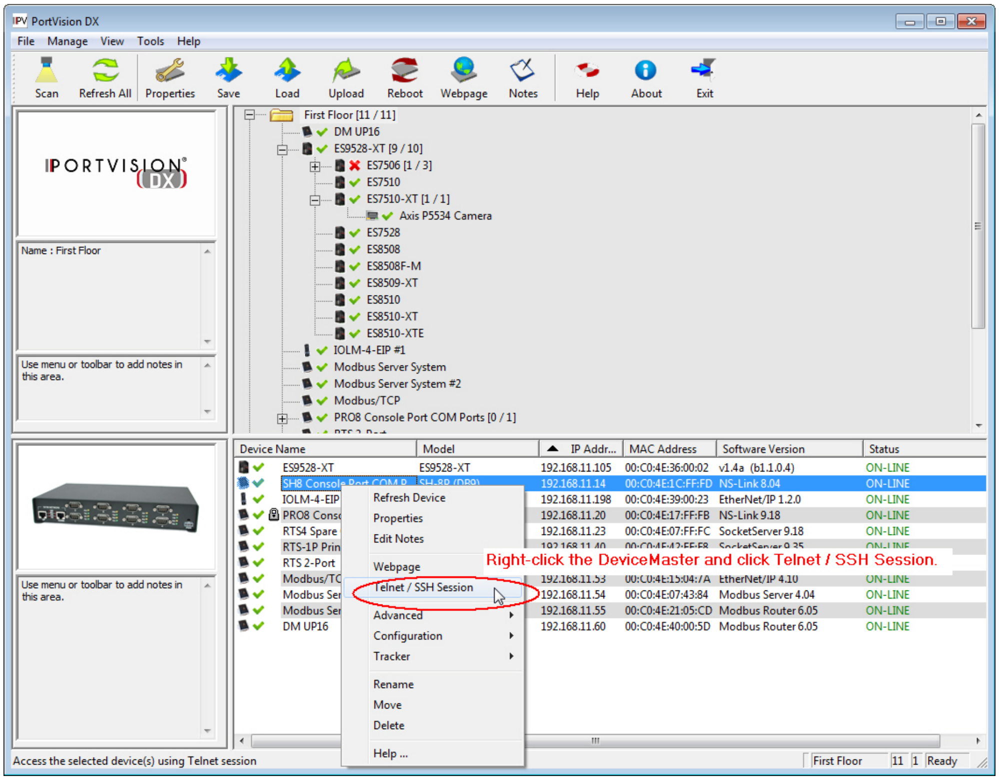
Note: *If the PuTTY screen flashes in the background and does not appear as shown above, make sure that* **Enable Telnet/ssh** *has not been disabled in SocketServer. To check this, return to PortVision DX, right-click the DeviceMaster LT in the Device List pane, and click* **Webpage**. *Click the* **Security**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

4. Type **Reset**, press **Enter**, and close the telnet session.



```
Password:

Comtrol DeviceMaster RTS  ModelID: 5002111

NS-Link 9.35
Built: Fri May  9 09:48:40 CDT 2014
IP Addr: 192.168.11.23, Mask: 255.255.0.0, Gateway: 192.168.11.1
MAC Addr: 00:c0:4e:07:ff:fc


dm> reset
```

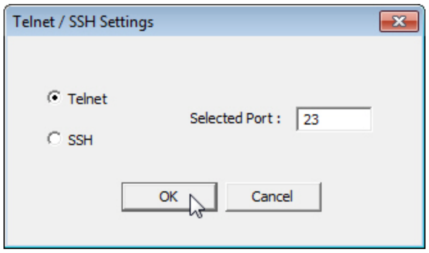
5. Quickly re-open the telnet or SSH session using the previous steps.



Device Name	Model	IP Addr...	MAC Address	Software Version	Status
ES9528-XT	ES9528-XT	192.168.11.105	00:C0:4E:36:00:02	v1.4a (b1.1.0.4)	ON-LINE
SH8 Console Port COM P...	SH-8P (DB9)	192.168.11.14	00:C0:4E:1C:FF:FD	NS-Link 8.04	ON-LINE
IOLM-4-EIP		192.168.11.198	00:C0:4E:39:00:23	EtherNet/IP 1.2.0	ON-LINE
PRO8 Conso...		192.168.11.20	00:C0:4E:17:FF:FB	NS-Link 9.18	ON-LINE
RTS4 Spare		192.168.11.23	00:C0:4E:07:FF:FC	SocketServer 9.18	ON-LINE
RTS-1P Prin...		192.168.11.40	00:C0:4E:42:FF:F8	SocketServer 9.35	ON-LINE
RTS 2-Port					
Modbus/TC...		192.168.11.53	00:C0:4E:15:04:7A	EtherNet/IP 4.10	ON-LINE
Modbus Ser...		192.168.11.54	00:C0:4E:07:43:84	Modbus Server 4.04	ON-LINE
Modbus Ser...		192.168.11.55	00:C0:4E:21:05:CD	Modbus Router 6.05	ON-LINE
DM UP16		192.168.11.60	00:C0:4E:40:00:5D	Modbus Router 6.05	ON-LINE

Right-click the DeviceMaster and click Telnet / SSH Session.

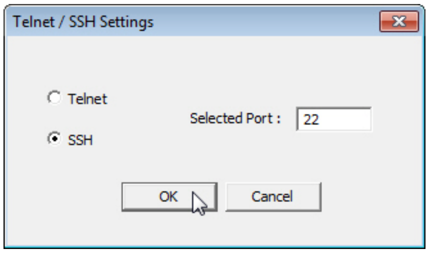
6. Select **Telnet** or **SSH**, leave the **Selected Port** number, and click **Ok**.


Telnet / SSH Settings

● Telnet

○ SSH

Selected Port : 23

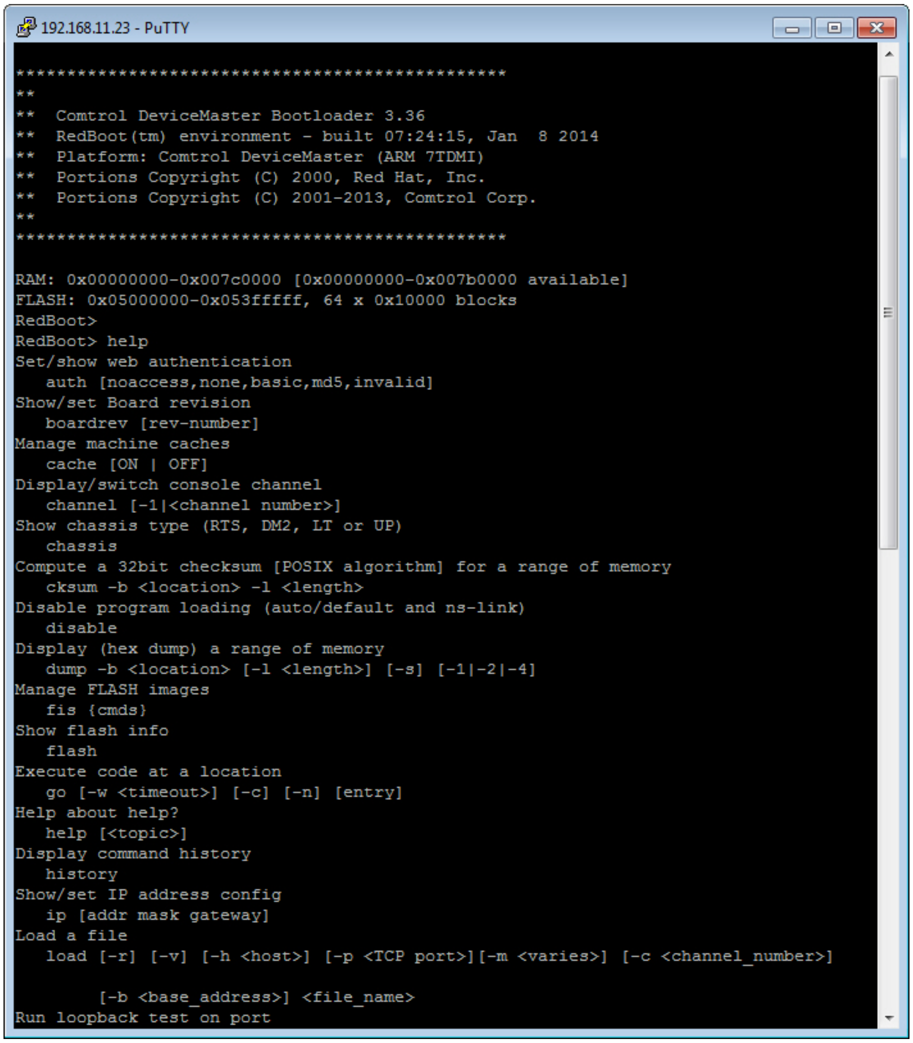

Telnet / SSH Settings

○ Telnet

● SSH

Selected Port : 22

7. Press **Enter**. You can type **help** to review the RedBoot commands. You can also refer to *RedBoot Command Overview* on Page 111.



```
************************************************
**
**  Comtrol DeviceMaster Bootloader 3.36
**  RedBoot(tm) environment - built 07:24:15, Jan  8 2014
**  Platform: Comtrol DeviceMaster (ARM 7TDMI)
**  Portions Copyright (C) 2000, Red Hat, Inc.
**  Portions Copyright (C) 2001-2013, Comtrol Corp.
**
************************************************

RAM: 0x00000000-0x007c0000 [0x00000000-0x007b0000 available]
FLASH: 0x05000000-0x053fffff, 64 x 0x10000 blocks
RedBoot>
RedBoot> help
Set/show web authentication
   auth [noaccess,none,basic,md5,invalid]
Show/set Board revision
   boardrev [rev-number]
Manage machine caches
   cache [ON | OFF]
Display/switch console channel
   channel [-1|<channel number>]
Show chassis type (RTS, DM2, LT or UP)
   chassis
Compute a 32bit checksum [POSIX algorithm] for a range of memory
   cksum -b <location> -l <length>
Disable program loading (auto/default and ns-link)
   disable
Display (hex dump) a range of memory
   dump -b <location> [-l <length>] [-s] [-1|-2|-4]
Manage FLASH images
   fis {cmds}
Show flash info
   flash
Execute code at a location
   go [-w <timeout>] [-c] [-n] [entry]
Help about help?
   help [<topic>]
Display command history
   history
Show/set IP address config
   ip [addr mask gateway]
Load a file
   load [-r] [-v] [-h <host>] [-p <TCP port>][-m <varies>] [-c <channel_number>]

        [-b <base_address>] <file_name>
Run loopback test on port
```

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

RedBoot Procedures

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

Optionally, you can install PortVision DX on a Windows system on the network and perform all of these tasks. PortVision DX provides a Telnet/SSH session, which is discussed in *Accessing RedBoot Commands in Telnet/SSH Sessions (PortVision DX)* on Page 100.

Accessing RedBoot Overview

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

- A *serial* connection between Port 1 on the DeviceMaster LT and a COM port on a PC (Page 106). If you plan on using the serial method, you will need a null modem cable, a terminal program installed and configured on the PC, and a **Bootloader Timeout** value in excess of 15 seconds. If the **Bootloader Timeout** value has been reduced to 1 second, this procedure will NOT be possible.

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

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

- A *telnet* connection (Page 107), if the DeviceMaster LT 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 LT default IP address if you have not changed the IP address to operate on your network.

Establishing a Serial Connection

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

1. Connect a null-modem cable from an available COM port on your PC to **Port 1** on the DeviceMaster LT.

   Note: *See Connecting Serial Devices on Page 73, 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 LT.

   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 105 or use the *RedBoot Command Overview* on Page 111 to perform the desired task.

