



User Guide



Trademark Notices

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

Microsoft and Windows are registered trademarks of Microsoft Corporation.

HyperTerminal is a registered trademark of Hilgraev, Inc.

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

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

First Edition, January 20, 2014

Copyright © 2014. Control Corporation.

All Rights Reserved.

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

Table of Contents

Introduction	7
DeviceMaster LT Port Usage	7
Installation Overview	7
NS-Link COM Port Driver Installation Overview	8
NS-Link tty Port Installation Overview	8
TCP/IP Socket Port Installation Overview	9
Locating Software and Documentation	9
Hardware Installation.....	11
Initial Configuration	13
PortVision DX Overview	13
PortVision DX Requirements.....	14
Configuring Security Settings and PortVision DX.....	14
Installing PortVision DX.....	15
Configuring the Network Settings	18
Checking the SocketServer Version	22
Uploading SocketServer with PortVision DX.....	24
Customizing PortVision DX	26
Accessing DeviceMaster LT Documentation from PortVision DX.....	27
How to Download Documentation	27
How to Open Previously Downloaded Documents	28
Device Driver (NS-Link) Installation	29
Overview	29
Before Installing the NS-Link Driver	29
Linux Installations	30
Windows Installations	31
Supported Operating Systems	31
Installation Overview for Windows	31
NS-Link for Windows Installation.....	31
Configuring the NS-Link Driver for Windows.....	35
Configuring COM Port Properties for Windows	38
Enabling Secure Data Mode.....	39
Socket Port Configuration	41
SocketServer Overview	41
Web Page Help System.....	41
SocketServer Architecture	42
Accessing Socket Configuration	43
Web Browser	43
PortVision DX	43
SocketServer Versions	44

DeviceMaster LT Security	45
Understanding Security Methods and Terminology	45
TCP and UDP Socket Ports Used by the DeviceMaster LT	50
DeviceMaster LT Security Features	51
Security Modes.....	51
Secure Data Mode and Secure Config Mode Comparison	52
Security Comparison	52
SSH Server.....	53
SSL Overview.....	53
SSL Authentication	53
Server Authentication.....	53
<i>Client Authentication</i>	54
Certificates and Keys	54
SSL Performance	56
SSL Cipher Suites.....	56
DeviceMaster LT Supported Cipher Suites	57
SSL Resources	57
Configure/Enable Security Features Overview	58
Example 1.....	60
Example 2.....	60
Example 3.....	61
Key and Certificate Management.....	61
Using a Web Browser to Set Security Features	63
Changing Security Configuration	63
Changing Keys and Certificates	64
Connecting Serial Devices	65
RJ45 Null-Modem Cables (RS-232)	66
RJ45 Null-Modem Cables (RS-422)	66
RJ45 Straight-Through Cables (RS-232/485)	66
RJ45 Loopback Plugs	67
RJ45 RS-485 Test Cable	67
Connecting RJ45 Devices	67
Managing the DeviceMaster LT	69
Rebooting the DeviceMaster LT	69
Updating Firmware Across WANs (Windows)	70
Uploading SocketServer to Multiple DeviceMaster LTs	74
Configuring Multiple DeviceMaster LTs Network Addresses	75
Adding a New Device in PortVision DX	75
Remote Using the IP Address	75
Local Using the IP Address or MAC Address	76
Using SocketServer Configuration Files	77
Saving a SocketServer Configuration File	77
Loading a SocketServer Configuration File	77
Using Driver Configuration Files	79
Saving Driver Configuration Files.....	79
Saving Device-Level Configuration.....	79
Saving Port-Level Configuration.....	80
Loading Driver Configuration Files.....	81
Loading Device Configuration	81
Loading Port Configuration	82
Changing the Bootloader Timeout	84

Managing Bootloader	85
Checking the Bootloader Version.....	85
Uploading Bootloader	85
Checking the NS-Link Version	87
Restoring Serial Port Settings	88
NS-Link COM Port	88
Socket Port	88
Accessing SocketServer Commands in Telnet/SSH Sessions (PortVision DX)	90
Telnet Session	90
SSH Session	92
Accessing RedBoot Commands in Telnet/SSH Sessions (PortVision DX)	94
RedBoot Procedures	99
Accessing RedBoot Overview	99
Establishing a Serial Connection	100
Establishing a Telnet Connection	101
Determining the Network Settings	102
Configuring the Network Settings	102
Changing the Bootloader Timeout	103
Determining the Bootloader Version	103
Resetting the DeviceMaster LT	104
Uploading Firmware - Telnet Method (Linux)	104
Setting Up a TFTP Server in Linux	104
Uploading the Firmware	105
Configuring Passwords	106
RedBoot Command Overview	107
Hardware Specifications	109
Locating DeviceMaster LT Specifications	109
External Power Supply Specifications	109
Notices	110
Radio Frequency Interference (RFI) (FCC 15.105).....	110
Labeling Requirements (FCC 15.19)	110
Modifications (FCC 15.21).....	110
Serial Cables (FCC 15.27)	110
Underwriters Laboratory	110
Important Safety Information.....	110
Troubleshooting and Technical Support	111
Troubleshooting Checklist	111
General Troubleshooting	113
Testing Ports Using Port Monitor (PMon2)	115
Overview	115
Testing Control COM Ports.....	115
Testing Ports Using Test Terminal	118
Overview	118
Opening Ports	119
Sending and Receiving Test Data (RS-232/422/485: 4-Wire)	119
Loopback Test (RS-232).....	120
Sending and Receiving Data (RS-485: 2-Wire)	121
Socket Mode Serial Port Testing	124

- DeviceMaster LT LEDs..... 129**
 - TX/RX LEDs..... 129
 - Network and Device LEDs 130
- Removing DeviceMaster LT Security Features..... 131**
 - Serial Connection Method..... 131
- Returning the DeviceMaster LT to Factory Defaults 133**
 - Clearing the Flash 134
 - Clearing EEPROM..... 134
 - Telnet Access 134
 - Serial Port Access 135
 - Web Server Access..... 135
- Technical Support 136**

Introduction

This section discusses the following topics:

- [DeviceMaster LT Port Usage](#) (below)
- [Installation Overview](#) on Page 7
 - [NS-Link COM Port Driver Installation Overview](#) on Page 8
 - [NS-Link tty Port Installation Overview](#) on Page 8
 - [TCP/IP Socket Port Installation Overview](#) on Page 9
- [Locating Software and Documentation](#) on Page 9

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 18 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 22 to determine the version on the DeviceMaster LT.
- b. If necessary, update SocketServer. See [Uploading SocketServer with PortVision DX](#) on Page 24.

Note: *In rare cases, you may need to update Bootloader to support a new*

feature. Notice will posted with SocketServer or the NS-Link device driver.

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 31 for an installation overview of the NS-Link driver for Windows operating systems.

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

Note: *Although the ftp link displays win7 in the path, the driver supports multiple [Windows](#) operating systems (Page 14).*
3. Configure the COM ports using the *Control Drivers Management Console*. See [Configuring the NS-Link Driver for Windows](#) on Page 35, which provides an overview of COM port configuration.
4. Configure device properties, you can refer to [Configuring COM Port Properties for Windows](#) on Page 38.
5. Optionally, you may need to configure one or more ports for socket mode. See [Socket Port Configuration](#) on Page 41 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 65 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. You can use the CD to access the ftp site or this address: ftp://ftp.comtrol.com/dev_mstr/lt/drivers/linux/ to locate the latest version of NS-Link Linux device driver.

Refer to the **readme** file packaged with the Linux driver assembly for driver installation and configuration procedures for the tty port.
3. Optionally, you may need to configure one or more ports for socket mode. See [Socket Port Configuration](#) on Page 41 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 65 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 41 for information for configuration procedures.

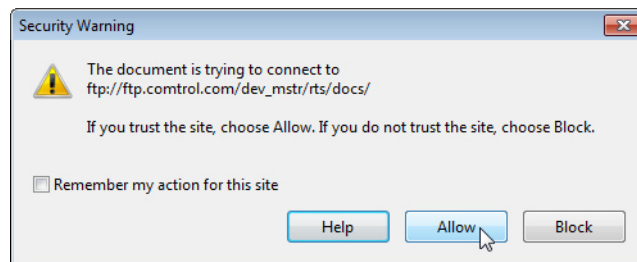
3. Connect the serial devices to the DeviceMaster LT. Refer to [Connecting Serial Devices](#) on Page 65 for cabling and connector information.

Locating Software and Documentation







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

- *Control Software and Documentation* CD shipped with the DeviceMaster LT provides links to the latest files.
- 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 27 for more information.
- Check for and download the latest files using the links in the following table.

Note: Depending on your Windows operating system you may need to respond to a Security Warning popup.



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. Note: <i>May sure that you download SocketServer for the DeviceMaster LT (link at right). Other DeviceMaster models use a unique version of SocketServer.</i>	
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 8 Windows Server 2012 Windows 7 Windows Server 2008 Windows Vista Windows Server 2003 Windows XP	Install if you want COM ports. Refer to the DeviceMaster Device Driver (NS-Link) User Guide . for detailed information.	
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 ftp site when checking for the latest SocketServer or device driver version. Note: <i>May sure that you download Bootloader for the DeviceMaster LT (link at right). Other DeviceMaster models use a unique version of Bootloader.</i>	
This Guide	Any	You can check for the latest version of this <i>Guide</i> .	

Hardware Installation

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

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

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

Note: Do not connect multiple units until you have changed the default IP address, see [Initial Configuration](#) on Page 13.

2. Place the DeviceMaster LT on a stable surface.
3. 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.

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 109 if you want to provide your own power supply.
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. Control 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 and upload SocketServer, see [RedBoot Procedures](#) on Page 99.

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 18](#))
- Check the SocketServer version on the DeviceMaster LT ([Page 22](#))
- If necessary, download the latest version SocketServer and upload it into the DeviceMaster LT ([Page 24](#))
- Organize how PortVision DX displays your Control Ethernet attached products
- Access the latest documentation for your Control Ethernet attached product

PortVision DX Overview

PortVision DX automatically detects Control 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
 - DeviceMaster PRO
 - DeviceMaster RTS
 - DeviceMaster Serial Hub
 - DeviceMaster UP
 - DeviceMaster 500
- DeviceMaster LT
- IO-Link Master
- RocketLinx switches

In addition to identifying Control 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-Control 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 the following Windows operating systems:

- Windows 8.1
- Windows 8
- Windows Server 2012
- Windows 7
- Windows Server 2008
- Windows Vista
- Windows Server 2003
- Windows XP

PortVision DX requires that you connect the Control 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.

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.

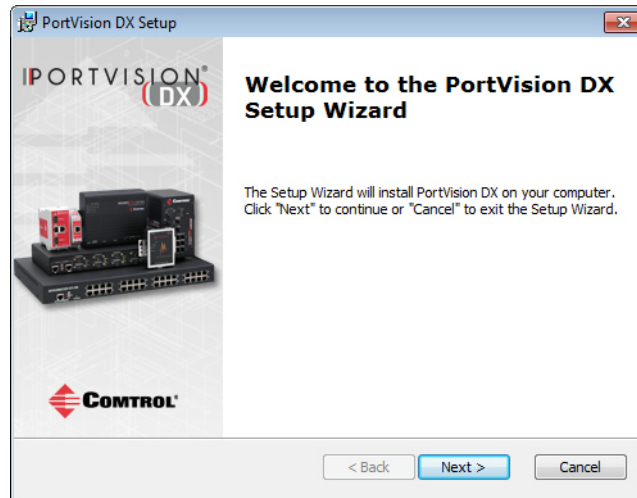
Use the *Software and Documentation* CD that came with the DeviceMaster LT to check for the latest version of PortVision DX or use the link below to download the latest version.

1. Locate PortVision DX using one of the following methods to download the latest version:
 - **Software and Documentation CD:** You can use the CD menu system to check the version on the CD against the latest released version.

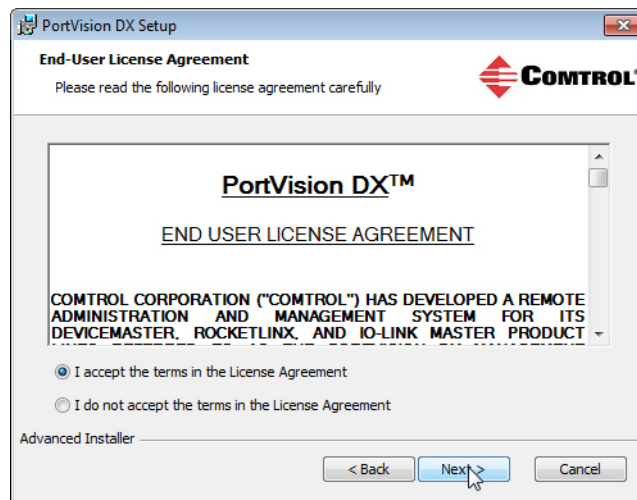
- **FTP site subdirectory:**
ftp://ftp.control.com/dev_mstr/portvision_dx.