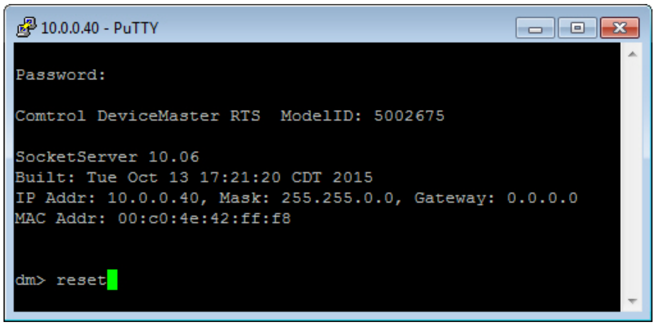
Establishing a Telnet Connection

Use the following procedure to telnet to the DeviceMaster LT.

1. Open a telnet session, enter the DeviceMaster LT IP address.

   If using Windows, you can use PortVision DX, see [Accessing RedBoot Commands in Telnet/SSH Sessions (PortVision DX)]() on Page 100.

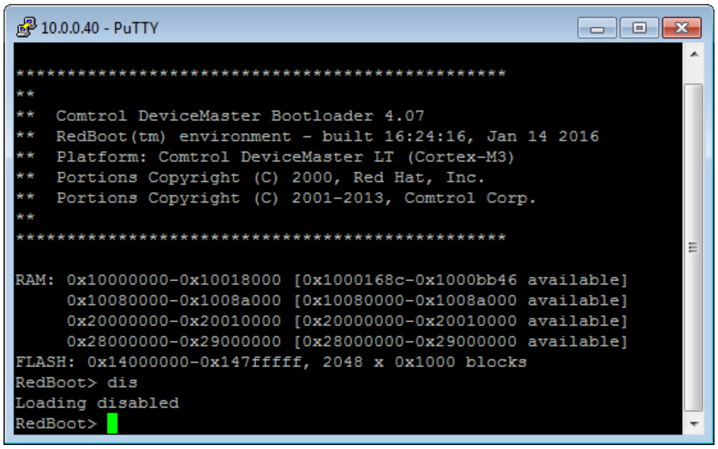
2. Press the **Enter** key if you did not program a password or type the password and press **Enter**.



```
Password:

Comtrol DeviceMaster RTS  ModelID: 5002675

SocketServer 10.06
Built: Tue Oct 13 17:21:20 CDT 2015
IP Addr: 10.0.0.40, Mask: 255.255.0.0, Gateway: 0.0.0.0
MAC Addr: 00:c0:4e:42:ff:f8


dm> reset
```

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

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



```
************************************************
**
**  Comtrol DeviceMaster Bootloader 4.07
**  RedBoot(tm) environment - built 16:24:16, Jan 14 2016
**  Platform: Comtrol DeviceMaster LT (Cortex-M3)
**  Portions Copyright (C) 2000, Red Hat, Inc.
**  Portions Copyright (C) 2001-2013, Comtrol Corp.
**
************************************************

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

Determining the Network Settings

Default Network Settings

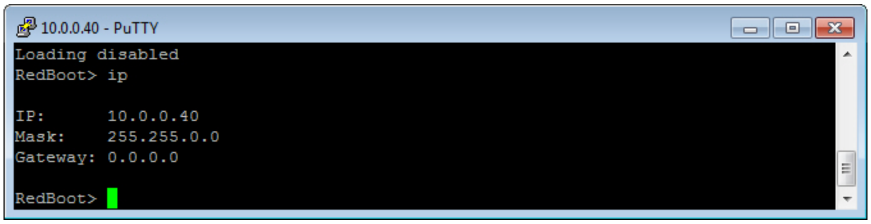
IP address:
192.168.250.250

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 LT, you can perform the following procedure.

1. Establish communications with the DeviceMaster LT using the serial (Page 106) or telnet (Page 107) method.
2. At the **RedBoot** prompt, type **ip**.



```
Loading disabled
RedBoot> ip

IP:      10.0.0.40
Mask:    255.255.0.0
Gateway: 0.0.0.0

RedBoot> 
```

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

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

Configuring the Network Settings

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

1. Establish communications with the DeviceMaster LT using the serial (Page 106) or telnet (Page 107) method.
2. Enter **ip [*addr mask gateway*]** and press the **Enter** key to configure the IP address. *Where*:

   addr = IP address you want to use

   mask = matches you network subnet mask

   gateway = assigned by your network administrator

   Make sure that each value is separated by a space.

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

3. Verify that RedBoot responds with your configured network information or reissue the command.
4. Type **reset** to reset the DeviceMaster LT, 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 LT using the serial (Page 106) or telnet (Page 107) method.
2. At the **RedBoot** prompt, type **timeout.**

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

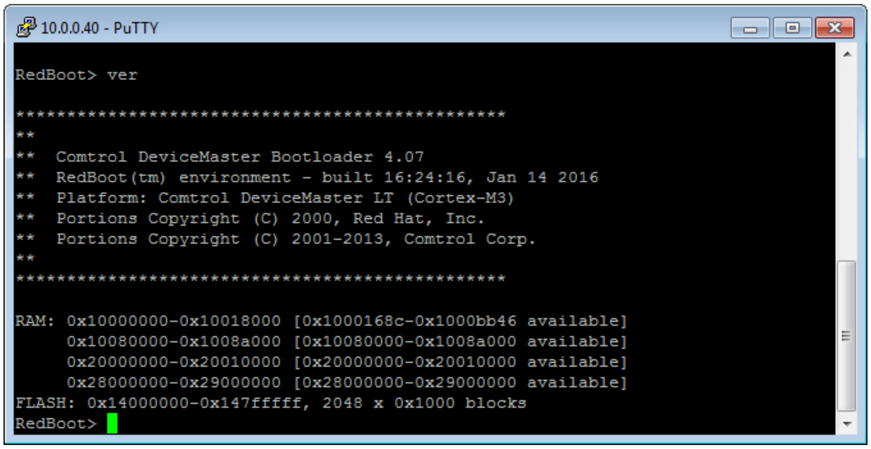
   RedBoot responds with the current Bootloader timeout value.

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 LT.

1. Establish communications with the DeviceMaster LT using the serial (Page 106) or telnet (Page 107) method.
2. At the **RedBoot** prompt, type **version**.



```
RedBoot> ver

************************************************
**
**   Comtrol DeviceMaster Bootloader 4.07
**   RedBoot(tm) environment - built 16:24:16, Jan 14 2016
**   Platform: Comtrol DeviceMaster LT (Cortex-M3)
**   Portions Copyright (C) 2000, Red Hat, Inc.
**   Portions Copyright (C) 2001-2013, Comtrol Corp.
**
************************************************

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

   The Bootloader information displays.

3. Type **reset** to reset the DeviceMaster LT, if you do not have any other related RedBoot tasks.

Note: *Optionally, you can install PortVision DX on a Windows system on the network and see the Bootloader version in the Device List pane. Reboot the DeviceMaster LT, right-click the DeviceMaster LT and click Refresh Device until the Bootloader version displays. The Bootloader version is only displayed for a few moments.*

Resetting the DeviceMaster LT

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

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

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

Configuring Passwords

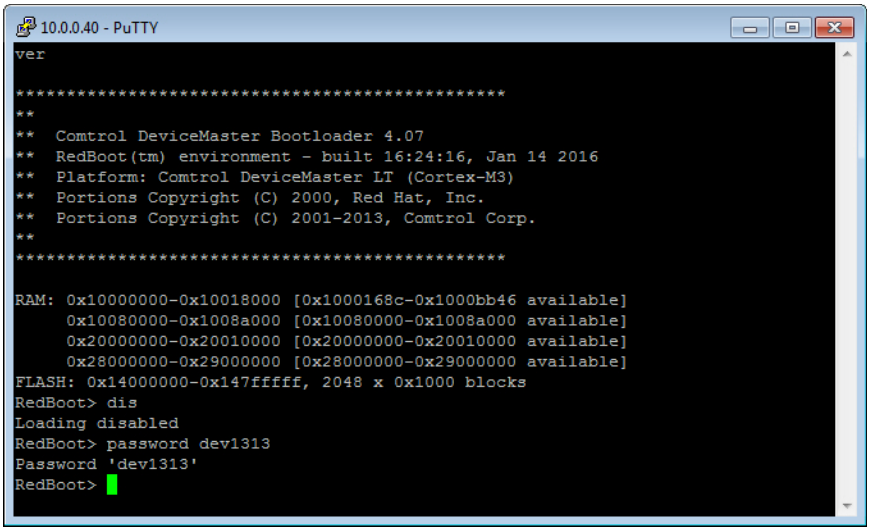
This section discusses how to configure a password for the web and telnet server.

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

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

1. Establish communications with the DeviceMaster LT using the serial (Page 106) or telnet method (Page 107).
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.*



```
ver

**************************************************
**
**  Comtrol DeviceMaster Bootloader 4.07
**  RedBoot(tm) environment - built 16:24:16, Jan 14 2016
**  Platform: Comtrol DeviceMaster LT (Cortex-M3)
**  Portions Copyright (C) 2000, Red Hat, Inc.
**  Portions Copyright (C) 2001-2013, Comtrol Corp.
**
**************************************************

RAM: 0x10000000-0x10018000 [0x1000168c-0x1000bb46 available]
     0x10080000-0x1008a000 [0x10080000-0x1008a000 available]
     0x20000000-0x20010000 [0x20000000-0x20010000 available]
     0x28000000-0x29000000 [0x28000000-0x29000000 available]
FLASH: 0x14000000-0x147fffff, 2048 x 0x1000 blocks
RedBoot> dis
Loading disabled
RedBoot> password dev1313
Password 'dev1313'
RedBoot>
```

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

See the **auth** command in the RedBoot Command Overview on Page 111, if you want to set up Web browser authentication.

RedBoot Command Overview

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

For more detailed information, see the *eCos Reference Manual* that you can download from: ftp://ftp.comtrol.com/dev_mstr/LT/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.)
baudrate [-b <rate>]	Set/Query the system console baud rate.
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.
cpufreq	Show/Set CPU clock frequency.
delaycal <passes>	Calibrate SDRAM clock delay.
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.
eepromvers [ver]	Show/set EEPROM version.
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.
history	Displays command history.
hwflags [flags]	Show/set hardware feature flags.
ip [addr mask gateway]	Displays or sets the IP address configuration.
load [-r] [-v] [-h <host>] **[-p <TCP port>]** **[-m <varies>]** **[-c <channel_number>]** **[-b <base_address>]** **<file_name>**	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.

RedBoot Commands (Continued)	
mac†	Displays Ethernet MAC address.
mcmp -s <location> **-s <location>** **-d <location> -l <length>** **[-1|-2|-4]**	Compares two blocks of memory.
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.
numether [num]†	Shows number of Ethernet ports.
numserial [num]†	Shows number of serial ports.
oemid [id]†	Shows OEM id.
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.
ramtest <passes>	Test the RAM.
ramtime [reg [<value>]]	Shows RAM timing register values.
reset	Resets the DeviceMaster LT.
secureconf [disable|enable]	Sets or displays secure config enable.
securedata [disable|enable]	Sets or displays secure data enable.
sernum [prefix] [serial_number] **sernum [serial_number]†**	Displays device serial number (if available).
?	Displays short help.
snmp [disable|enable]	Sets or displays SNMP enable.
summary	Displays a summary that includes the bootloader version, network address information, MAC address, and security settings.
telnet [disable | enable}	Sets or displays telnet server enable. Disables telnet.
teltimeout [seconds]	Shows or sets telnet time-out.
terse	Terse command response mode.
timeout {seconds}	Displays or sets Bootloader time-out value.
version	Displays RedBoot version information.
x -b <location> [-l <length>] [-s] [-1|2|4]	Displays (hex dump) a range of memory.
kszdump	Dumps a pre-determined set of KSZ8863 registers
kszrd <r1> [r2]	Reads specified KSZ8863 registers.
kszrestart	Restarts KSZ8863.
kszwr <r1> <val>	Reads specified KSZ8863 registers.
† Read-only items that you cannot change in Redboot.	

Hardware Specifications

Locating DeviceMaster LT Specifications

Specifications can be found on the Comtrol web site (www.comtrol.com) .

External Power Supply Specifications

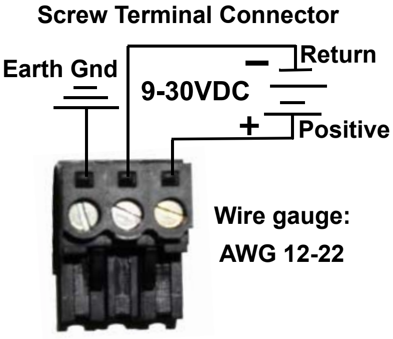
This subsection discusses information that you may need if you wish to use your own external power supplies.

This table provides specifications for the power supply shipped with the DeviceMaster LT.

Comtrol Power Supply: 24 VDC	
Input line frequency Input line voltage Output voltage Output current	43-63 Hz 90-264 VAC 24 VDC 500 mA @ 24VDC

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

External Power Supply: 9-30VDC	
Output voltage† Current† Power	9 - 30 VDC 400 mA (Min) @ 24VDC 3.6 W
† *Any power supply that meets current consumption, voltage, power, and connector pinouts requirements can be used.*	



Troubleshooting and Technical Support

This section contains troubleshooting information for your DeviceMaster LT. 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 115
- *General Troubleshooting* on Page 117
- *Testing Ports Using Port Monitor (PMon2)* on Page 119
- *Testing Ports Using Test Terminal* on Page 122
- *Socket Mode Serial Port Testing* on Page 128
- *DeviceMaster LT LEDs* on Page 134
- *Removing DeviceMaster LT Security Features* on Page 135
- *Returning the DeviceMaster LT to Factory Defaults* on Page 137

If you cannot diagnose the problem, you can contact *Technical Support* on Page 140.

Troubleshooting Checklist

The following checklist may help you diagnose your problem:

- Verify that you are using the correct types of cables on the correct connectors and that all cables are connected securely.

  Note: *Most customer problems reported to Comtrol Technical Support are eventually traced to cabling or network problems.*

Model	Connected to	Ethernet Cable	Connector Name
16-Port - 2E (Dual Ethernet Ports)	Ethernet hub or NIC	Standard	10/100

- 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 LT 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 LT.
  - 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 LT are powered up and operating.
- Verify that the hardware MAC address in the NS-Link device driver matches the address on the DeviceMaster LT.
- If using a driver for Windows, verify that you are addressing the port correctly. In many applications, device names above COM9 require the prefix **\\.** in order to be recognized. For example, to reference COM20, use **\\.\COM20** as the file or port name.
- If using a driver for Windows, you can use one of the Comtrol tools.

  - *Advanced* tab in the *Comtrol Drivers Management Console* which helps identify problems.
  - PortVision DX contains two applications that can be used to test or monitor the DeviceMaster LT:
    - *Test Terminal* program, which can be used to troubleshoot communications on a port-by-port basis. See *Testing Ports Using Test Terminal* on Page 122 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 119 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 LT and watch the **Status** (Page 134) light activity.

Status LED	Description
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.

- Remove and reinstall the DeviceMaster LT NS-Link device driver.
- If you have a spare DeviceMaster LT, 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 115.*

General Condition	Explanation/Action
Status LED flashing	Indicates that the bootloader has not downloaded to the DeviceMaster LT. 1. If applicable, remove the NS-Link driver. 2. Make sure that you have downloaded the most current driver: ftp://ftp.comtrol.com/dev_mstr/LT/drivers/. 3. Install the latest driver and configure the DeviceMaster LT using the MAC address. Make sure that you reboot the system. See *Device Driver (NS-Link) Installation* on Page 31 for procedures. ***Note:*** *If the* **Status** *LED is still flashing, contact Technical Support.*
Status LED not lit	Indicates that power has not been applied or there is a hardware failure. Contact Technical Support.
Can ping the Comtrol device, but cannot open the ports from a remote location. (You must have previously programmed the IP address, subnet mask, and IP gateway.)	The NS-Link driver uses Port 4606 (**11FE** h) to communicate with the DeviceMaster LT. When using a *sniffer* to track NS-Link packets, filtering for Port 4606 will easily track the packet. The packet should also contain the MAC address of the device and the originating PC so that it can be determined if the packet is able to travel the full distance one way or not. If the 4606 packet is found on one side of a firewall or router, using sniffer, and not on the other side, then that port needs to be opened up to allow the 4606 to pass. This will most often be seen with firewalls, but is also seen in some routers.
Cannot ping the device through Ethernet hub	Isolate the DeviceMaster LT from the network. Connect the device directly to the NIC in the host system.
Cannot ping or connect to the DeviceMaster LT	The default DeviceMaster LT IP address is often not accessible due to the subnet masking from another network unless **192.168** is used in the network. In most cases, it will be necessary to program in an address that conforms to your network. See *Configuring the Network Settings* on Page 19 to use PortVision DX to program the IP address. If you do not use PortVision DX (or the NS-Link driver for Windows) to program the IP address, you can use RedBoot. If you use RedBoot, you only have 15 seconds to disable the Bootloader with RedBoot to get into the setup utility. See *RedBoot Procedures* on Page 105 for the RedBoot method of programming an IP address.

General Condition	Explanation/Action
DeviceMaster LT continuously reboots when connected to some Ethernet switches with the NS-Link driver	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. *Resolution*: There will be no firmware fix for this problem. Only ***one*** of the following fixes is required for resolution. 1. Disable STA in the switch. 2. Enable STA fast forwarding on the port. 3. Change the STA Forward Delay and Message Age to minimum time values. 4. On the device, set the time-out value to 0 (to disable loading of SocketServer) or 120. The command from the redboot prompt is “Timeout 120” without the quotes. *Problem Details*: 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. The normal NS-Link driver load process is: 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 LT. 2. After a 6 second delay, NS-Link sends an ID query to the device. This query is to verify that the device is in RedBoot and can accept **load binary** commands. 3. The device sends an ID query response. 4. NS-Link loads the device. If the device is not loaded after **timeout** seconds (default 15), it loads SocketServer. The above process fails when STA is running because the switch blocks packets for 30 seconds after the DeviceMaster LT reboots. Therefore, the ID query is not received by the DeviceMaster LT and after 15 seconds the device loads SocketServer. After 30 seconds, NS-Link finally can do an ID query, which reveals that the device is not in RedBoot. NS-Link therefore reboots the device, and the process repeats.
DeviceMaster LT continuously reboots when connected to some Ethernet switches or routers	Invalid IP information may also cause the switch or router to check for a gateway address. Lack of a gateway address is a common cause.

Testing Ports Using Port Monitor (PMon2)

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

Overview

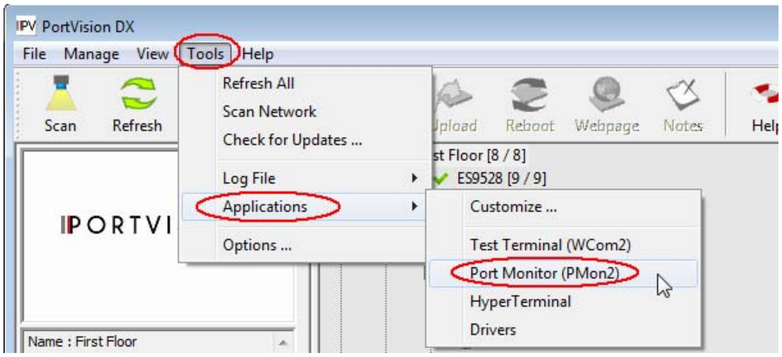
This procedure will check whether the DeviceMaster LT can:

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

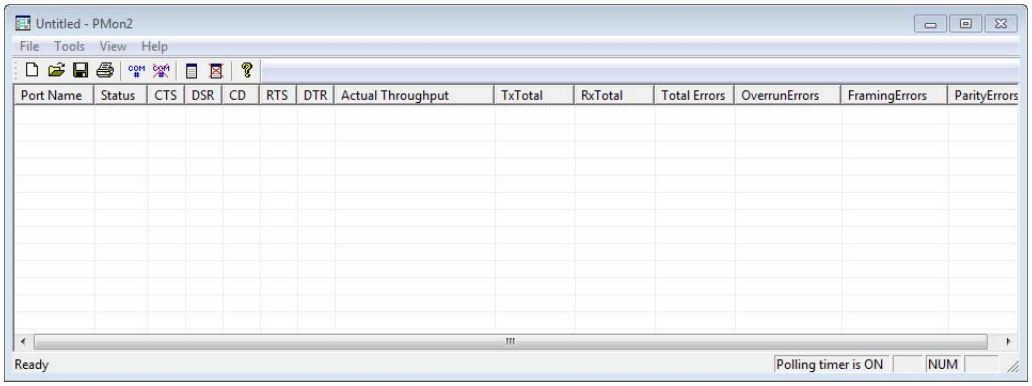
Testing Comtrol COM Ports

If necessary, *Installing PortVision DX* on Page 15 to install PortVision DX, which contains Port Monitor.

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

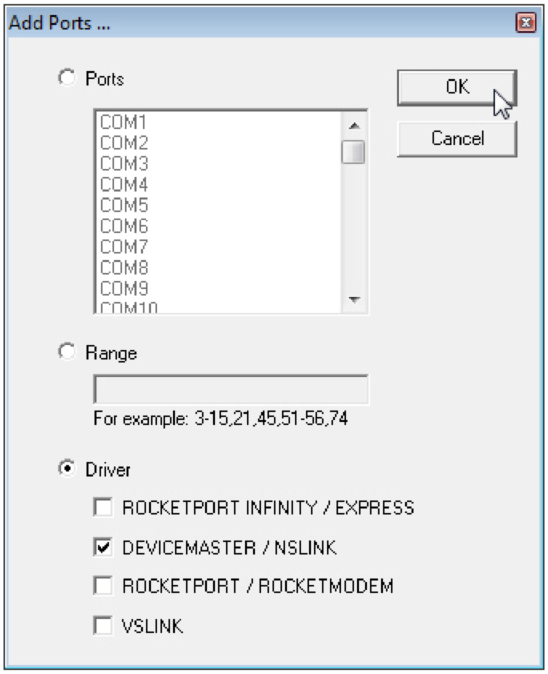


3. Click **Add Ports** using the icon or **Tools > Add Ports**,



Port Name	Status	CTS	DSR	CD	RTS	DTR	Actual Throughput	TxTotal	RxTotal	Total Errors	OverrunErrors	FramingErrors	ParityErrors

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



Add Ports ...