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

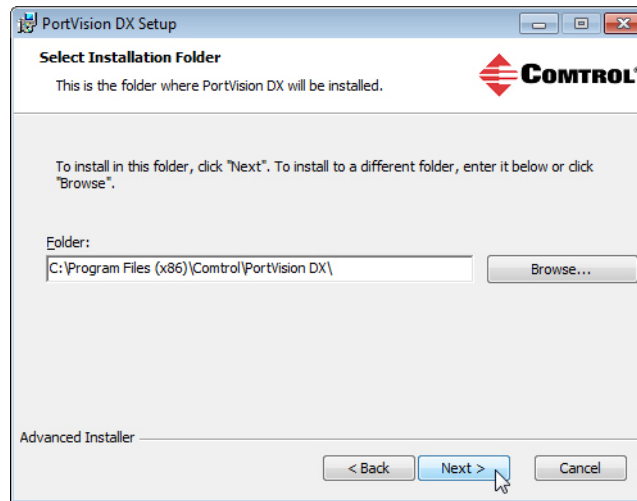
2. Execute the **PortVision_DX[version].msi** file.
3. Click **Next** on the *Welcome* screen.



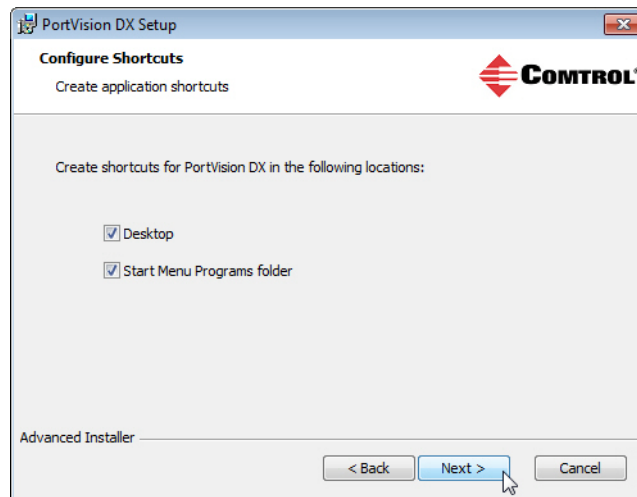
4. Click **I accept the terms in the License Agreement** and **Next**.



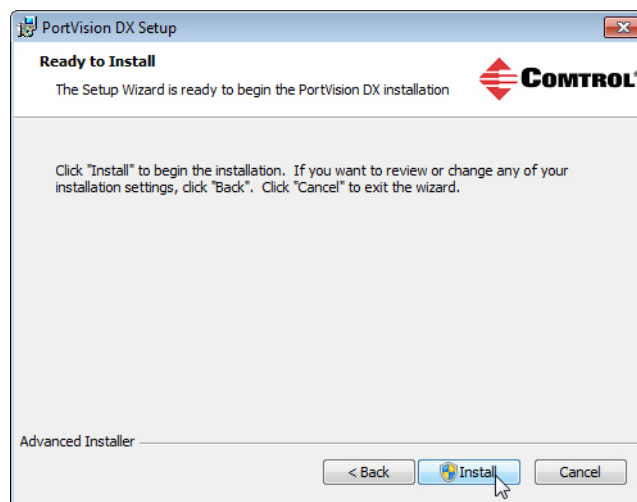
5. Click **Next** or optionally, browse to a different location and then click **Next**.



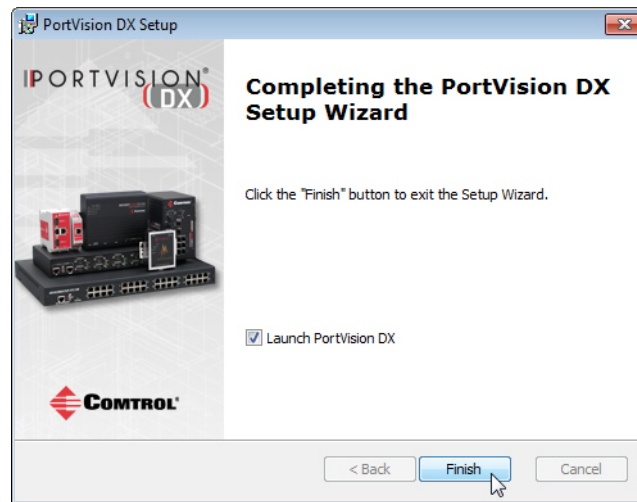
6. Click **Next** to configure the shortcuts.



7. Click **Install**.

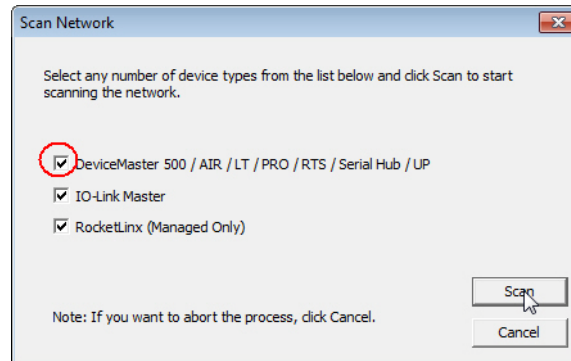


8. Depending on the operating system, you may need to click **Yes** to the *Do you want to allow the following program to install software on this computer?* query.
9. Click **Launch PortVision DX** and **Finish** in the last installation screen.



10. 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.
11. Select the Control Ethernet attached products that you want to locate and then click **Scan**.

You can save time if you only scan for DeviceMasters.



Note: *If the Control 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 Control Ethernet attached product to PortVision DX.*

12. 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

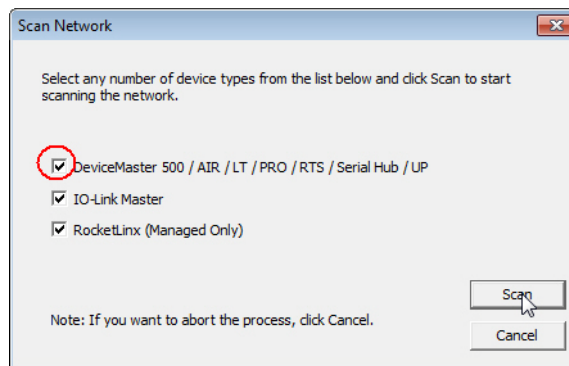
Subnet mask:
255.255.0.0

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 75.*

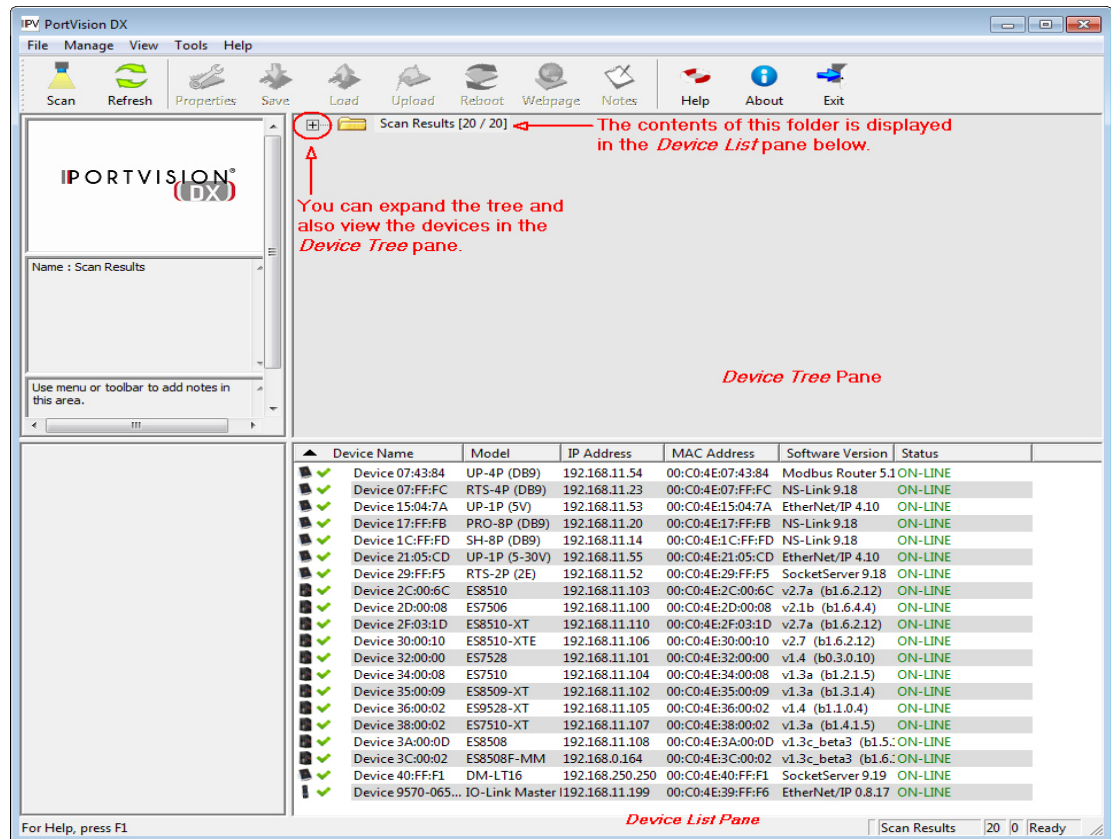
The following procedure shows how to configure a single DeviceMaster LT connected to the same network segment as the Windows system. If the DeviceMaster LT is not on the same physical segment, you can add it manually using [Adding a New Device in PortVision DX](#) on Page 75.

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 > Control > 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 Control Ethernet attached products including the DeviceMaster LT on the network.

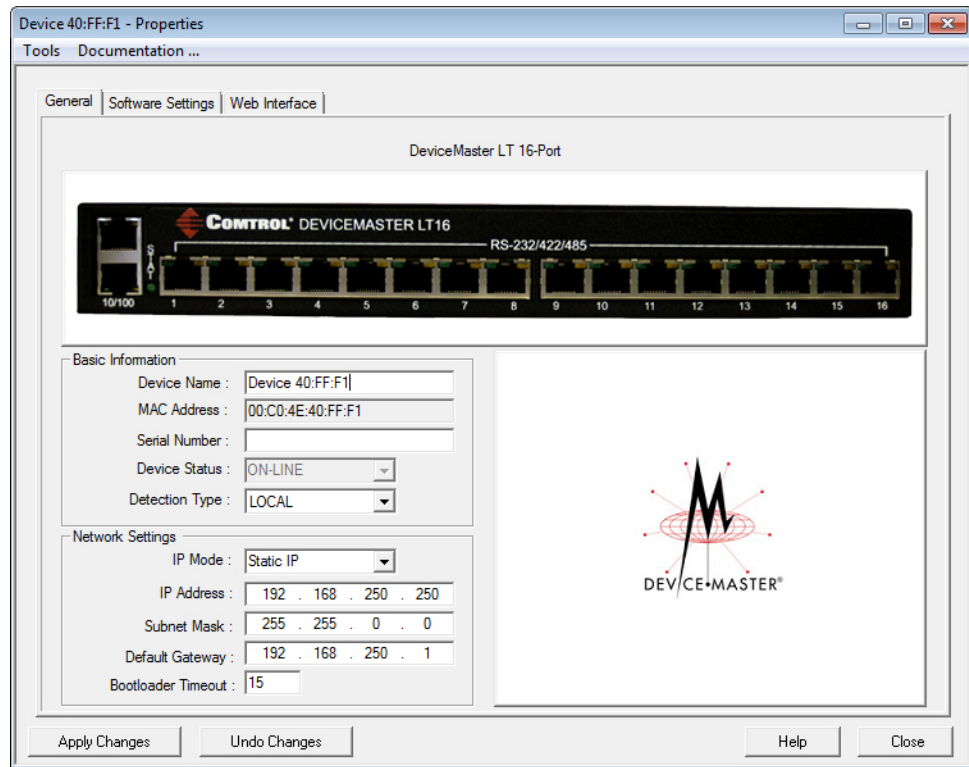


Note: *If you do not have any RocketLinx managed switches or IO-Link Masters, it saves scanning time if you do not scan for them.*

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**.



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



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 its 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 77 for more information.*
12. Click **Close** to exit the *Properties* window.
13. Go to [Checking the SocketServer Version](#) on Page 22 to check the SocketServer version. You should update SocketServer firmware before any further configuration.