○ Ports

COM1
COM2
COM3
COM4
COM5
COM6
COM7
COM8
COM9
COM10

○ Range

For example: 3-15,21,45,51-56,74

● Driver

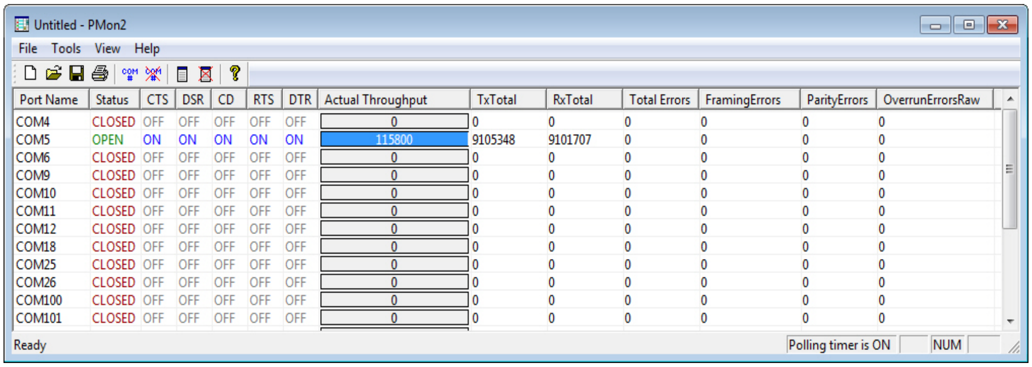
□ ROCKETPORT INFINITY / EXPRESS

☑ DEVICEMASTER / NSLINK

□ ROCKETPORT / ROCKETMODEM

□ VSLINK

5. If the DeviceMaster LT 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.



Untitled - PMon2

Port Name	Status	CTS	DSR	CD	RTS	DTR	Actual Throughput	TxTotal	RxTotal	Total Errors	FramingErrors	ParityErrors	OverrunErrorsRaw
COM4	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM5	OPEN	ON	ON	ON	ON	ON	115800	9105348	9101707	0	0	0	0
COM6	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM9	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM10	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM11	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM12	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM18	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM25	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM26	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM100	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM101	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0

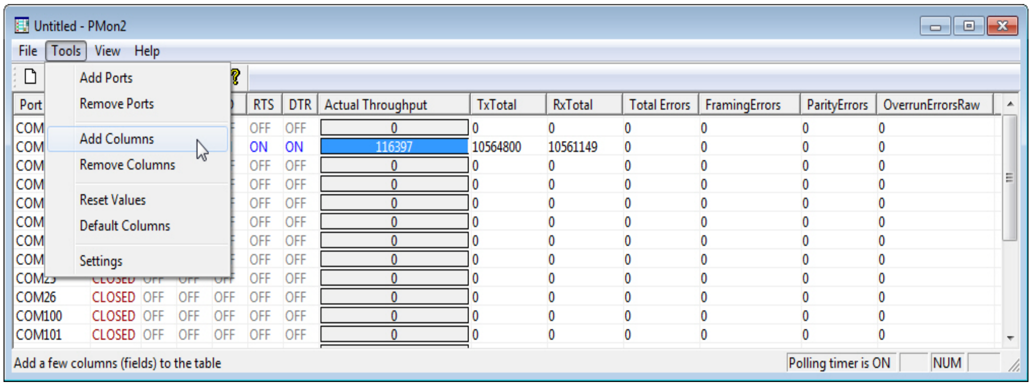
Ready | Polling timer is ON | NUM

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

If the errors are:

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

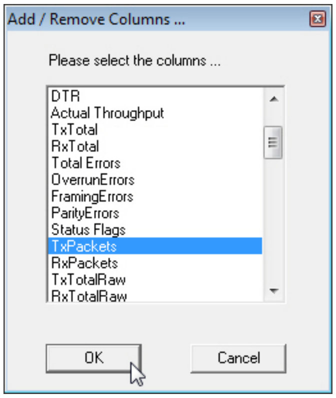


Port					RTS	DTR	Actual Throughput	TxTotal	RxTotal	Total Errors	FramingErrors	ParityErrors	OverrunErrorsRaw
COM					OFF	OFF	0	0	0	0	0	0	0
COM					ON	ON	116397	10564800	10561149	0	0	0	0
COM					OFF	OFF	0	0	0	0	0	0	0
COM					OFF	OFF	0	0	0	0	0	0	0
COM					OFF	OFF	0	0	0	0	0	0	0
COM					OFF	OFF	0	0	0	0	0	0	0
COM					OFF	OFF	0	0	0	0	0	0	0
COM					OFF	OFF	0	0	0	0	0	0	0
COM25	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM26	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM100	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM101	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0

Add a few columns (fields) to the table

Polling timer is ON NUM

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

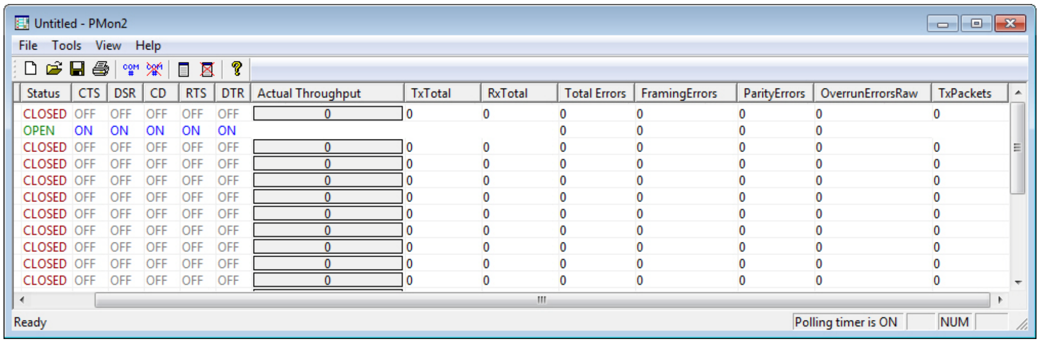


Please select the columns ...

DTR
Actual Throughput
TxTotal
RxTotal
Total Errors
OverrunErrors
FramingErrors
ParityErrors
Status Flags
TxPackets
RxPackets
TxTotalRaw
RxTotalRaw

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.



Status	CTS	DSR	CD	RTS	DTR	Actual Throughput	TxTotal	RxTotal	Total Errors	FramingErrors	ParityErrors	OverrunErrorsRaw	TxPackets
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0
OPEN	ON	ON	ON	ON	ON				0	0	0	0	
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0
CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0	0

Ready

Polling timer is ON NUM

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 LT device driver, 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 73.

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

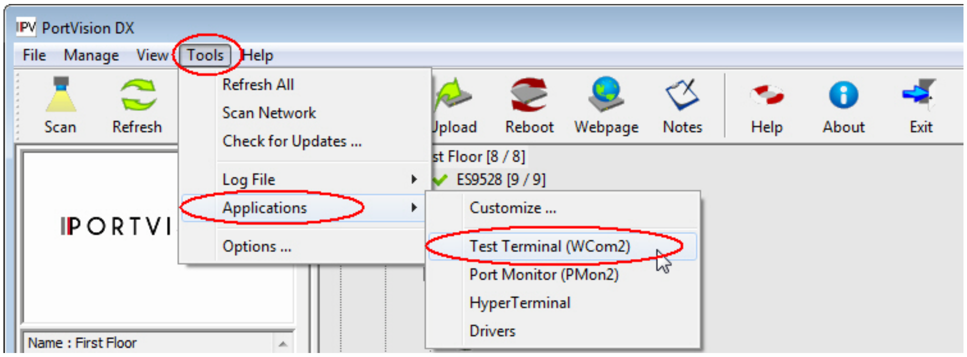
The following procedure shows how to use **Test Terminal** to send and receive test data to the serial ports. If necessary, use *Installing PortVision DX* on Page 15, which contains Test Terminal.

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

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

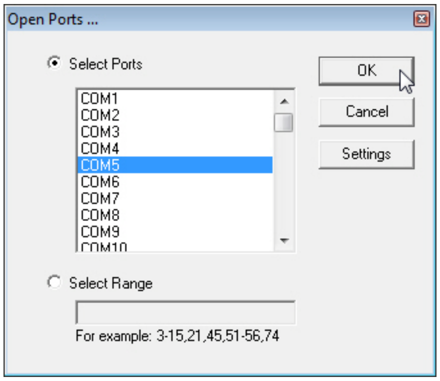
2. Start Test Terminal (WCom2). If necessary, start PortVision DX from the **Start** menu, select **Programs > Comtrol > PortVision DX > PortVision DX** or click the desktop shortcut.

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



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

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



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

- *Sending and Receiving Test Data (RS-232/422/485: 4-Wire)* (below)
- *Sending and Receiving Data (RS-485: 2-Wire)* on Page 125

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

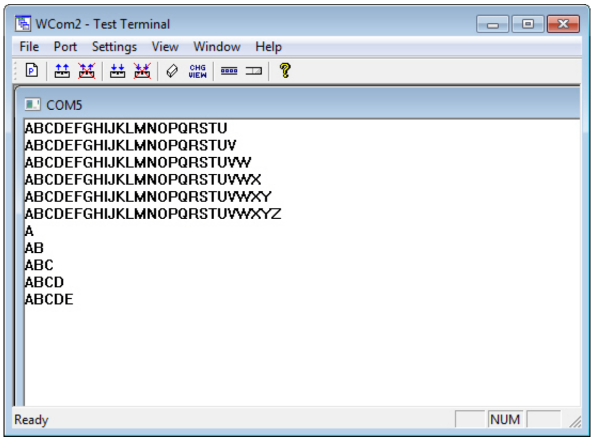
You can use this procedure to send and receive test data through the RS-232/422/485 (4-wire, full-duplex) port or ports that you want to test.

1. If you have not done so, perform Steps 1 through 2 on Page 123.
2. Install the loopback plug onto the port (or ports) that you want to test.

   See *Connecting Serial Devices* on Page 73, if you need to build loopback plugs.
3. Select **Port** > **Send and Receive Test Data**.

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

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



```
ABCDEFGHIJKLMNOPQRSTU
ABCDEFGHIJKLMNOPQRSTUV
ABCDEFGHIJKLMNOPQRSTUVW
ABCDEFGHIJKLMNOPQRSTUVWX
ABCDEFGHIJKLMNOPQRSTUVWXY
ABCDEFGHIJKLMNOPQRSTUVWXYZ
A
AB
ABC
ABCD
ABCDE
```

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 124 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 123, Steps 1 through 2).
2. Click **Port > Loopback Test**.

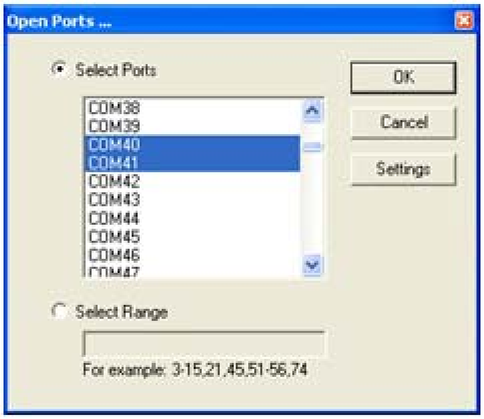
   This is a pass fail test and will take a second or two to complete. Repeat for each port that needs testing.

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

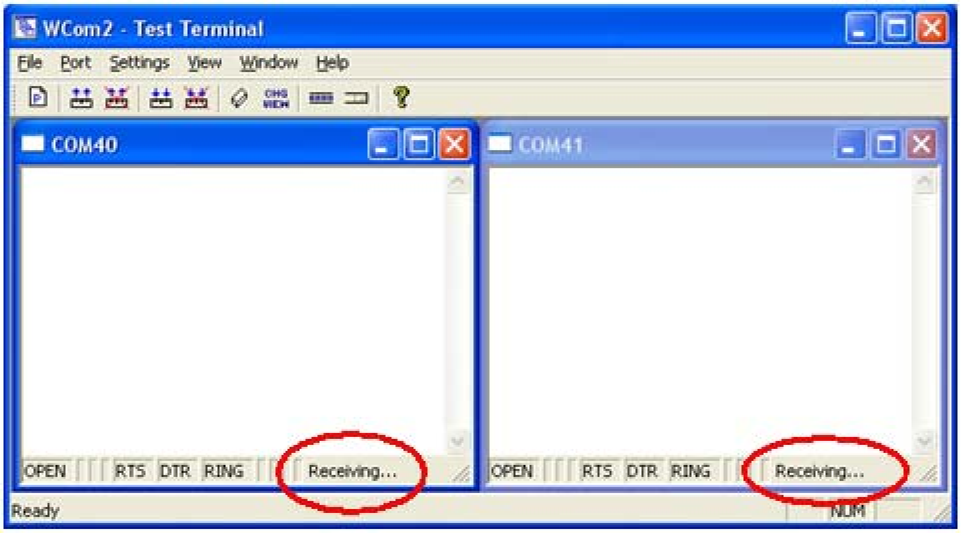
Sending and Receiving Data (RS-485: 2-Wire)

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

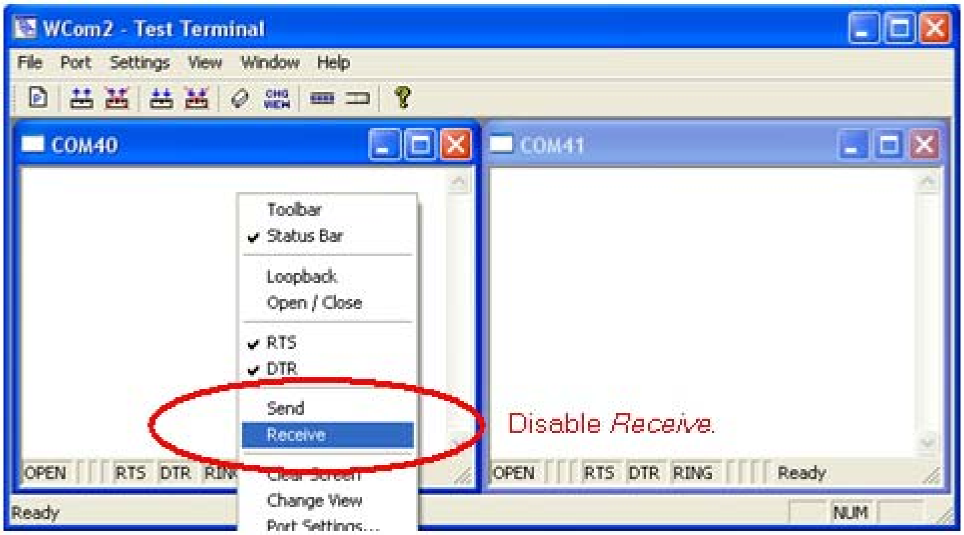
1. In PortVision DX, click **Tools >Applications >Test Terminal (WCom2)** to start Test Terminal.
2. Open two ports RS-485 ports. This example uses COM40 and COM41.



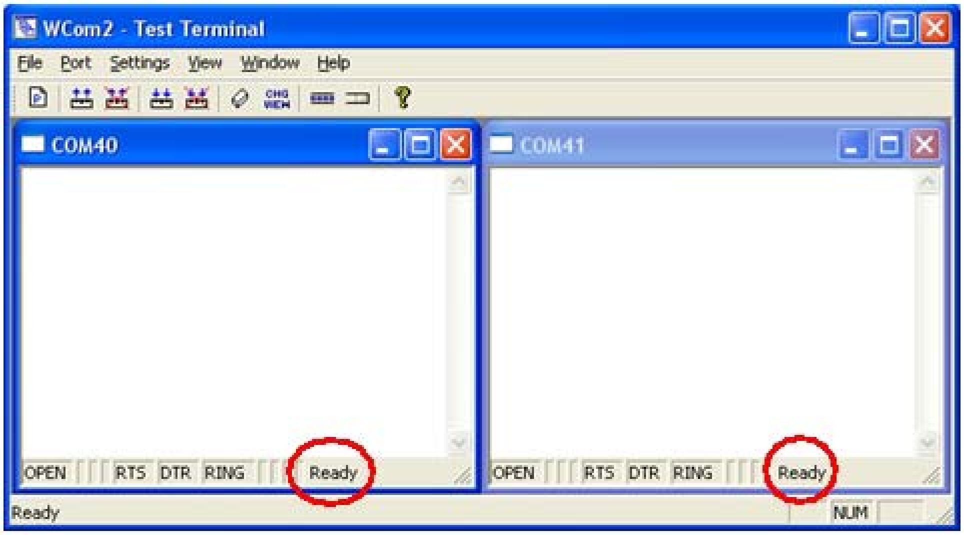
Test Terminal will open two windows, note that both ports show *Receiving* on the status bar.



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

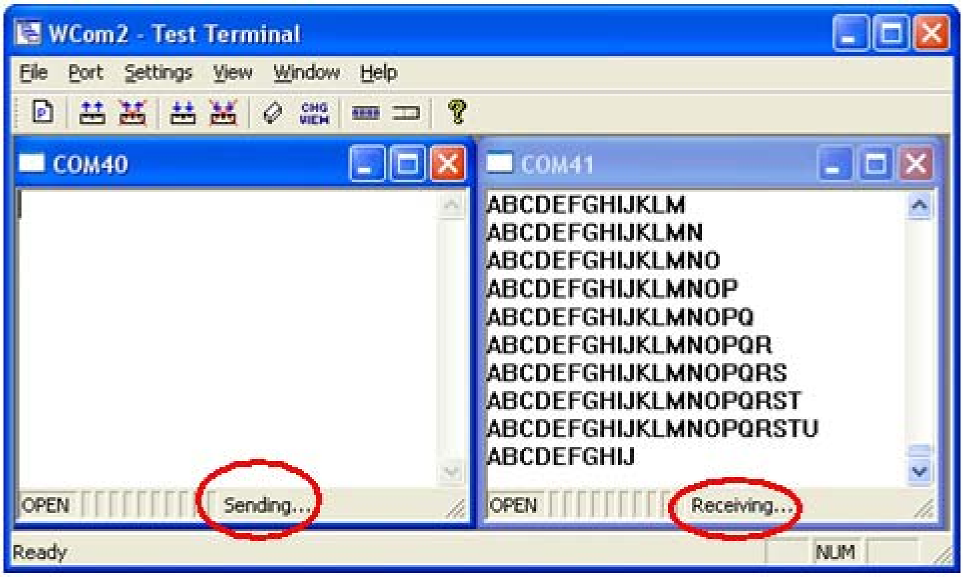


Both COM ports show *Ready* on the status bar.



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

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

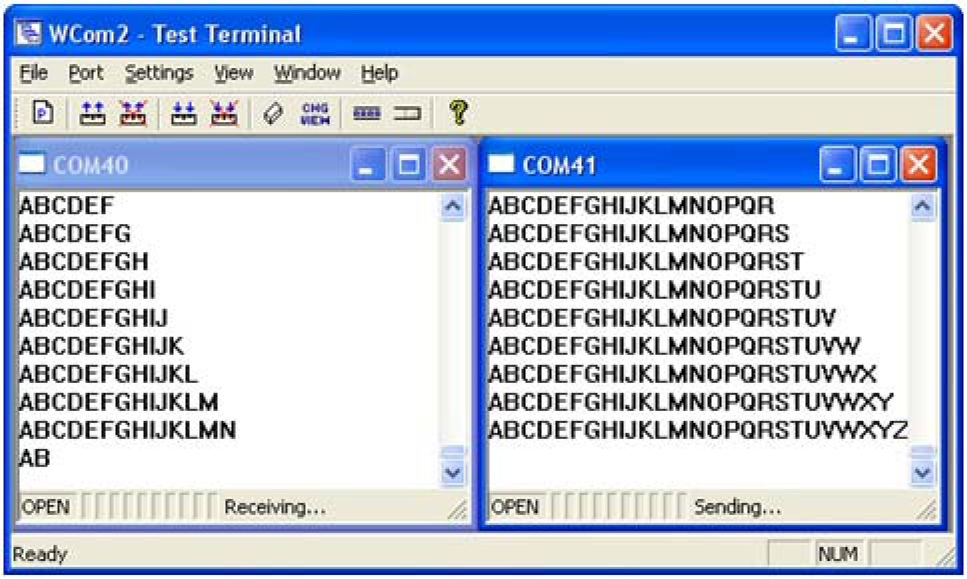


```
ABCDEFGHIJKLM
ABCDEFGHIJKLMN
ABCDEFGHIJKLMNO
ABCDEFGHIJKLMNOP
ABCDEFGHIJKLMNOPQ
ABCDEFGHIJKLMNOPQR
ABCDEFGHIJKLMNOPQRS
ABCDEFGHIJKLMNOPQRST
ABCDEFGHIJKLMNOPQRSTU
ABCDEFGHIJ
```

The *Status* line shows *Sending* or *Receiving*. In this case, COM40 is sending data and COM41 is receiving the data which is visually confirmed by the data scrolling across the COM41 window.

Note: *If you do not see the data being received it MAY be necessary to also disable the RTS and DTR options from the right-click pop-up menu in each COM port.*