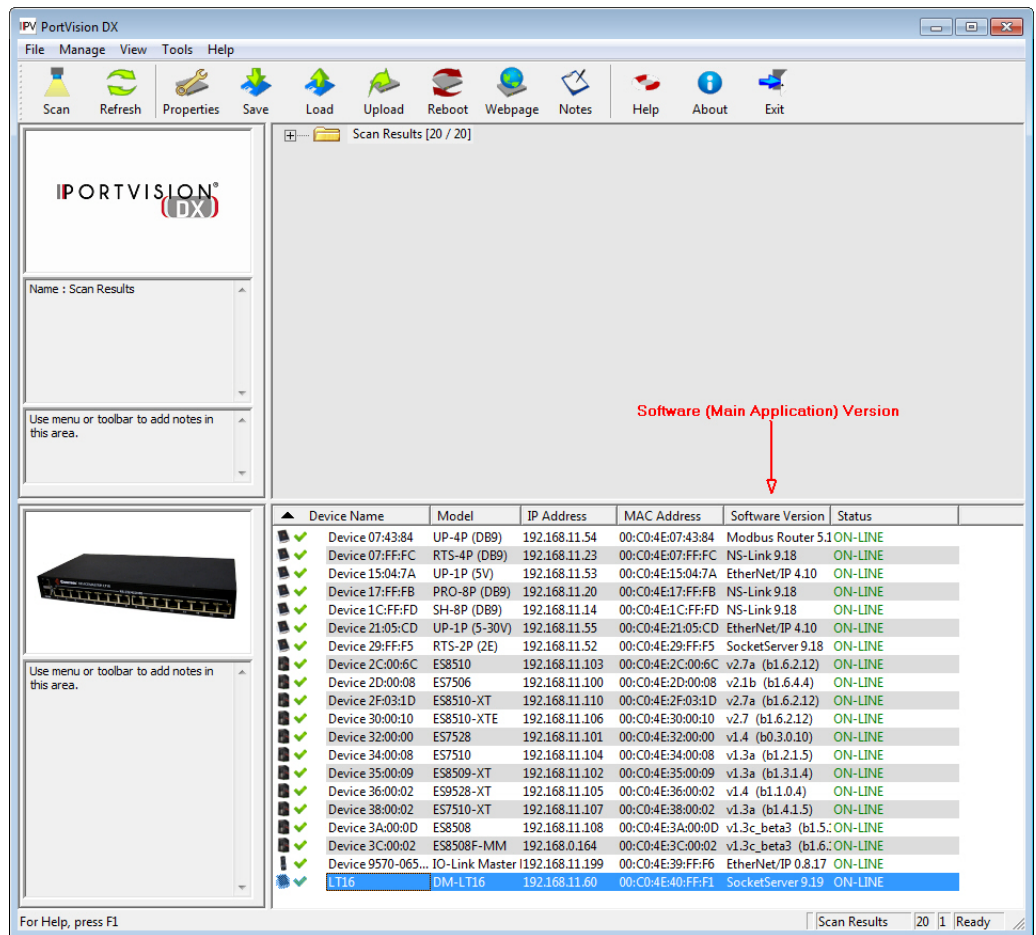
Checking the SocketServer Version

[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 > Start/Programs > Control > PortVision DX > 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.



3. Check the Control 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](#)

03/11/2013 02:16PM	124,405	1800111_socketserver_history.pdf
02/08/2013 10:42AM	Directory	help
10/02/2012 10:08AM	1,174,340	socketserver-8.04.bin

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 24.

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

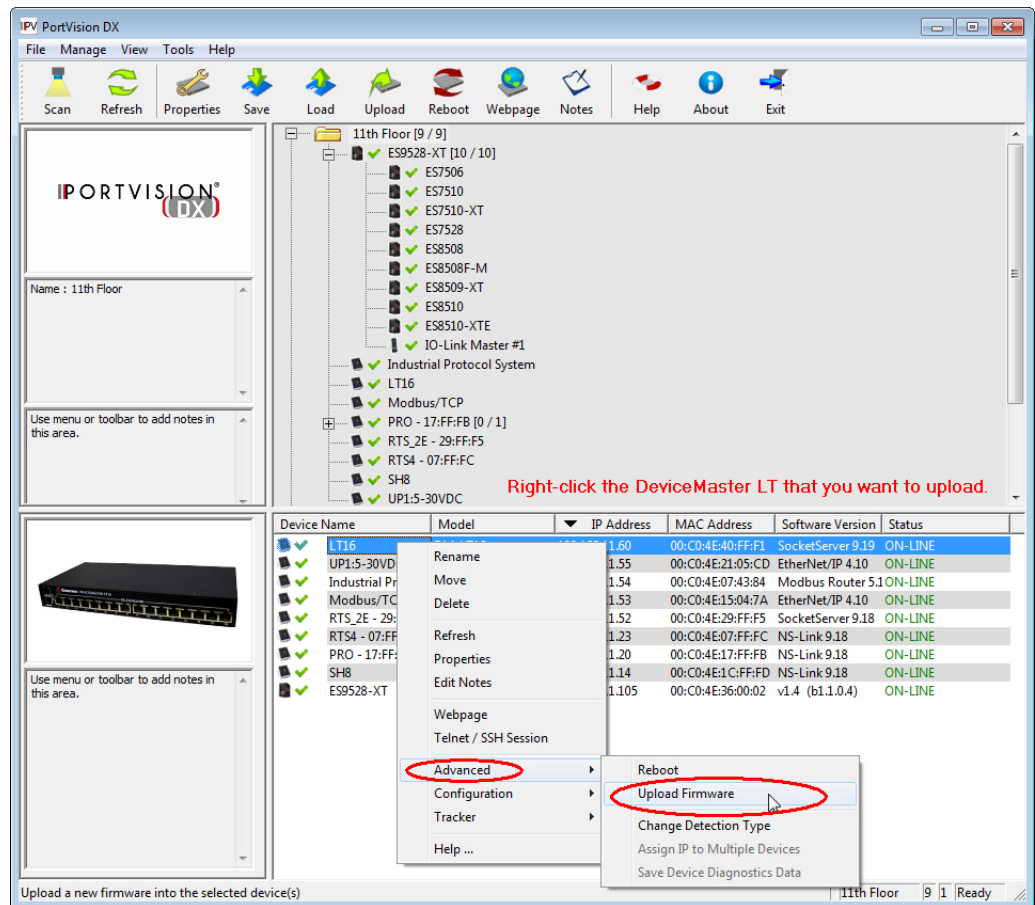
Uploading SocketServer with PortVision DX

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.

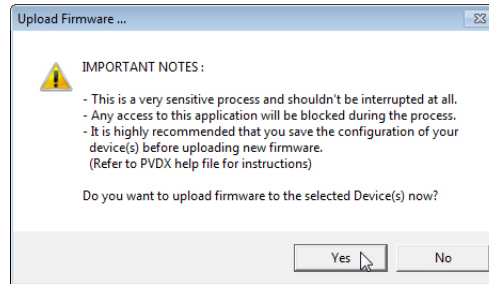
If the DeviceMaster LT is on the other side of several switches, a router, or wireless, go to [Updating Firmware Across WANs \(Windows\)](#) on Page 70, which provides more reliable uploads.

1. Make sure that you have downloaded the latest SocketServer version from: ftp://ftp.control.com/dev_mstr/rts/software/socketserver.
2. If necessary, open **PortVision DX > Start/Programs > Control > PortVision DX > 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 .bin file, and then click **Open**.



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.



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 84.

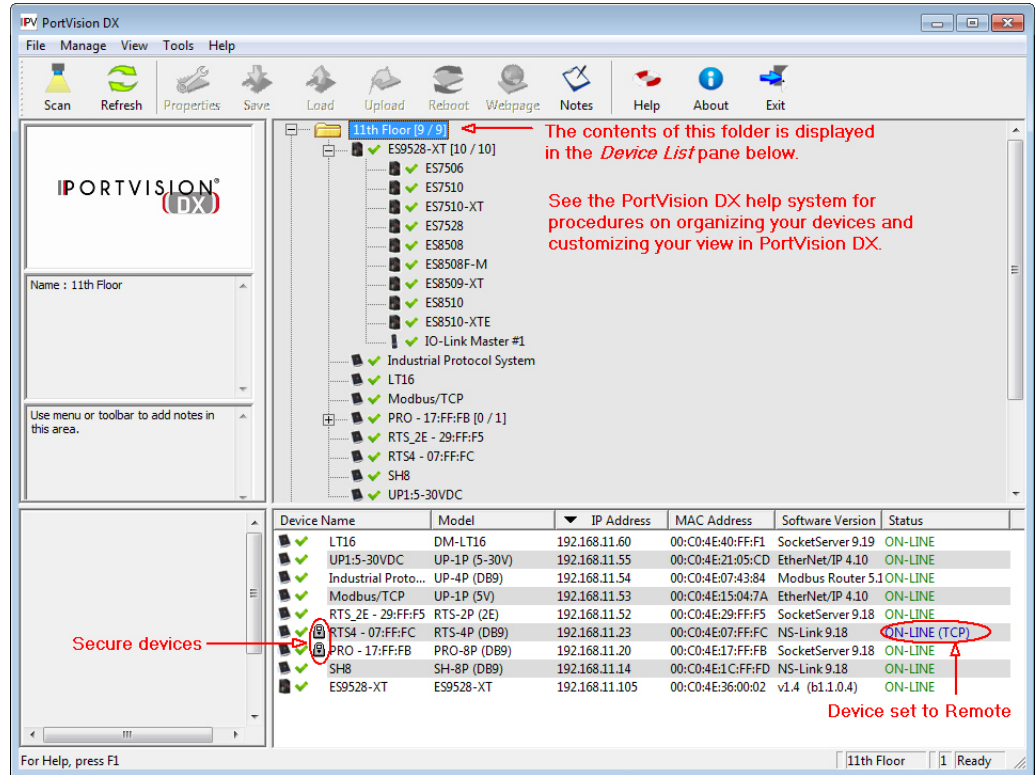
You are now ready to continue the installation and configuration process.

- [Device Driver \(NS-Link\) Installation](#) on Page 29
- [Socket Port Configuration](#) on Page 41

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.



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

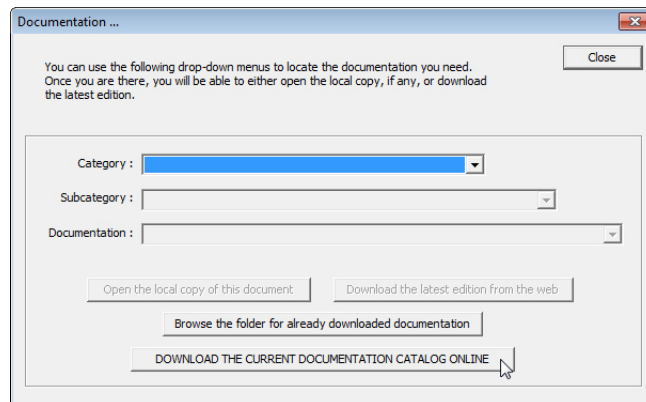
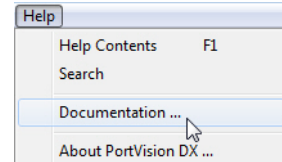
Accessing DeviceMaster LT Documentation from PortVision DX

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.

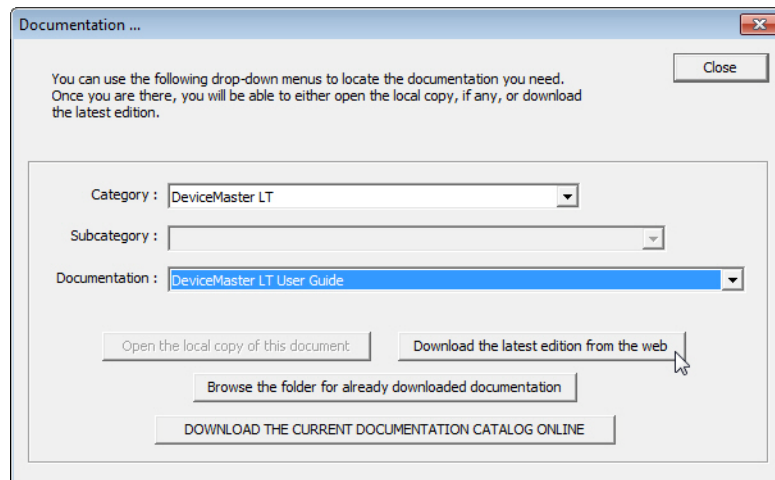
How to Download Documentation

Use this procedure to initially download a document or documents.

1. If necessary, open **PortVision DX > Start/Programs > Control > PortVision DX > 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.



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.