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



```
ABCDEF
ABCDEFG
ABCDEFGH
ABCDEFGHI
ABCDEFGHIJ
ABCDEFGHIJK
ABCDEFGHIJKL
ABCDEFGHIJKLM
ABCDEFGHIJKLMN
AB
```

```
ABCDEFGHIJKLMNOPQR
ABCDEFGHIJKLMNOPQRS
ABCDEFGHIJKLMNOPQRST
ABCDEFGHIJKLMNOPQRSTU
ABCDEFGHIJKLMNOPQRSTUV
ABCDEFGHIJKLMNOPQRSTUVW
ABCDEFGHIJKLMNOPQRSTUVWX
ABCDEFGHIJKLMNOPQRSTUVWXY
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Neither COM port is sending or receiving data but shows *Ready* on the *Status* bar.

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

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

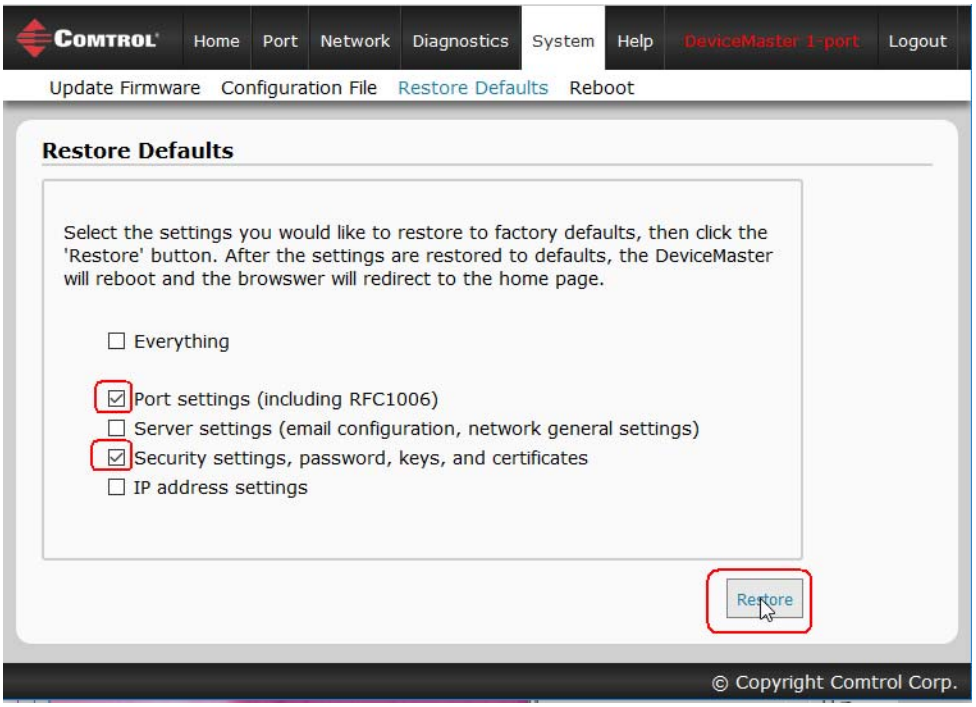
Data is now scrolling in the COM40 window. COM41 is static as it is not receiving data but transmitting data.

Socket Mode Serial Port Testing

This procedure illustrates using Putty, which is available in PortVision DX. Optionally, you can use any other Winsock compatible application.

Note: *The following procedure starts with resetting DeviceMaster LT to factory default values. You may want to save the DeviceMaster LT socket configuration using [PortVision DX - Saving a SocketServer Configuration File](#) on Page 81.*

1. If necessary, install PortVision DX using *[Installing PortVision DX](#)* on Page 15 and scan the network to locate the DeviceMaster LT that you want to test.
2. Right-click the DeviceMaster LT and click **Webpage**.
3. Click **System | Restore Defaults**.
4. Click the **Port settings** and **Security settings, password, keys, and certificates** options, and then the **Restore** button.



Restore Defaults

Select the settings you would like to restore to factory defaults, then click the 'Restore' button. After the settings are restored to defaults, the DeviceMaster will reboot and the browswer will redirect to the home page.

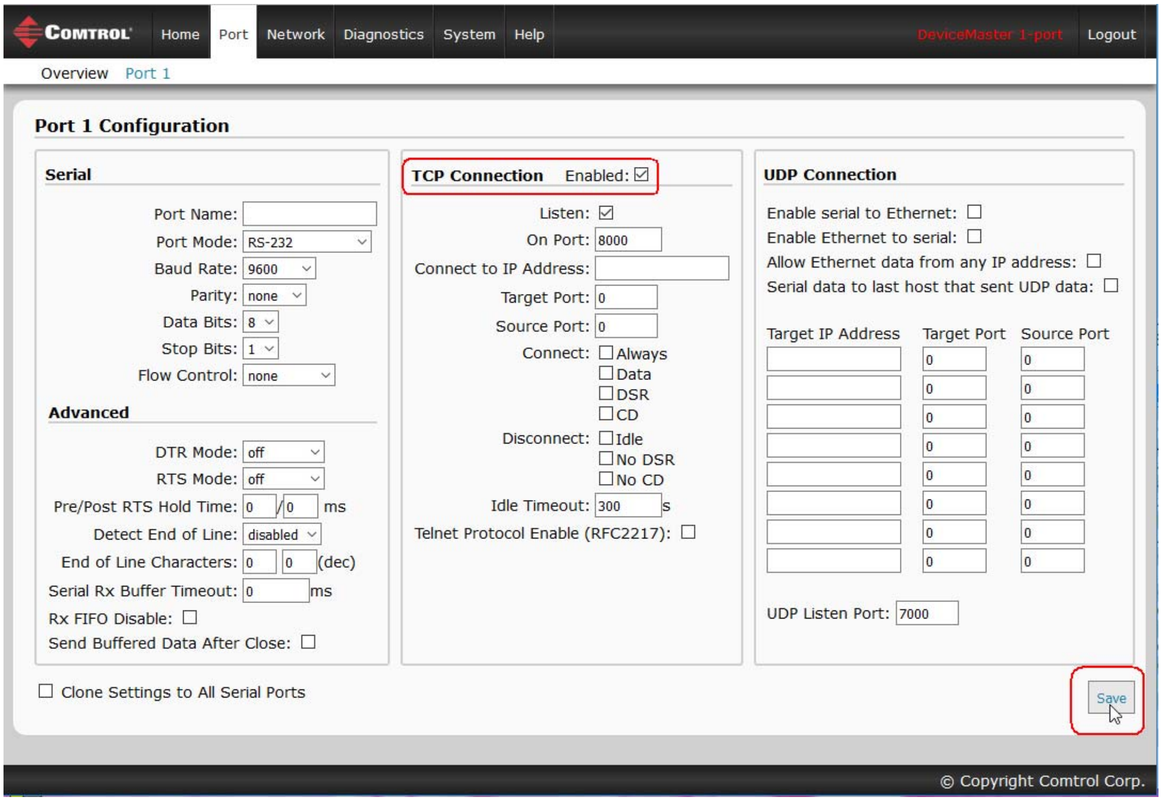
☐ Everything

☑ Port settings (including RFC1006)
☐ Server settings (email configuration, network general settings)
☑ Security settings, password, keys, and certificates
☐ IP address settings

Note: *The DeviceMaster LTwill reboot.*

5. If necessary, re-open the web pages and click the port that you want to test.

6. Under the *TCP Connection Configuration* section, click the **Enable** option, and leave all other settings on this page at their default values.



Port 1 Configuration

Serial

Port Name:
Port Mode: RS-232
Baud Rate: 9600
Parity: none
Data Bits: 8
Stop Bits: 1
Flow Control: none

Advanced

DTR Mode: off
RTS Mode: off
Pre/Post RTS Hold Time: 0 / 0 ms
Detect End of Line: disabled
End of Line Characters: 0 0 (dec)
Serial Rx Buffer Timeout: 0 ms
Rx FIFO Disable: □
Send Buffered Data After Close: □

TCP Connection Enabled: ☑

Listen: ☑
On Port: 8000
Connect to IP Address:
Target Port: 0
Source Port: 0
Connect: □Always □Data □DSR □CD
Disconnect: □Idle □No DSR □No CD
Idle Timeout: 300 s
Telnet Protocol Enable (RFC2217): □

UDP Connection

Enable serial to Ethernet: □
Enable Ethernet to serial: □
Allow Ethernet data from any IP address: □
Serial data to last host that sent UDP data: □

Target IP Address	Target Port	Source Port
	0	0
	0	0
	0	0
	0	0
	0	0
	0	0
	0	0
	0	0

UDP Listen Port: 7000

□ Clone Settings to All Serial Ports

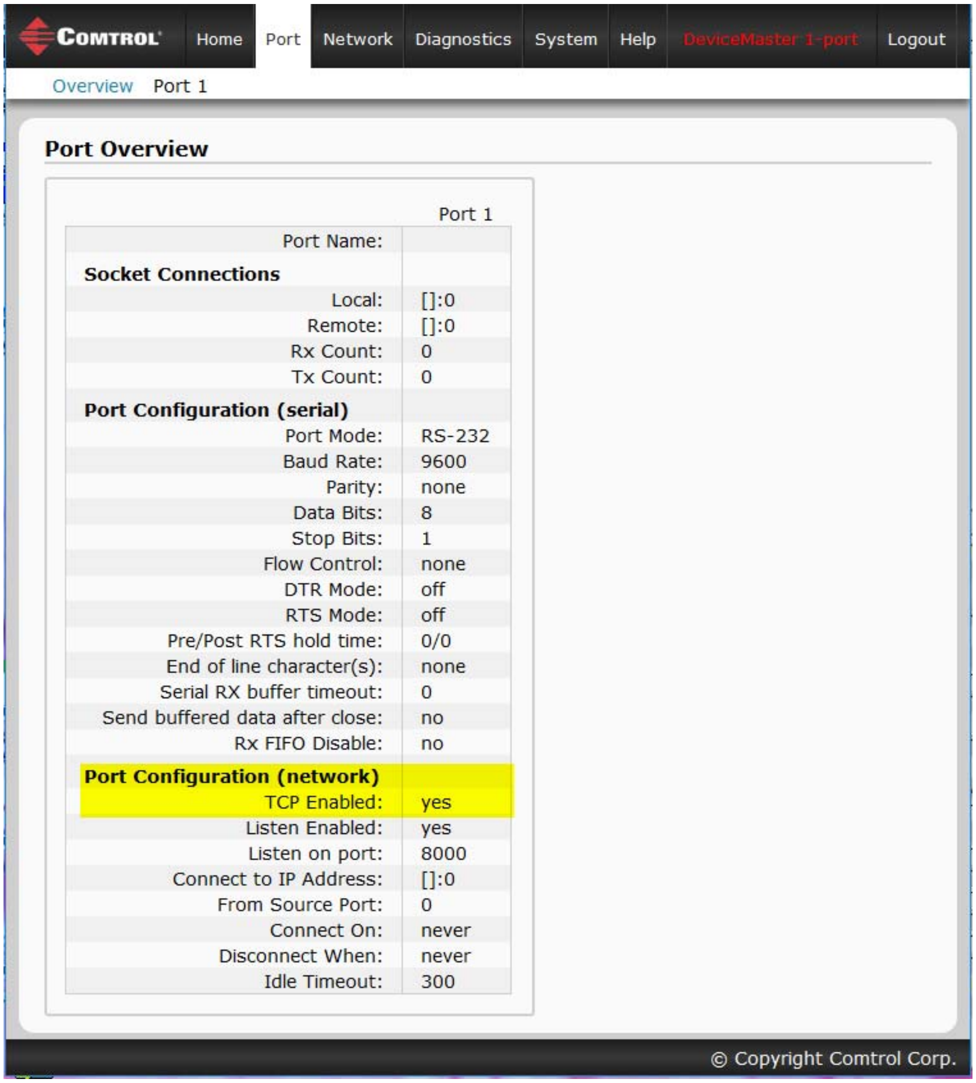
Save

© Copyright Comtrol Corp.

Note: *The Port number as it is needed later in this procedure. In this example, the port number is 8000.*

7. Click the **Save** button.

8. Verify that the port has been enabled.



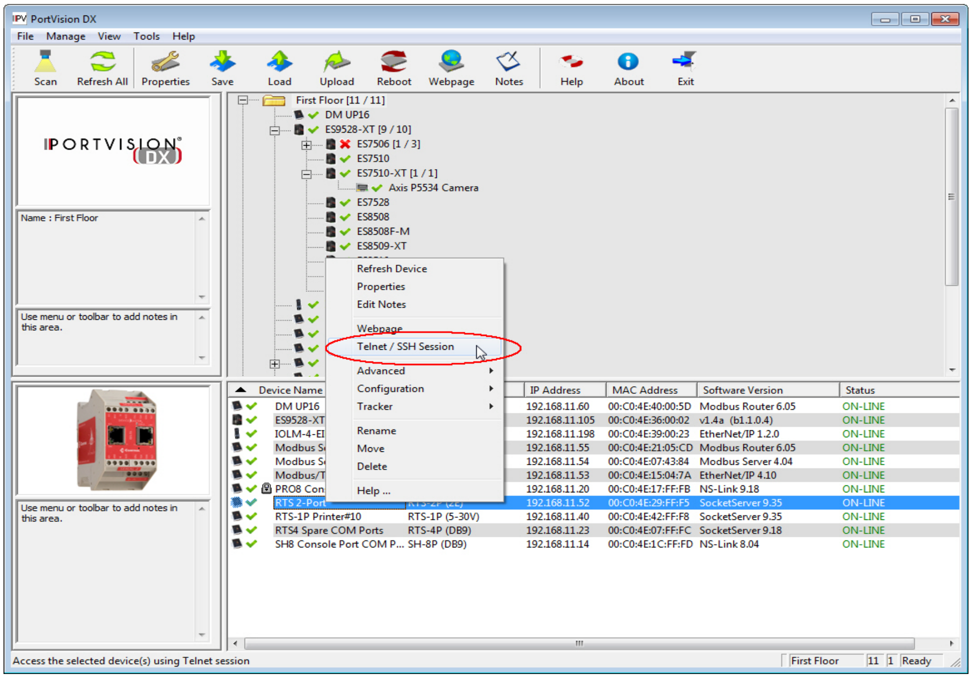
Port Overview

	Port 1
Port Name:	
Socket Connections	
Local:	[]:0
Remote:	[]:0
Rx Count:	0
Tx Count:	0
Port Configuration (serial)	
Port Mode:	RS-232
Baud Rate:	9600
Parity:	none
Data Bits:	8
Stop Bits:	1
Flow Control:	none
DTR Mode:	off
RTS Mode:	off
Pre/Post RTS hold time:	0/0
End of line character(s):	none
Serial RX buffer timeout:	0
Send buffered data after close:	no
Rx FIFO Disable:	no
Port Configuration (network)	
TCP Enabled:	yes
Listen Enabled:	yes
Listen on port:	8000
Connect to IP Address:	[]:0
From Source Port:	0
Connect On:	never
Disconnect When:	never
Idle Timeout:	300

9. Leave the web page open.

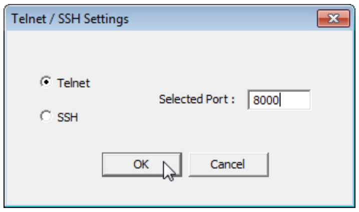
10. Attach the loopback plug that was shipped with the DeviceMaster LT to the serial port of the DeviceMaster LT. See *Connecting Serial Devices* on Page 73 if you need to build a loopback plug.

11. Right-click the DeviceMaster LT in the *Device List* pane and click **Telnet / SSH Session**.



Device Name		IP Address	MAC Address	Software Version	Status
DM UP16		192.168.11.60	00:C0:4E:40:00:5D	Modbus Router 6.05	ON-LINE
ES9528-XT		192.168.11.105	00:C0:4E:36:00:02	v1.4a (b1.1.0.4)	ON-LINE
IOLM-4-EI		192.168.11.198	00:C0:4E:39:00:23	EtherNet/IP 1.2.0	ON-LINE
Modbus S		192.168.11.55	00:C0:4E:21:05:CD	Modbus Router 6.05	ON-LINE
Modbus S		192.168.11.54	00:C0:4E:07:43:84	Modbus Server 4.04	ON-LINE
Modbus/T		192.168.11.53	00:C0:4E:15:04:7A	EtherNet/IP 4.10	ON-LINE
PRO8 Con		192.168.11.20	00:C0:4E:17:FF:FB	NS-Link 9.18	ON-LINE
RTS 2-Port	RTS-2P (2E)	192.168.11.52	00:C0:4E:29:FF:F5	SocketServer 9.35	ON-LINE
RTS-1P Printer#10	RTS-1P (5-30V)	192.168.11.40	00:C0:4E:42:FF:F8	SocketServer 9.35	ON-LINE
RTS4 Spare COM Ports	RTS-4P (DB9)	192.168.11.23	00:C0:4E:07:FF:FC	SocketServer 9.18	ON-LINE
SH8 Console Port COM P...	SH-8P (DB9)	192.168.11.14	00:C0:4E:1C:FF:FD	NS-Link 8.04	ON-LINE

12. Enter the socket number of the port that you are testing (Step 6) and click **Ok**.

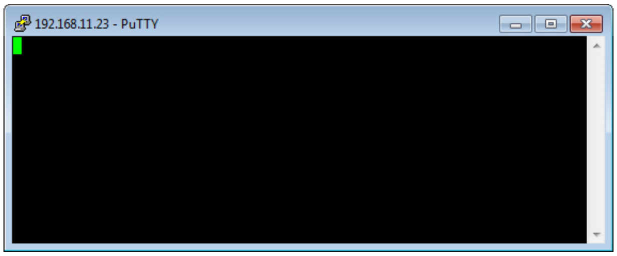


● Telnet

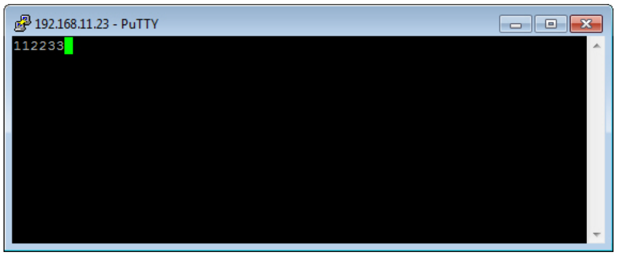
○ SSH

Selected Port : 8000

PuTTY loads.



13. Type 123.

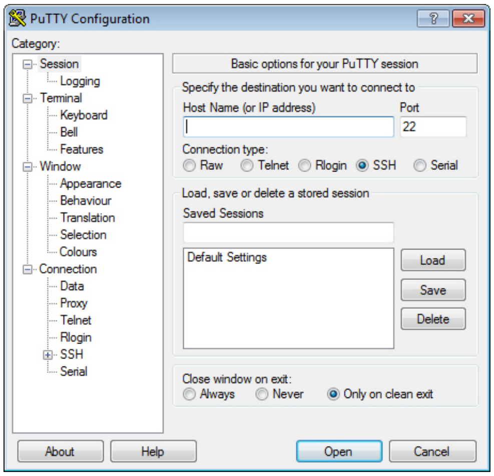


```
112233
```

If 112233 displays, you need to disable local echo. Use the following steps to disable local echo.

a. Go to **c: \Program Files (x86)\Comtrol\PortVision DX**.

b. Execute **PUTTY.EXE** to open the application.



Specify the destination you want to connect to

Host Name (or IP address): | Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

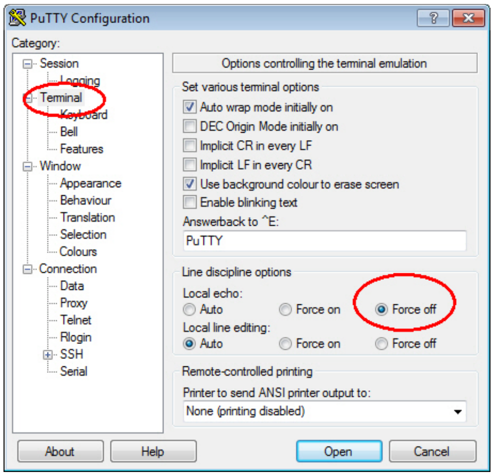
Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

c. Click **Terminal** and click **Force off** for the *Local echo* option.



Set various terminal options

☑ Auto wrap mode initially on

☐ DEC Origin Mode initially on

☐ Implicit CR in every LF

☐ Implicit LF in every CR

☑ Use background colour to erase screen

☐ Enable blinking text

Answerback to ^E: PuTTY

Line discipline options

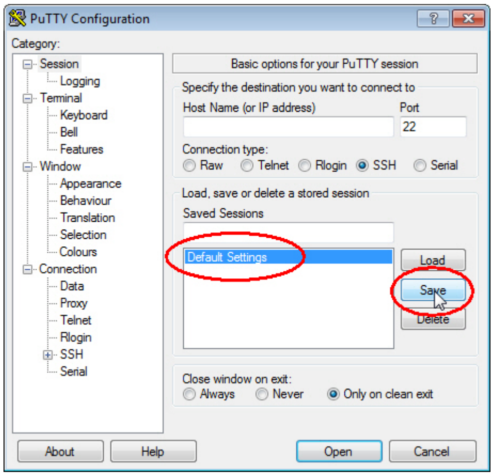
Local echo: ○ Auto ○ Force on ● Force off

Local line editing: ● Auto ○ Force on ○ Force off

Remote-controlled printing

Printer to send ANSI printer output to: None (printing disabled)

d. Return to the **Session** menu, highlight **Default Settings** and then click **Save**.



Specify the destination you want to connect to

Host Name (or IP address): | Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

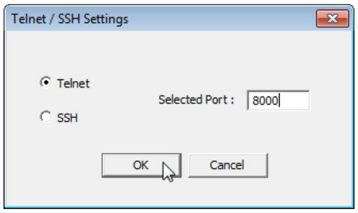
Close window on exit: ○ Always ○ Never ● Only on clean exit

e. Click **Cancel** to close PuTTY.

f. Close the telnet (PuTTY) session that you opened from PortVision DX.

g. Re-open the telnet session by right-clicking the DeviceMaster LT, and select the **Telnet / SSH Session** option.

h. Enter the Socket Port number and then click **Ok**.



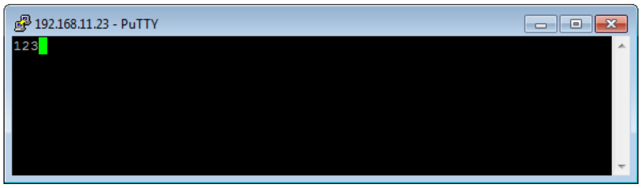
Telnet / SSH Settings

● Telnet

○ SSH

Selected Port : 8000

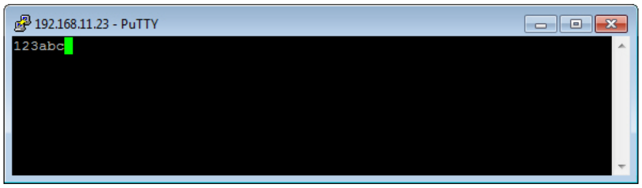
i. Enter **123**, single digits should appear.



192.168.11.23 - PuTTY

```
123
```

14. Remove the loopback plug and type **abc**. No characters should display because the return path is open.
15. Re-attach the loopback plug, type **abc**, and the characters should appear.



192.168.11.23 - PuTTY

```
123abc
```

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.

DeviceMaster LT LEDs

The DeviceMaster LT has network and port LEDs to indicate status. This subsection discusses:

- *TX/RX LEDs*
- *Network and Device LEDs* on Page 134

TX/RX LEDs

This subsection discusses RX and TX LEDS on the DeviceMaster LT.

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

Note: *The RX/TX LEDs cycle during the reboot cycle.*

The LEDs do not function as described until the port has been opened by an application.

You can use Test Terminal to open a port or ports if you want to test a port or ports.

The RX (green) and TX (yellow) LEDs functions are displayed in the following table when the cable is attached properly to a serial device.

LED	Mode	Description	LED Status
RX (Green)	RS-232	No valid RS-232 device is connected	Always off
		Valid RS-232 device is connected but no data transmission is occurring	On
		Data being received	LED blinks
	RS-422/485	No data being received	Always off
		Data being received	LED blinks
	No mode	No mode selected	Always off
TX (Yellow)	RS-232/422/485	No data being transmitted	Always off
		Data being transmitted	LED blinks

Network and Device LEDs

- The LEDs indicate that the default DeviceMaster LT application, SocketServer is running or after driver installation, that the NS-Link driver loads. If you have loaded PortVision DX, you can check the DeviceMaster LT status on-line.If the **Status** LED on the DeviceMaster LT is lit, it indicates the DeviceMaster LT has power and it has completed the boot cycle.

  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.

- The green Ethernet LED indicates that a link has been established and the yellow Ethernet LED indicates activity.

Removing DeviceMaster LT Security Features

When presented with a DeviceMaster LT that has had all security options set and the user is unaware of what the settings are, the restoring of a DeviceMaster LT can be very difficult.

It may be necessary to use the DeviceMaster LT debug dongle provided with the *Software Developers Kit* (SDK) or return the DeviceMaster LT to Comtrol after obtaining an return material authorization (RMA) so that Comtrol can re-flash the DeviceMaster LT with default values.

One of the following two conditions must be true, so that you can remove the security settings from the DeviceMaster LT.

- 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 DX.

Serial Connection Method

Use the following procedure to set up serial connection with a terminal server program (for example, Test Terminal (WCom2), HyperTerminal or Minicom) and the DeviceMaster LT.

Note: *Optionally, you can use Test Terminal, which is included in PortVision DX under the* **Tools >Applications > Test Terminal** *menu.*

1. Connect a null-modem cable from an available COM port on your PC to **Port 1** on the DeviceMaster LT.

   Note: *See Connecting Serial Devices on Page 73 to build a null-modem cable.*

2. Configure the terminal server program to the following values:
   - Bits per second = 57600
   - Data bits = 8
   - Parity = None
   - Stop bits = 1
   - Flow control = None

3. Reset the DeviceMaster LT.

   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
```

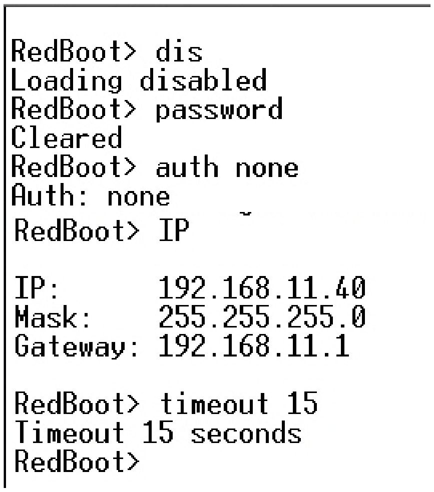
5. At the **RedBoot>** prompt, type **dis**, and press **Enter**.