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

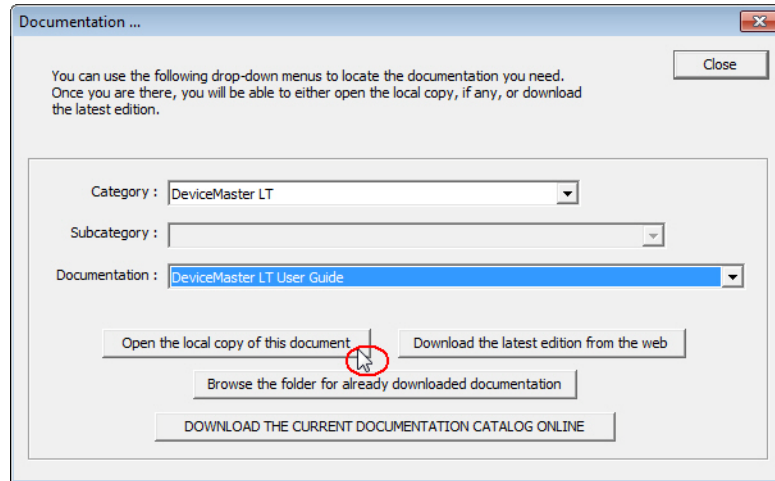
7. Click **Close** if you have downloaded all of the documents that you wanted.

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) > Control > PortVision DX > Docs** subdirectory and open the document.*

1. If necessary, open **PortVision DX > Start/Programs > Control > PortVision DX > 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.



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 30
- [Windows Installations](#) on Page 31

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 18).
- Checked to see if the latest version of SocketServer resides on the DeviceMaster LT ([Checking the SocketServer Version](#) on Page 22 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 24 or you can use RedBoot, [Uploading Firmware - Telnet Method \(Linux\)](#) on Page 104).

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 41).

Linux Installations

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

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

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

Before you install the Linux NS-Link device driver:

1. Make sure that you have programmed an appropriate network address into the DeviceMaster LT. If you do not want to install PortVision DX on a Windows system, you can use RedBoot, which is discussed in [Configuring the Network Settings](#) on Page 102.
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.

Note: Following images show the difference between SocketServer v9.xx and previous versions.

- b. Check the ftp site for the latest version: ftp://ftp.comtrol.com/dev_mstr/LT/software/SocketServer.

Server Status	Network	Security	EMail	RFC1006
Server Status				
	Software:		SocketServer 9.19	
	Host Name:		Static	
	IPv4 Config:		192.168.11.60	
	IPv4 Address:		255.255.0.0	
	IPv4 Netmask:		192.168.0.254	
	IPv4 Gateway:		Disabled	
	IPv6 Config:		ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/255	
IPv6 Address:		ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff		
IPv6 Gateway:				
Connection Status				
Port 1 Port 2 Port 3 Port 4 Port 5 Port 6 Port 7 Port 8 Port 9 Port 10 Port 11 Port 12				

- c. If necessary, download the latest version. If you do not want to use PortVision DX, use RedBoot to upload the latest version of SocketServer, which is discussed in [Uploading Firmware - Telnet Method \(Linux\)](#) on Page 104.

Note: Technical Supports recommends that you update to the latest version of

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 *Software and Documentation CD* or you can [download](#) the latest.

Supported Operating Systems

The NS-Link device driver for Windows supports:

- Windows 8
- Windows Server 2012
- Windows 7
- Windows Server 2008
- Windows Vista
- Windows Server 2003
- Window XP

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

Note: *Administrative privileges are required to install device drivers on Windows systems (excluding Windows Server 2003 and Windows XP).*

Installation Overview for Windows

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

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

NS-Link for Windows Installation

1. If necessary, locate the NS-Link device driver and make it available to the host system. The driver assembly is available on the *Software and Documentation CD* if you do not have internet access, or download the latest driver from:

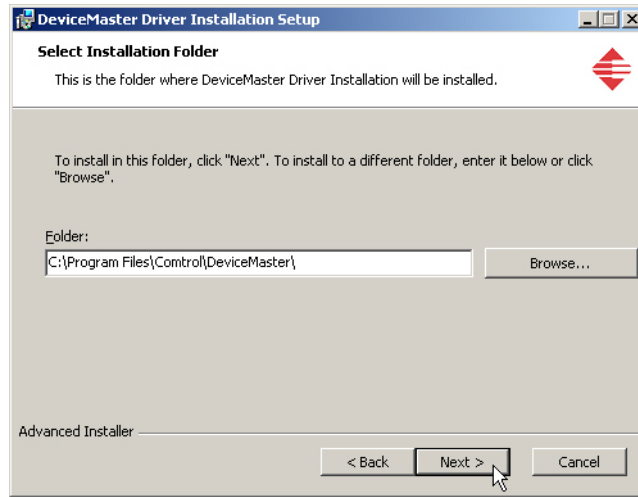
ftp://ftp.comtrol.com/dev_mstr/LT/drivers/win7.

Note: *Although the ftp link displays win7 in the path, the driver supports the previously listed [Windows operating systems](#).*

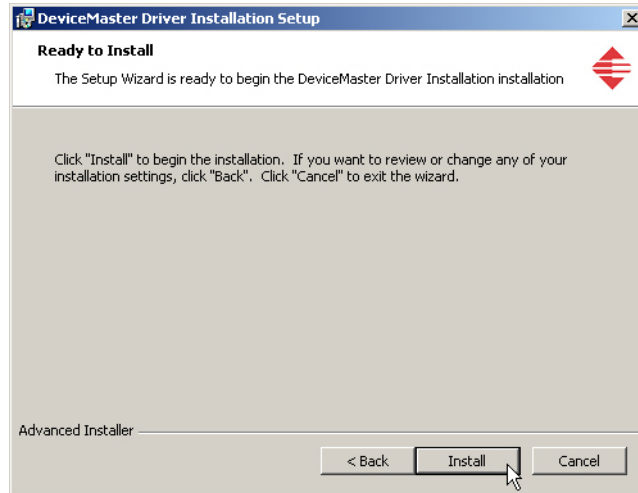
2. Execute the driver assembly `DeviceMaster_Windows_x.xx.exe` file and click **Next** to start the installation.



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



4. Click **Install**



5. Leave the **Launch DeviceMaster Driver Installation** box checked.
If you do not check this box, you can use the shortcut under the **Start** button at:
Programs > Control > DeviceMaster > DeviceMaster Driver Installation Wizard.
6. Click **Finish** to complete the installation of the wizard.



7. Click Next to start the driver installation.



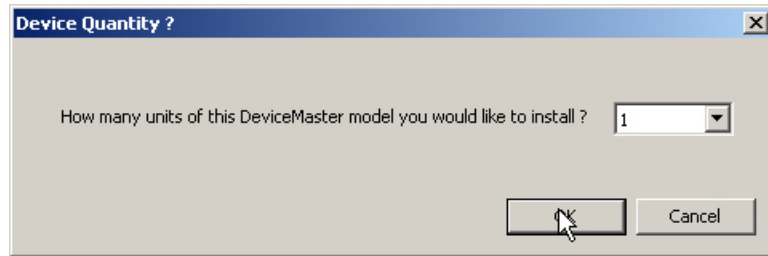
8. Click Install and Next.



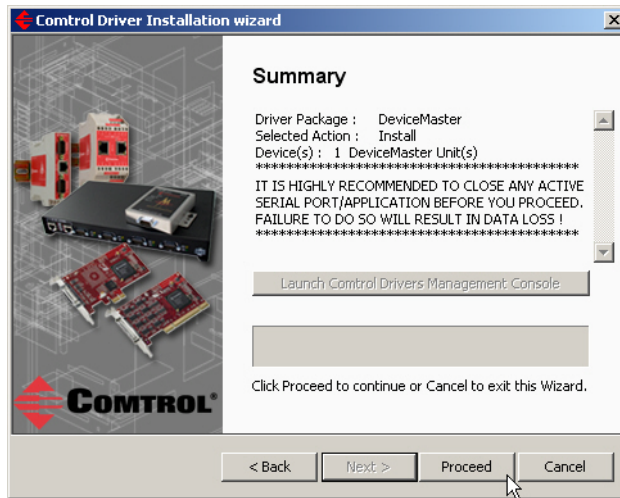
9. Select the DeviceMaster LT from the list.



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

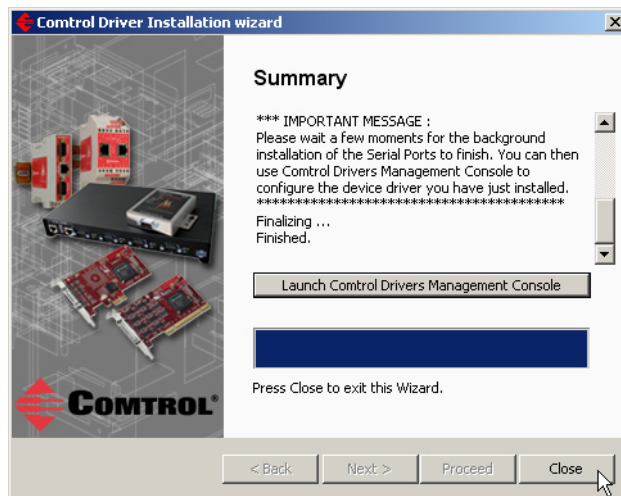


11. Repeat Steps 9 and 10 for each DeviceMaster LT that you are installing and click Next.
12. Click Proceed.



You may see the popup at the right for each port.

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



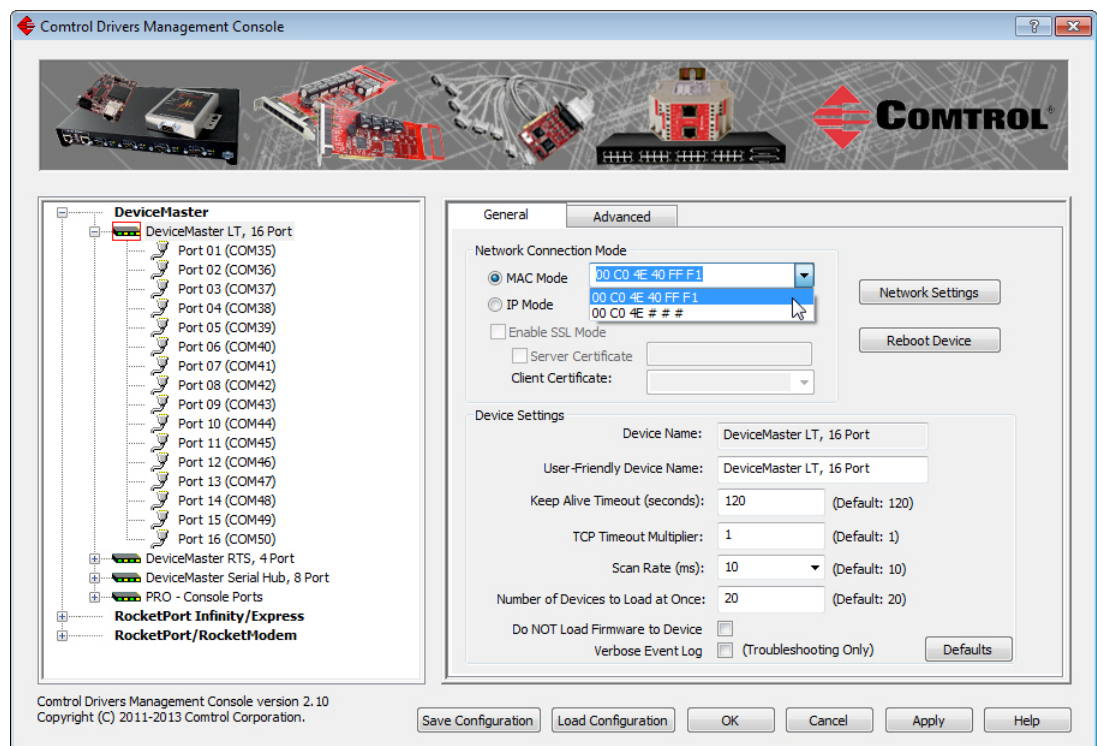
14. Go to the next subsection for NS-Link driver configuration procedures.

Configuring the NS-Link Driver for Windows

This subsection provides a configuration overview for the NS-Link driver. For detailed information or if the DeviceMaster LT is on a different physical segment, refer to the help system or the *DeviceMaster LT Device Driver (NS-Link) User Guide*, which is available on the *Software and Documentation CD* or you can [download the latest](#).

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 *Control Drivers Management Console* using the desktop shortcut or **Start > Programs > Control > DeviceMaster > 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.