   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 LT must be returned to Comtrol for re-flashing.*

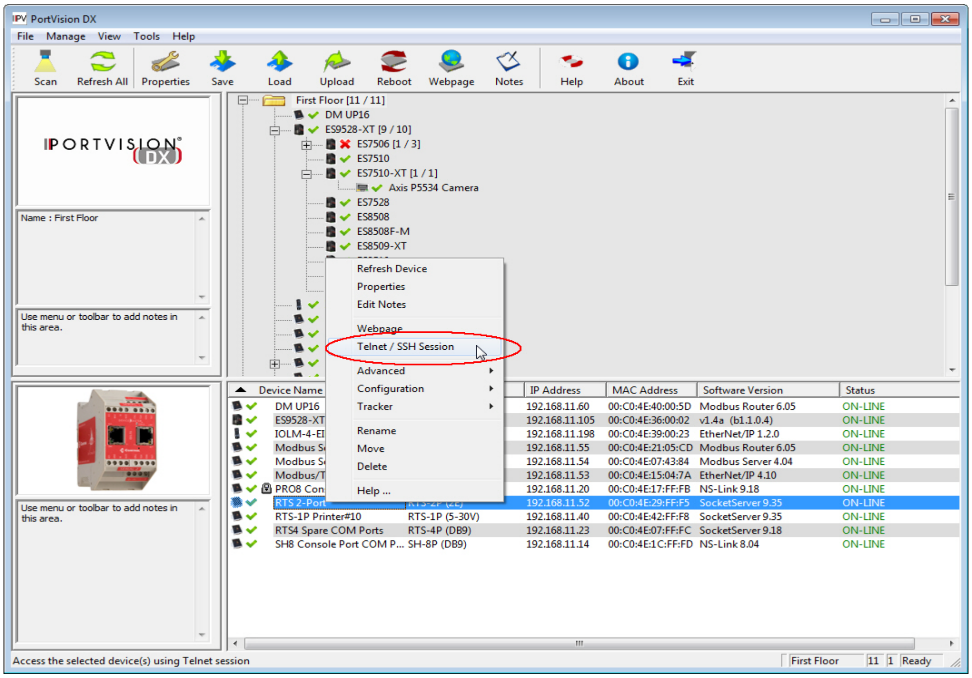
10. Connect the DeviceMaster LT directly to the PC/laptop running PortVision DX.



```
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>
```

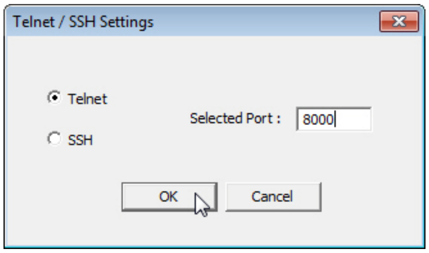
   Note: *If necessary, see Installing PortVision DX on Page 15.*

11. Open PortVision DX.
12. Scan the network so that PortVision DX discovers the DeviceMaster LT.
13. Right-click the DeviceMaster LT and then click **Telnet/SSH Session**.



Device Name		IP Address	MAC Address	Software Version	Status
DM UP16		192.168.11.60	00:C0:4E:40:00:5D	Modbus Router 6.05	ON-LINE
ES9528-XT		192.168.11.105	00:C0:4E:36:00:02	v1.4a (b1.1.0.4)	ON-LINE
IOLM-4-EI		192.168.11.198	00:C0:4E:39:00:23	EtherNet/IP 1.2.0	ON-LINE
Modbus S		192.168.11.55	00:C0:4E:21:05:CD	Modbus Router 6.05	ON-LINE
Modbus S		192.168.11.54	00:C0:4E:07:43:84	Modbus Server 4.04	ON-LINE
Modbus/T		192.168.11.53	00:C0:4E:15:04:7A	EtherNet/IP 4.10	ON-LINE
PRO8 Con		192.168.11.20	00:C0:4E:17:FF:FB	NS-Link 9.18	ON-LINE
RTS 2-Port	RTS-2P (2E)	192.168.11.52	00:C0:4E:29:FF:F5	SocketServer 9.35	ON-LINE
RTS-1P Printer#10	RTS-1P (5-30V)	192.168.11.40	00:C0:4E:42:FF:F8	SocketServer 9.35	ON-LINE
RTS4 Spare COM Ports	RTS-4P (DB9)	192.168.11.23	00:C0:4E:07:FF:FC	SocketServer 9.18	ON-LINE
SH8 Console Port COM P...	SH-8P (DB9)	192.168.11.14	00:C0:4E:1C:FF:FD	NS-Link 8.04	ON-LINE

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



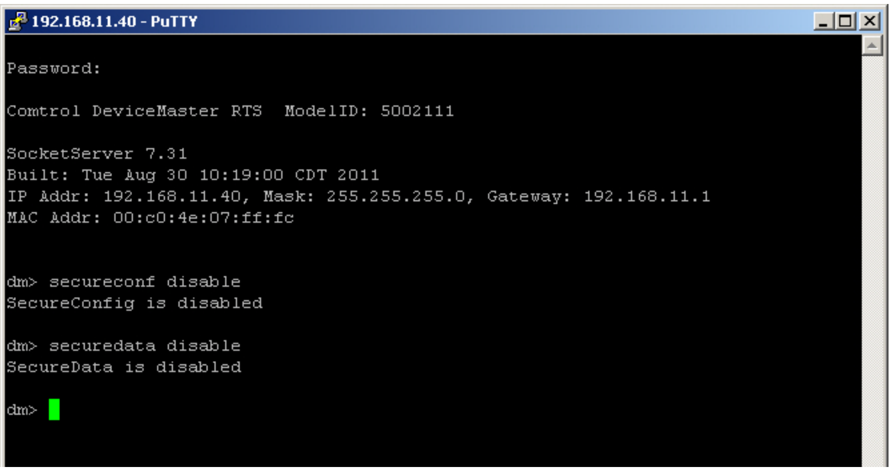
Telnet / SSH Settings

● Telnet

○ SSH

Selected Port : 8000

15. Press **Enter** at the *Password* prompt.
16. Enter **secureconf disable** and press **Enter**.
17. Enter **securedata disable** and press **Enter**.



192.168.11.40 - PuTTY

```
Password:

Comtrol DeviceMaster RTS  ModelID: 5002111

SocketServer 7.31
Built: Tue Aug 30 10:19:00 CDT 2011
IP Addr: 192.168.11.40, Mask: 255.255.255.0, Gateway: 192.168.11.1
MAC Addr: 00:c0:4e:07:ff:fc


dm> secureconf disable
SecureConfig is disabled

dm> securedata disable
SecureData is disabled

dm>
```

Returning the DeviceMaster LT to Factory Defaults

The DeviceMaster LT 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 LT.

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 LT using a serial connection, that is Port 1 through a null-modem cable and a COM port.

See *Establishing a Serial Connection* on Page 106 (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 LT 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 139
- *Web Server Access* on Page 139

Telnet Access

Use this procedure to access the DeviceMaster LT configuration through telnet,

Note: *To reset authentication, see Serial Port Access on Page 139 or use the RedBoot Command Overview on Page 111.*

1. Open a telnet session, enter the DeviceMaster LT 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 LT 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 LT products running SocketServer 7.0 and later.

Serial Port Access

To use the serial method to access the DeviceMaster LT configuration, use *Establishing a Serial Connection* on Page 106. 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 LT products running SocketServer 7.0 and later.

Web Server Access

You can optionally use SocketServer (or the NS-Link equivalent) to access the DeviceMaster LT configuration and reset many values to their default values.

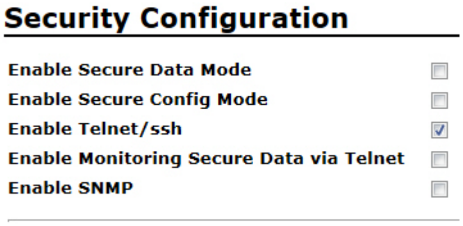
Some of the values require resetting the DeviceMaster LT to take effect. After changing the IP addresses and resetting the DeviceMaster LT, it will not reconnect automatically. You will need to use the new IP address to reconnect.

Note: *The authentication method and the password cannot be changed using SocketServer.*

To reset authentication, see Serial Port Access on Page 139 or use the RedBoot Command Overview on Page 111.

To reset the password, see Configuring Passwords on Page 110 or Telnet Access on Page 138.

1. Open your web browser and enter the IP address of the DeviceMaster LT.
2. Click the **Security** tab:



Security Configuration

Enable Secure Data Mode ☐

Enable Secure Config Mode ☐

Enable Telnet/ssh ☑

Enable Monitoring Secure Data via Telnet ☐

Enable SNMP ☐

   a. Verify that the **Enable Secure Data Mode** option is not checked.
   b. Verify that the **Enable Secure Config Mode** option is not checked.
   c. Verify that the **Enable Telnet/SSH** option is checked.
   d. Verify that the **Enable Monitoring Secure Data via Telnet** option is not checked.
   e. Verify that the **Enable SNMP** option is checked.
   f. Click **Save**.
   g. Click **OK** when reminded it is necessary to reboot to take effect.
3. Click the **Email** tab:
   a. Verify that the **SMTP Server IP Address** is set to: 0.0.0.0.
   b. Verify that all remaining options are clear.
   c. Click **Save**.
   d. Click **OK**.
4. Return to the *Server Status* (home) page and click **Reboot**.
5. Click **Set configuration for all ports to factory default settings**.

6. Click **Yes: Reboot**.
7. Click the **Network** tab and make the following changes:
   a. Click the **Use static configuration below** check box and enter the following values:
      - Set the IP Address to 192.168.250.250.
      - Set the Netmask to 255.255.0.0.
      - Set the Gateway to 192.168.250.1.
      - Set the Bootloader Timeout to 15.

   b. Click **Save**.

   c. Click **OK** when reminded it is necessary to reboot to take effect.

The DeviceMaster LT reboots. When it starts running, everything will have been returned to factory default values.If you choose to verify the values, the IP address has been reset to 192.168.250.250.

Technical Support

If you are using an NS-Link driver for a Windows system, you should review the troubleshooting section in the *DeviceMaster LT Device Driver (NS-Link) User Guide for Windows* (Page 9) before contacting Technical Support.

It contains troubleshooting procedures that you should perform before contacting Technical Support since they will request that you perform, some or all of the procedures before they will be able to help you diagnose your problem. If you need technical support use one of the following methods.

Comtrol Contact Information	
Downloads (FTP)	ftp://ftp.comtrol.com/html/up_main.htm
Downloads (HTTP)	http://downloads.comtrol.com/html/default.htm
Web site	http://www.comtrol.com
Phone	(763) 957-6000