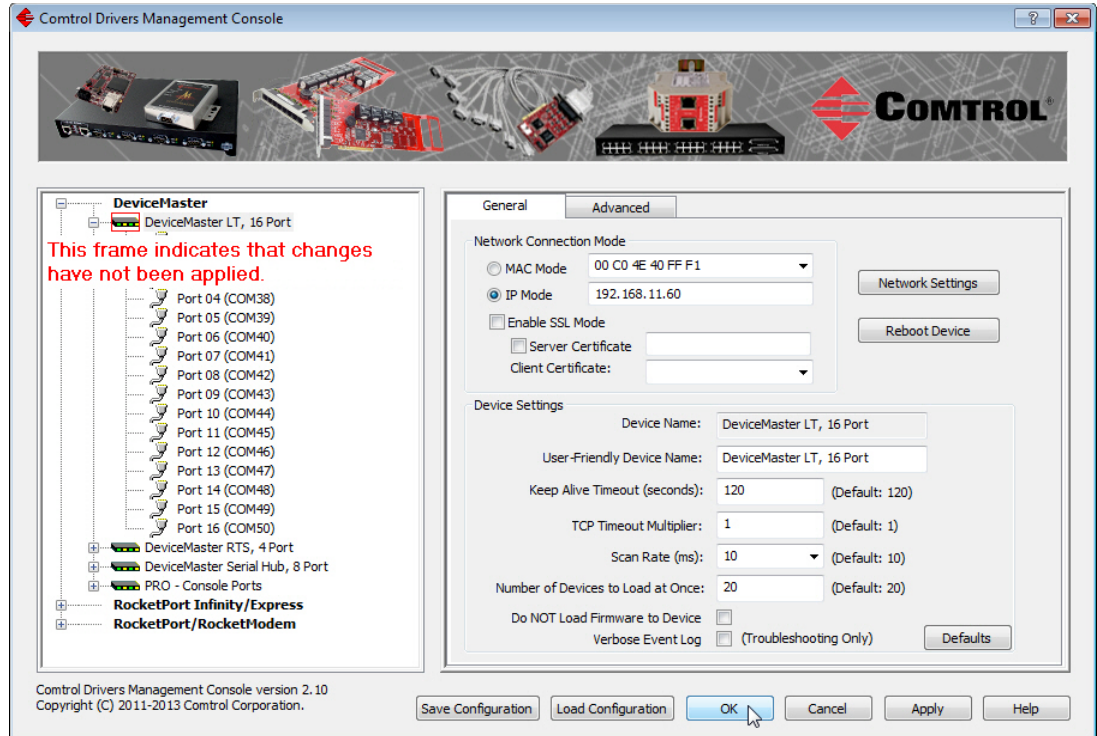
Note: If you enter the MAC address, make sure that you use the correct format: **00 C0 4E xx xx xx**. A space must separate each pair of digits. The MAC address is located on a label on the DeviceMaster LT or you can view it using PortVision DX.

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 *Control Drivers Management Console*.

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



5. Now that the MAC address has been associated to the DeviceMaster 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

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

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

6. Optionally, click **Enable SSL Mode** if you want to configure secure COM ports. The DeviceMaster LT must be configured using IP Mode 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 Control proprietary serial driver protocol are encrypted using SSL/TLS.
- Since SSL/TLS can not be used for either UDP data streams or for the

Control proprietary MAC mode Ethernet driver protocol, both UDP and MAC mode serial data transport features are disabled.

In 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.

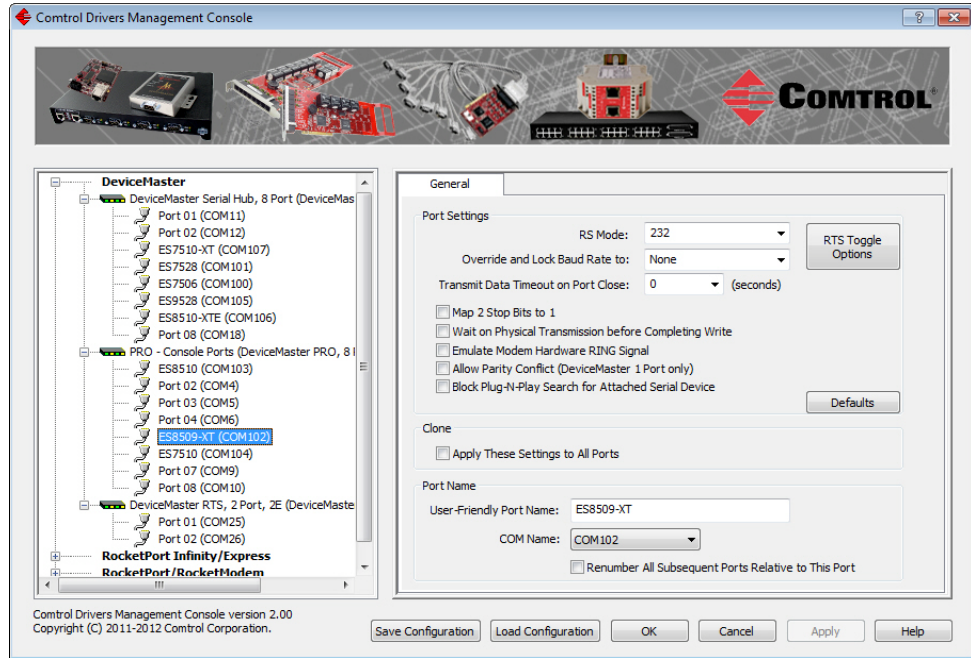
Note: See the help system or the [DeviceMaster NS-Link User Guide for Windows](#) if you need additional information on SSL and the corresponding options.

7. If you are using a server certificate, click the **Server Certificate** check box and enter the name in the **Server Certificate** text box.
 8. If you are using a client certificate, click the drop list and browse to the appropriate client certificate file.
 9. Configure the device properties:
 - a. If desired, change the **User-Friendly Device Name**.
 - b. Optionally, set a different **Keep Alive Timeout** period. You can set the amount of time in seconds that this DeviceMaster 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, change the **Number of Devices to Load at Once**.
 - f. If necessary, click **Do NOT Attempt to Load Firmware in Device**.
 - g. Optionally, click **Verbose Event Log** if you want to log additional DeviceMaster LT information into the event log.
 - h. After making your changes, click **Apply** if you have additional configuration procedures or click **Ok** if you have completed configuring your DeviceMaster 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*.
 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](#) (also available on the CD) or the NS-Link **Help** system for detailed configuration information.

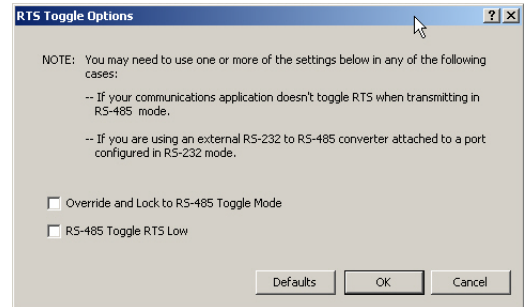
1. Highlight the first port you want to configure.



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

- a. Select the appropriate communications mode.
- b. Enable the features that you want to use.
- c. Optionally, click the **RTS Toggle Options** button:

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



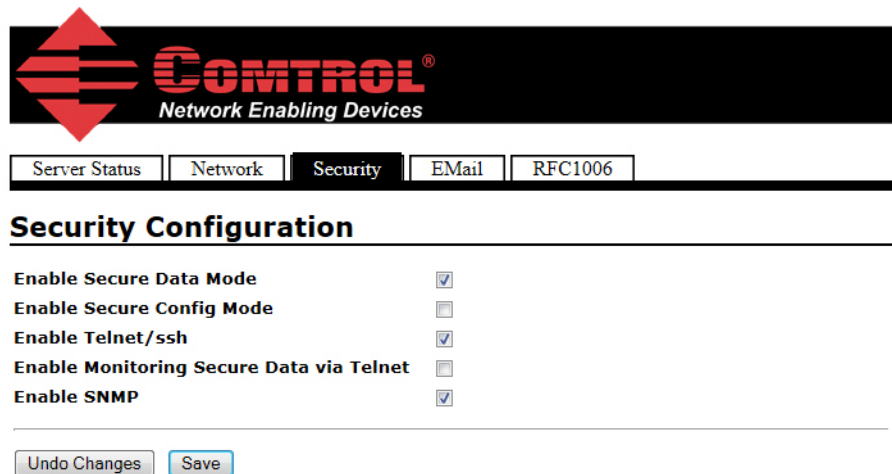
- d. Click the appropriate options for your environment.
 - e. Click **OK** to save the changes and return to the port **General** tab.
3. If desired, click the **Clone** check box to set all of the ports on this DeviceMaster LT to these characteristics.
 4. Optionally, change the **User-Friendly Port 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 43 to attach your serial device.
9. Optionally, you may need to configure one or more ports for socket mode ([Socket Port Configuration](#) on Page 41).

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 the **Security** tab.
3. Click **Enable Secure Data Mode** and **Save**.



4. Configure your security key and certificate and click **Set**.

Key and Certificate Management

RSA Key pair used by SSL and SSH servers	factory	Set	Delete
RSA Server Certificate used by SSL servers	factory	Set	Delete
DH Key pair used by SSL servers	factory	Set	Delete
Client Authentication Certificate used by SSL servers	none	Set	Delete

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 45.

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 Status*) provides access to configure.

- Socket port characteristics for:

- Serial
- TCP connection
- UDP connection

See [SocketServer Architecture](#) on Page 42 for more information about socket port support.

- Network settings (after initial configuration)
- [Security](#), which is discussed in detail starting on Page 45
- Email notification services
- RFC1006 (ISO over TCP)

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

Web Page Help System

The web page *Help* system is available separately for your convenience. The web page Help system contains detailed information and configuration procedures for each mode discussed in [SocketServer Architecture](#) on Page 42.

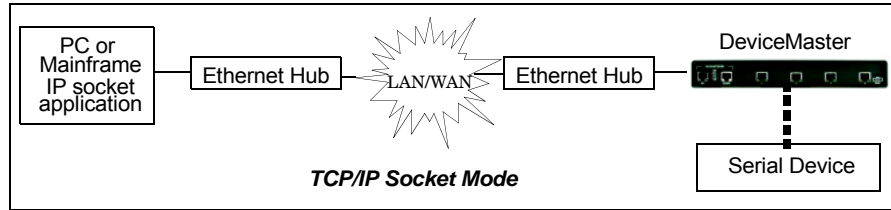
The *Help* system for the web page is available on the CD on the *Supporting Documents* page for your DeviceMaster LT or you can download the latest version from: ftp://ftp.control.com/dev_mstr/LT/software/socketserver/help/ssvr_help.zip.

To use the help system:

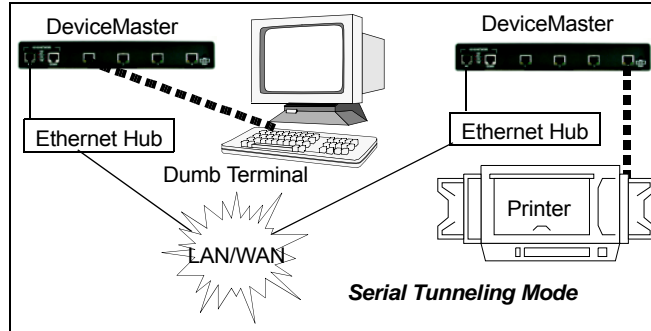
1. Unzip the files in a folder.
2. Open the **ssvr_help.htm** file.
3. Use your browser find function to locate the option or information for which are searching.

SocketServer Architecture

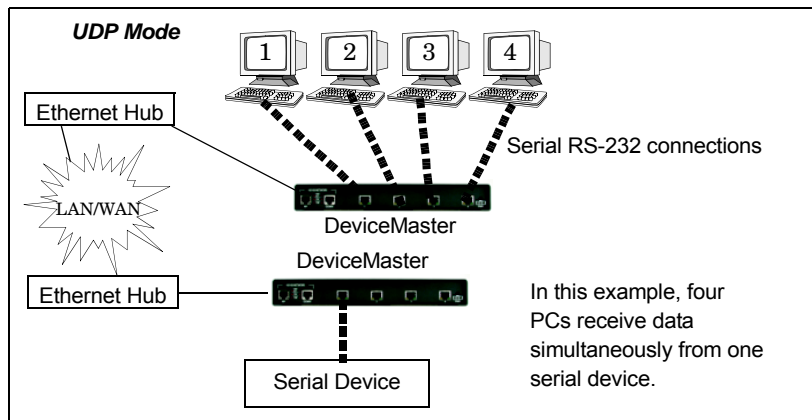
TCP/IP socket mode operation is used to connect serial devices with an application that supports TCP/IP socket communications addressing.



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.



Accessing Socket Configuration

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

- *Web Browser*
- *PortVision DX*

Web Browser

To access the socket configuration page for the DeviceMaster LT using a web browser, 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 the IP address in PortVision DX.
3. Click the port number that you want to configure socket port settings (serial, TCP connection configuration, and UDP connection configuration).
Note: See the web page Help system, if you need information about configuring sockets or serial tunneling. The Help system provides detailed configuration procedures and descriptions for all fields. See [Web Page Help System](#) on Page 41 for information about downloading the help file separately.
4. Click **Save** to return to the *Server Status* page.
5. Optionally, access the following pages to configure additional settings:
 - a. Click the **Network** tab to change the network settings.
 - b. Click the **Security** tab to enable DeviceMaster LT security.
 - c. Click the **Email** tab to configure email notification services.
 - d. Click the **RFC1006** tab to configure RFC1006 settings.

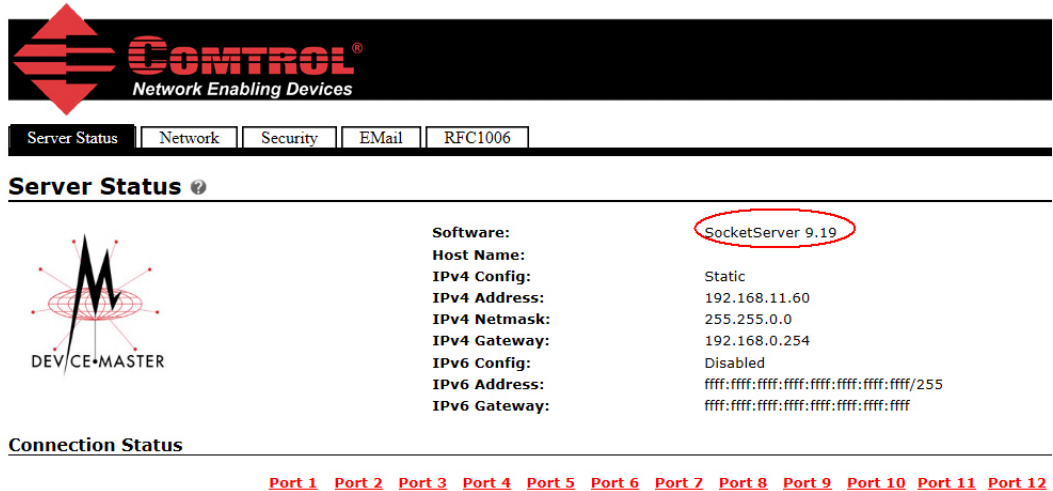
PortVision DX

There are several ways to access the socket configuration (NS-Link or SocketServer) 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. Click the port for which you want to configure socket port settings (serial, TCP connection configuration, and UDP connection configuration).
Note: For socket configuration information see the Help system. Click the ? in a configuration area for field specific information or the Help button at the bottom of the page to view page level help. To locate configuration procedures, scroll to the top of the Help file and view the Table of Contents.
3. Click **Save** to return to the *Server Status* (main) page.
4. Optionally, access the following pages to configure additional settings.
 - e. Click the **Network** tab to change the network settings.
 - f. Click the **Security** tab to enable DeviceMaster LT security.
 - g. Click the **Email** tab to configure email notification services.
 - h. Click the **RFC1006** tab to configure RFC1006 (ISO over TCP) settings.

SocketServer Versions

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

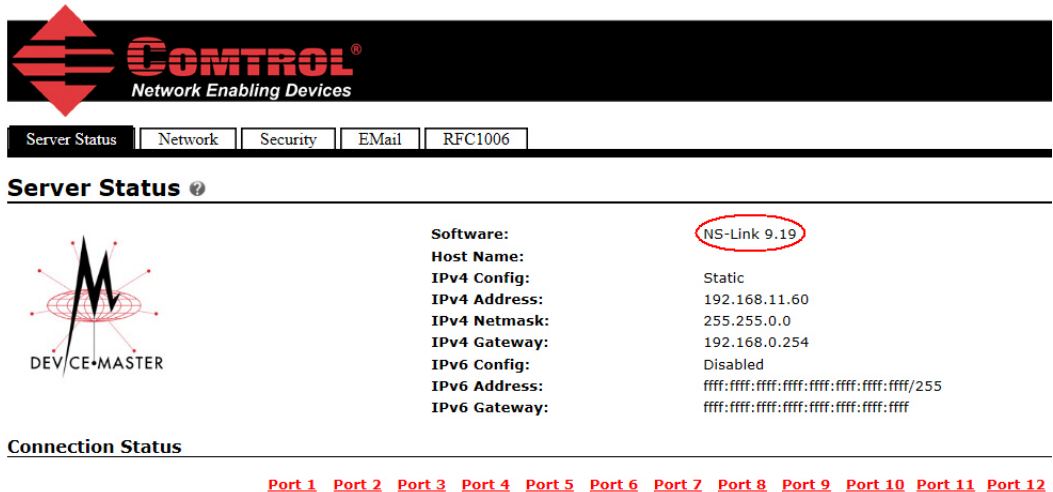


The screenshot shows the 'CONTROL Network Enabling Devices' header with navigation tabs for 'Server Status', 'Network', 'Security', 'EMail', and 'RFC1006'. The 'Server Status' section features a 'DEV/CE+MASTER' logo and a configuration table:

Software:	SocketServer 9.19
Host Name:	
IPv4 Config:	Static
IPv4 Address:	192.168.11.60
IPv4 Netmask:	255.255.0.0
IPv4 Gateway:	192.168.0.254
IPv6 Config:	Disabled
IPv6 Address:	ffff:ffff:ffff:ffff:ffff:ffff/255
IPv6 Gateway:	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Below the table is a 'Connection Status' section with a row of links: Port 1, Port 2, Port 3, Port 4, Port 5, Port 6, Port 7, Port 8, Port 9, Port 10, Port 11, Port 12.

Your SocketServer or NS-Link version may be different than these examples. The top illustration shows the web page before a NS-Link device driver installation and the bottom illustration shows the web page after a device driver installation.



The screenshot shows the 'CONTROL Network Enabling Devices' header with navigation tabs for 'Server Status', 'Network', 'Security', 'EMail', and 'RFC1006'. The 'Server Status' section features a 'DEV/CE+MASTER' logo and a configuration table:

Software:	NS-Link 9.19
Host Name:	
IPv4 Config:	Static
IPv4 Address:	192.168.11.60
IPv4 Netmask:	255.255.0.0
IPv4 Gateway:	192.168.0.254
IPv6 Config:	Disabled
IPv6 Address:	ffff:ffff:ffff:ffff:ffff:ffff/255
IPv6 Gateway:	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Below the table is a 'Connection Status' section with a row of links: Port 1, Port 2, Port 3, Port 4, Port 5, Port 6, Port 7, Port 8, Port 9, Port 10, Port 11, Port 12.

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 131 if you need to reset DeviceMaster LT security options. See [Returning the DeviceMaster LT to Factory Defaults](#) on Page 133 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) †	<p>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.</p> <p>This uploaded CA certificate that is used to validate a client's identity is sometimes referred to as a <i>trusted root certificate</i>, a <i>trusted authority certificate</i>, or a <i>trusted CA certificate</i>. This CA certificate might be that of a trusted commercial certificate authority or it may be a privately generated certificate that an organization creates internally to provide a mechanism to control access to resources that are protected by the SSL/TLS protocols.</p> <p>See Key and Certificate Management on Page 61 for more information. This section does not discuss the creation of CA Certificates.</p>
Client Authentication	<p>A process using paired keys and identity certificates to prevent unauthorized access to the DeviceMaster LT. Client authentication is discussed in Client Authentication on Page 54 and Changing Keys and Certificates on Page 64.</p>
DH Key Pair Used by SSL Servers ‡	<p>This is a private/public key pair that is used by some cipher suites to encrypt the SSL/TLS handshaking messages. Possession of the private portion of the key pair allows an eavesdropper to decrypt traffic on SSL/TLS connections that use DH encryption during handshaking.</p> <p>The DH (Diffie-Hellman) key exchange, also called exponential key exchange, is a method of digital encryption that uses numbers raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted, making the task of a would-be code breaker mathematically overwhelming.</p> <p>The most serious limitation of Diffie-Hellman (DH key) in its basic or <i>pure</i> form is the lack of authentication. Communications using Diffie-Hellman all by itself are vulnerable to man in the middle attacks. Ideally, Diffie-Hellman should be used in conjunction with a recognized authentication method such as digital signatures to verify the identities of the users over the public communications medium.</p> <p>See Certificates and Keys on Page 54 and Key and Certificate Management on Page 61 for more information.</p>
<p>† All DeviceMaster LT units are shipped from the factory with identical configurations. They all have the identical, self-signed, Control Server RSA Certificates, Server RSA Keys, Server DH Keys, and no Client Authentication Certificates. For maximum data and access security, you should configure all DeviceMaster LT units with custom certificates and keys.</p>	

Term or Issue	Explanation
Digital Certificate	<p>A digital certificate is an electronic <i>credit card</i> that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys.</p> <p>See Key and Certificate Management on Page 61 for more information.</p>
PKI (public key infrastructure)	<p>A public key infrastructure (PKI) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on.</p> <p>The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message. Traditional cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This secret or private key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the public key infrastructure is the preferred approach on the Internet. (The private key system is sometimes known as symmetric cryptography and the public key system as asymmetric cryptography.)</p> <p>A public key infrastructure consists of:</p> <ul style="list-style-type: none"> • A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key • A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor • One or more directories where the certificates (with their public keys) are held • A certificate management system <p>For more information, see SSL Authentication on Page 53, SSL Performance on Page 56, SSL Cipher Suites on Page 56, and DeviceMaster LT Supported Cipher Suites on Page 57.</p>

Term or Issue	Explanation
RSA Key Pair†	<p>This is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption. RSA is widely used in electronic commerce protocols, and is believed to be sufficiently secure given sufficiently long keys and the use of up-to-date implementations. The system includes a communications channel coupled to at least one terminal having an encoding device, and to at least one terminal having a decoding device.</p> <ul style="list-style-type: none"> • Public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures. • Private Key <ul style="list-style-type: none"> - One half of the <i>key pair</i> used in conjunction with a public key - Both the public and the private keys are needed for encryption / decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet. - The private key is used to decrypt text that has been encrypted with the public key. <p>Thus, if <i>User A</i> sends <i>User B</i> a message, <i>User A</i> can find out <i>User B's</i> public key (but not <i>User B's</i> private key) from a central administrator and encrypt a message to <i>User B</i> using <i>User B's</i> public key. When <i>User B</i> receives it, <i>User B</i> decrypts it with <i>User B's</i> private key. In addition to encrypting messages (which ensures privacy), <i>User B</i> can authenticate <i>User B</i> to <i>User A</i> (so that <i>User A</i> knows that it is really <i>User B</i> who sent the message) by using <i>User B's</i> private key to encrypt a digital certificate.</p> <p>See Key and Certificate Management on Page 61 for more information.</p>
SSH (Secure Shell)	<p>Secure Shell (SSH) allows data to be exchanged using a secure channel between two networked devices. Replaces telnet which has no security. SSH requires password authentication – even if password is empty.</p> <p>See SSH Server on Page 53 for more information.</p>
SSL (Secure Sockets Layer)	<p>The Secure Sockets Layer (SSL) is the predecessor of (TLS) Transport Layer Security.</p> <p>SSL is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers.</p> <p>SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security.</p> <p>SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.</p> <p>See Pages 53 through 57 for detailed information about SSL.</p> <p>Note: <i>Two slightly different SSL protocols are supported by the DeviceMaster LT: SSLv3 and TLSv1.</i></p>

Term or Issue	Explanation
<p>TLS (Transport Layer Security)</p>	<p>Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).</p> <p>TLS and SSL are not interoperable. The TLS protocol does contain a mechanism that allows TLS implementation to back down to SSL 3.0.</p>
<p>Secure Data Mode</p>	<p>TCP connections that carry data to/from the DeviceMaster LT serial ports are encrypted using SSL or TLS security protocols. See Security Modes on Page 51 and Configure/Enable Security Features Overview on Page 58 for more information.</p>
<p>Secure Config Mode</p>	<p>Unencrypted access to administrative and diagnostic functions are disabled. See Security Modes on Page 51 and Configure/Enable Security Features Overview on Page 58 for more information.</p>
<p>Secure Monitor Data Mode via Telnet</p>	<p>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 59.</p>
<p><i>Man in the Middle attack</i></p>	<p>A man in the middle attack is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other.</p> <p>The attack gets its name from the ball game where two people try to throw a ball directly to each other while one person in between them attempts to catch it. In a man in the middle attack, the intruder uses a program that appears to be the server to the client and appears to be the client to the server. The attack may be used simply to gain access to the message, or enable the attacker to modify the message before retransmitting it.</p>
<p><i>How Public and Private Key Cryptography Works</i></p>	<p>In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority (CA).</p> <p>The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access.</p> <p>The private key is never shared with anyone or sent across the Internet. You use the private key to decrypt text that has been encrypted with your public key by someone else (who can find out what your public key is from a public directory).</p> <p>Thus, if <i>User A</i> sends <i>User B</i> a message, <i>User A</i> can find out <i>User B's</i> public key (but not <i>User B's</i> private key) from a central administrator and encrypt a message to <i>User B</i> using <i>User B's</i> public key. When <i>User B</i> receives it, <i>User B</i> decrypts it with <i>User B's</i> private key. In addition to encrypting messages (which ensures privacy), <i>User B</i> can authenticate <i>User B</i> to <i>User A</i> (so <i>User A</i> knows that it is really <i>User B</i> who sent the message) by using <i>User B's</i> private key to encrypt a digital certificate. When <i>User A</i> receives it, <i>User A</i> can use <i>User B's</i> public key to decrypt it.</p>

Term or Issue	Explanation
<i>Who Provides the Infrastructure?</i>	<p>A number of products are offered that enable a company or group of companies to implement a PKI. The acceleration of e-commerce and business-to-business commerce over the Internet has increased the demand for PKI solutions. Related ideas are the virtual private network (VPN) and the IP Security (IPsec) standard. Among PKI leaders are:</p> <ul style="list-style-type: none"> • RSA, which has developed the main algorithms used by PKI vendors. • Verisign, which acts as a certificate authority and sells software that allows a company to create its own certificate authorities. • GTE CyberTrust, which provides a PKI implementation methodology and consultation service that it plans to vend to other companies for a fixed price. • Xcert, whose Web Sentry product that checks the revocation status of certificates on a server, using the Online Certificate Status Protocol (OCSP). • Netscape, whose Directory Server product is said to support 50 million objects and process 5,000 queries a second; Secure E-Commerce, which allows a company or extranet manager to manage digital certificates; and Meta-Directory, which can connect all corporate directories into a single directory for security management.
<p>The following topic references are from: http://searchsecurity.techtarget.com/</p> <ul style="list-style-type: none"> • PKI (public key infrastructure) • How Public/Private Key Cryptography Works • Who Provides the Infrastructure • Digital Certificate • DH Key • Man in the Middle attack <p>The RSA Key pair topic reference is from: http://en.wikipedia.org/wiki/RSA</p>	

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: <ul style="list-style-type: none"> • Requires SSL encryption of TCP connections to SocketServer (Ports 8000, 8001, 8002, and so forth). • Disables UDP access to SocketServer. • Disables RFC1006 (ISO-over-TCP) access to SocketServer. • Disables MAC-mode access to serial ports. MAC mode admin and ID commands are still allowed. • Requires SSL encryption of NS-Link TCP connections (Port 4606). Not directly supported by NS-Link drivers for Windows and Linux. The Linux driver has been tested using stunnel, but manual setup is required. • Requires SSH instead of telnet connection to the diagnostic log (TCP Port 4607). • Two values for http READ and WRITE commands: A2: Enable.
Secure Config	Encrypts/authenticates configuration and administration operations (web server, IP settings, load SW, and so forth.). Secure Config mode: <ul style="list-style-type: none"> • Disables MAC mode admin commands except for ID request†. • Disables TCP/IP admin commands except for ID request†. • Disables telnet console access (Port 23)†. • Disables unencrypted http:// access via Port 80. • Disables e-mail notification and SNMP features. • Two values for http READ and WRITE commands: A3: Enable.
† Affects both RedBoot and SocketServer / NS-Link applications.	

Secure Data Mode and Secure Config Mode Comparison

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

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.

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

	Weakest			Strongest		
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 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.
- Two slightly different SSL protocols are supported by the DeviceMaster LT, SSLv3 and TLSv1.
- 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 also significant. The time required to open a connection to SocketServer varies depending on the public-key encryption scheme used for the initial handshaking. Typical setup times for the three public-key encryption schemes supported by the DeviceMaster LT are shown below:
 - RSA 0.66 seconds
 - DHE 3.84 seconds
 - DHA 3.28 seconds
- Since there is a certain amount of overhead for each block of data sent/received on an SSL connection, the SocketServer polling rate and size of blocks that are written to the SocketServer also has a noticeable effect on CPU usage. Writing larger blocks of data and a slower SocketServer polling rate will decrease CPU usage and allow somewhat higher throughputs.

SSL Cipher Suites

This subsection provides information about SSL cipher suites.

- An SSL connection uses four different facilities, each of which can use one of several different ciphers or algorithms. A particular combination of four ciphers/algorithms is called a “cipher suite”.
- A Cipher Suite consists of
 - Public Key Encryption Algorithm
 - Used to protect the initial handshaking and connection setup.
 - Typical options are RSA, DH, DHA, DHE, EDH, SRP, PSK
 - DeviceMaster 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
 - 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
 - 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
 - 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 attached 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:

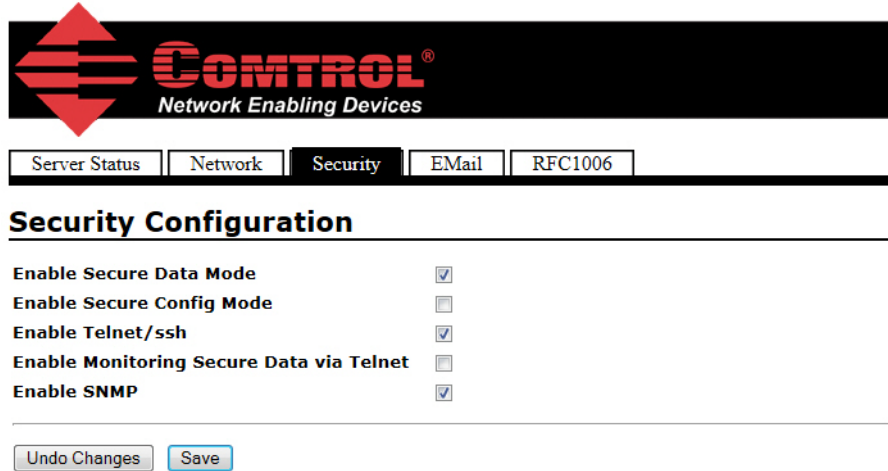
- Standard reference book is SSL and TLS by Eric Rescorla
- Wikipedia page on SSL/TLS provides a good overview: <http://en.wikipedia.org/wiki/TLS>
- **openssl** contains command-line tools to do the following. More information is available at: <http://www.openssl.org/>
 - Create/examine keys/certificates
 - 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 29.

The following illustration shows the *Security Configuration* area of the **Security** tab and are discussed in the following table.



Security Option	Description
Enable Secure Data Mode	<p>If Secure Data Mode is enabled TCP connections which carry data to/from the serial ports will be encrypted using SSL or TLS security protocols. This includes the following:</p> <ul style="list-style-type: none"> • TCP connections to the per-serial-port TCP ports (default is 8000, 8001, 8002, and so forth) are encrypted using SSL/TLS. • TCP connections to TCP Port 4606 on which the DeviceMaster LT implements the Control proprietary serial driver protocol are encrypted using SSL/TLS. • Since SSL/TLS can not be used for either UDP data streams or for the Control proprietary MAC mode Ethernet driver protocol, both UDP and MAC mode serial data transport features are disabled. • In order to minimize possible security problems, e-mail and RFC1006 features are also disabled in <i>Secure Data</i> mode. <p>In addition to encrypting the data streams, it is possible to configure the DeviceMaster LT so that only authorized client applications can connect using SSL/TLS. See the Client Authentication discussion on Page 54 for details.</p>

Security Option	Description
<p>Enable Secure Config Mode</p>	<p>If Secure Config Mode is enabled, unencrypted access to administrative and diagnostic functions is disabled. Secure Config Mode changes DeviceMaster LT behavior as follows:</p> <ul style="list-style-type: none"> • Telnet access to administrative and diagnostic functions is disabled. SSH access is still allowed. • Unencrypted access to the web server via Port 80 (http:// URLs) is disabled. • Encrypted access to the web server via Port 443 (https:// URLs) is still allowed. • Administrative commands that change configuration or operating state which are received using the 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.
<p>Enable Monitoring Secure Data via Telnet</p>	<p>When checked, this allows the monitor command to be used while Secure Data Mode is enabled. When unchecked, the monitor command can only be used if Secure Data Mode is not enabled. You must click Save and reboot the DeviceMaster LT for the change to go into affect. This option is disabled by default.</p> <p>The Enable Monitoring Secure Data via Telnet feature allows you to monitor serial data being sent/received on a serial port (either via NS-Link or SocketServer). The monitoring is done by telnetting to the DeviceMaster LT and using the following commands:</p> <ul style="list-style-type: none"> • 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 60 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 60. - 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 61. <p><i>(continued)</i></p>

Security Option	Description
<p><i>(Continued from the previous page)</i></p> <p>Enable Monitoring Secure Data via Telnet</p>	<ul style="list-style-type: none"> securemon [enable disable] <p>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.</p> <p>Currently, because of issues with the DeviceMaster LT ssh implementation, monitoring serial port data via the ssh command-line interface is not supported. It is expected that it will be supported in the future. Once it is supported, the securemon setting will not affect the ability to monitor secure data via ssh (which will always be allowed).</p>
Enable Telnet/ssh	This option enables or disables the telnet security feature after you click Save and the DeviceMaster LT has been rebooted. <i>This option is enabled by default.</i>
Enable SNMP	This option enables or disables the SNMP security feature after you click Save and the DeviceMaster LT has been rebooted. <i>This option is enabled by default.</i>

Example 1

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

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

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 *Edit Security Configuration* web page.

Key and Certificate Management

RSA Key pair used by SSL and SSH servers	factory	<input type="button" value="Set"/>	<input type="button" value="Delete"/>
RSA Server Certificate used by SSL servers	factory	<input type="button" value="Set"/>	<input type="button" value="Delete"/>
DH Key pair used by SSL servers	factory	<input type="button" value="Set"/>	<input type="button" value="Delete"/>
Client Authentication Certificate used by SSL servers	none	<input type="button" value="Set"/>	<input type="button" value="Delete"/>

Key and Certificate Management Options	Description
<p>RSA Key pair used by SSL and SSH servers</p>	<p>This is a private/public key pair that is used for two purposes:</p> <p>It is used by some cipher suites to encrypt the SSL/TLS handshaking messages. Possession of the private portion of this key pair allows an eavesdropper to both decrypt traffic on SSL/TLS connections that use RSA encryption during handshaking.</p> <p>It is used to sign the Server RSA Certificate in order to verify that the &dm; is authorized to use the server RSA identity certificate. Possession of the private portion of this key pair allows somebody to pose as the &dm;.</p> <p>If the Server RSA Key is to be replaced, a corresponding RSA identity certificate must also be generated and uploaded or clients are not able to verify the identity certificate.</p>
<p>RSA Server Certificate used by SSL servers</p>	<p>This is the RSA identity certificate that the DeviceMaster uses during SSL/TLS handshaking to identify itself. It is used most frequently by SSL server code in the DeviceMaster when clients open connections to the DeviceMaster's secure web server or other secure TCP ports. If a DeviceMaster serial port configuration is set up to open (as a client) a TCP connection to another server device, the DeviceMaster also uses this certificate to identify itself as an SSL client if requested by the server.</p> <p>In order to function properly, this certificate must be signed using the Server RSA Key. This means that the server RSA certificate and server RSA key must be replaced as a pair.</p>
<p>DH Key pair used by SSL servers</p>	<p>This is a private/public key pair that is used by some cipher suites to encrypt the SSL/TLS handshaking messages.</p> <p>Note: <i>Possession of the private portion of the key pair allows an eavesdropper to decrypt traffic on SSL/TLS connections that use DH encryption during handshaking.</i></p>
<p>Client Authentication Certificate used by SSL servers</p>	<p>If configured with a CA certificate, the DeviceMaster requires all SSL/TLS clients to present an RSA identity certificate that has been signed by the configured CA certificate. As shipped, the DeviceMaster is not configured with a CA certificate and all SSL/TLS clients are allowed.</p> <p>See Client Authentication on Page 54 for more detailed information</p>
<ul style="list-style-type: none"> • <i>All DeviceMaster LT units are shipped from the factory with identical configurations. They all have the identical, self-signed, Control Server RSA Certificates, Server RSA Keys, Server DH Keys, and no Client Authentication Certificates.</i> • <i>For maximum data and access security, you should configure all DeviceMaster LT units with custom certificates and keys.</i> 	

Using a Web Browser to Set Security Features

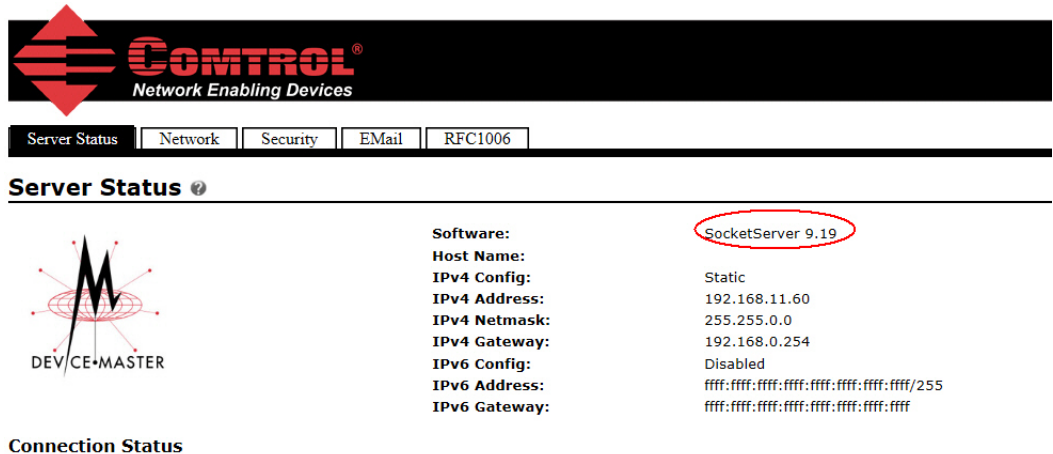
The following procedures are discussed below:

- [Changing Security Configuration](#)
- [Changing Keys and Certificates](#) on Page 64

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.



CONTROL
Network Enabling Devices

Server Status | Network | Security | EMail | RFC1006

Server Status

 DEV/CE+MASTER	Software:	SocketServer 9.19
	Host Name:	
	IPv4 Config:	Static
	IPv4 Address:	192.168.11.60
	IPv4 Netmask:	255.255.0.0
	IPv4 Gateway:	192.168.0.254
	IPv6 Config:	Disabled
IPv6 Address:	ffff:ffff:ffff:ffff:ffff:ffff:ffff:255	
IPv6 Gateway:	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	

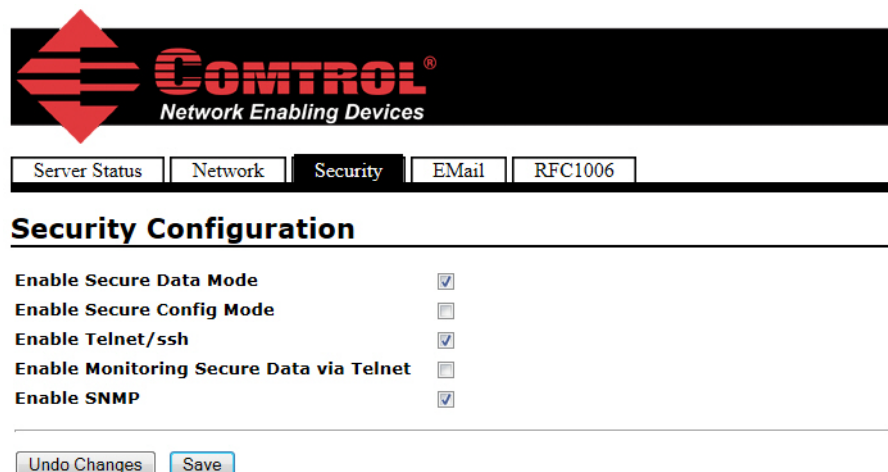
Connection Status

Port 1 Port 2 Port 3 Port 4 Port 5 Port 6 Port 7 Port 8 Port 9 Port 10 Port 11 Port 12

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

2. Click the **Security** tab.
3. Click the appropriate check boxes in the *Security Configuration* area to enable or disable security accordingly.

Refer to the help system or [Configure/Enable Security Features Overview](#) on Page 58 for detailed information.



CONTROL
Network Enabling Devices

Server Status | Network | Security | EMail | RFC1006

Security Configuration

Enable Secure Data Mode	<input checked="" type="checkbox"/>
Enable Secure Config Mode	<input type="checkbox"/>
Enable Telnet/ssh	<input checked="" type="checkbox"/>
Enable Monitoring Secure Data via Telnet	<input type="checkbox"/>
Enable SNMP	<input checked="" type="checkbox"/>

Undo Changes Save

4. After making changes to the *Security Configuration* area, click **Save**.

5. Make the appropriate selection for your situation:
 - Click **Continue**, if you addition configuration and then make sure that you reboot the DeviceMaster LT later so that the changes take affect.
 - Click **Reboot** so that changes take affect as soon as the DeviceMaster LT returns online.



Changing Keys and Certificates

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

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

Refer to the help system or [Key and Certificate Management](#) subsection on Page 64 for detailed information.

Key and Certificate Management

RSA Key pair used by SSL and SSH servers	factory	<input type="button" value="Set"/>	<input type="button" value="Delete"/>
RSA Server Certificate used by SSL servers	factory	<input type="button" value="Set"/>	<input type="button" value="Delete"/>
DH Key pair used by SSL servers	factory	<input type="button" value="Set"/>	<input type="button" value="Delete"/>
Client Authentication Certificate used by SSL servers	none	<input type="button" value="Set"/>	<input type="button" value="Delete"/>

4. Click **Browse** to locate the key or certificate file, highlight the file, and click **Open**.
5. Click **Upload** when you return to the *Key and Certificate Management* area. The key or certificate notation changes from *factory* or *none* to **User** when the DeviceMaster LT is secure.
6. You do not need to click **Save**, but changes will not take effect until the DeviceMaster LT is rebooted.
You can reboot the DeviceMaster LT by returning to the *Server Status* tab (scroll to the bottom of the page) or using PortVision DX.

Connecting Serial Devices

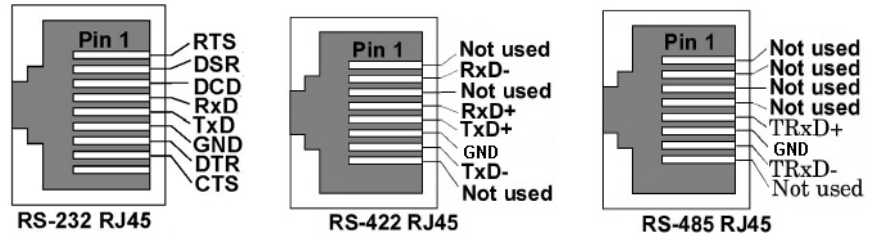
This section discusses connecting your serial devices to the DeviceMaster LT. It also provides you with information to build serial cables and loopback connectors to test the serial ports.

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 66
- [RJ45 Null-Modem Cables \(RS-422\)](#) on Page 66
- [RJ45 Straight-Through Cables \(RS-232/485\)](#) on Page 66
- [RJ45 Loopback Plugs](#) on Page 67
- [RJ45 RS-485 Test Cable](#) on Page 67
- [Connecting RJ45 Devices](#) on Page 67

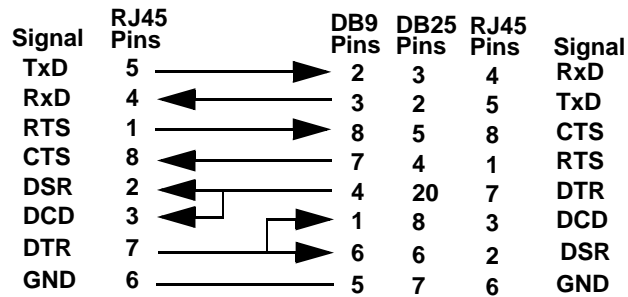
You can build your own null-modem or straight-through RJ45 serial cables if you are using the DB9 to RJ45 adapters using the following subsections.



Pin	RS-232	RS-422	RS-485
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)

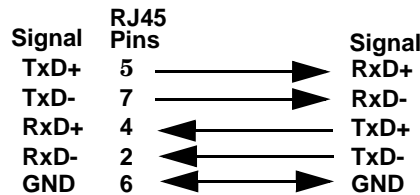
Use the following figure if you need to build an RS-232 null-modem cable. A null-modem cable is required for connecting DTE devices.



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

RJ45 Null-Modem Cables (RS-422)

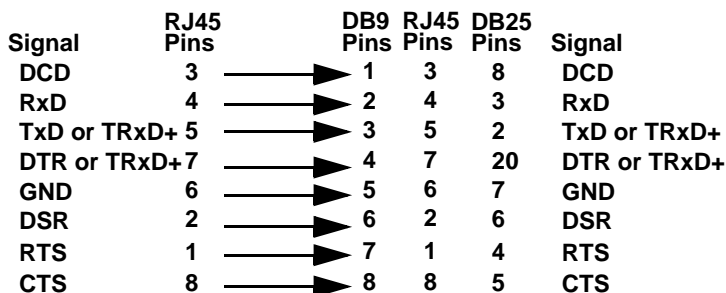
Use the following figure if you need to build an RS-422 null-modem RJ45 cable. A null-modem cable is required for connecting DTE devices.



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

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

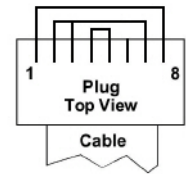
Use the following figure if you need to build an RS-232 or RS-485 straight-through cable. Straight-through cables are used to connect modems and other DCE devices. For example, a straight-through cable can be used to connect COM2 of one PC to COM2 to a modem.



RJ45 Loopback Plugs

Loopback connectors are RJ45 serial port plugs with pins wired together that are used in conjunction with application software (Test Terminal 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).

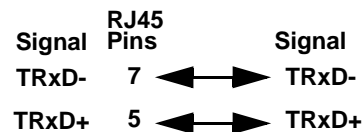
- Pins 4 to 5
- Pins 1 to 8
- Pins 2 to 3 to 7



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

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.

Connecting RJ45 Devices

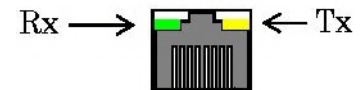
You can use this information to connect serial devices to RJ45 connectors.

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 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
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 129 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](#)
- [Updating Firmware Across WANs \(Windows\)](#) on Page 70
- [Uploading SocketServer to Multiple DeviceMaster LTs](#) on Page 74
- [Configuring Multiple DeviceMaster LTs Network Addresses](#) on Page 75
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 75
- [Using SocketServer Configuration Files](#) on Page 77
- [Using Driver Configuration Files](#) on Page 79
- [Changing the Bootloader Timeout](#) on Page 84, which discusses changing the Bootloader timeout
- [Managing Bootloader](#) on Page 85, which also discusses checking the Bootloader version and downloading the latest Bootloader
- [Checking the NS-Link Version](#) on Page 87
- [Accessing SocketServer Commands in Telnet/SSH Sessions \(PortVision DX\)](#) on Page 90
Note: You can optionally refer to [RedBoot Procedures](#) on Page 99 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 <i>Device List</i> 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	<i>Main page (Server Status):</i> Scroll to the bottom of the page, click Reboot and then Yes: Reboot .
Telnet	Type reset .
DeviceMaster LT	DeviceMaster LT has a Reset/Restore switch. <ul style="list-style-type: none">• If the Reset/Restore switch is depressed for less than 2 seconds, the DeviceMaster LT reboots.• If the Reset/Restore switch is depressed for greater than approximately 5 seconds it restores the DeviceMaster LT to the factory default values.

Optionally, you can power cycle the DeviceMaster LT.

Updating Firmware Across WANs (Windows)

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

This procedure is also recommended in cases where SocketServer fails to load using convention methods.

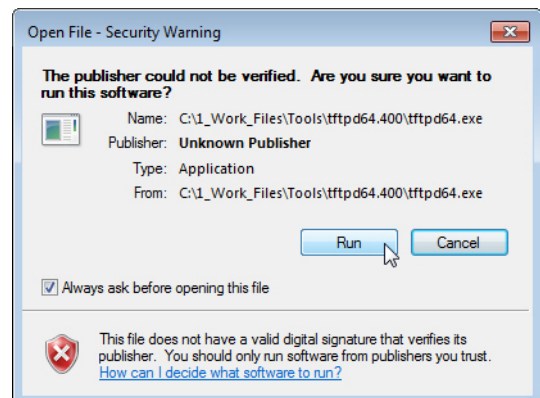
1. If you do not have a TFTP server, you can download the appropriate one for your Windows operating system from the Control ftp site.

ftp://ftp.comtrol.com/contribs/utilities/3rd_party_utils_free/tftp_server

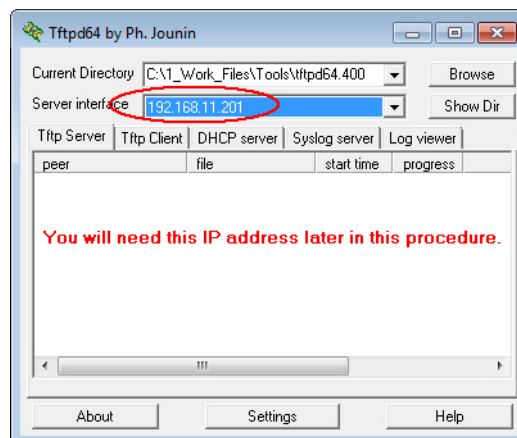


Note: Depending on your Windows operating system, you may need to respond to a Security Warning popup.

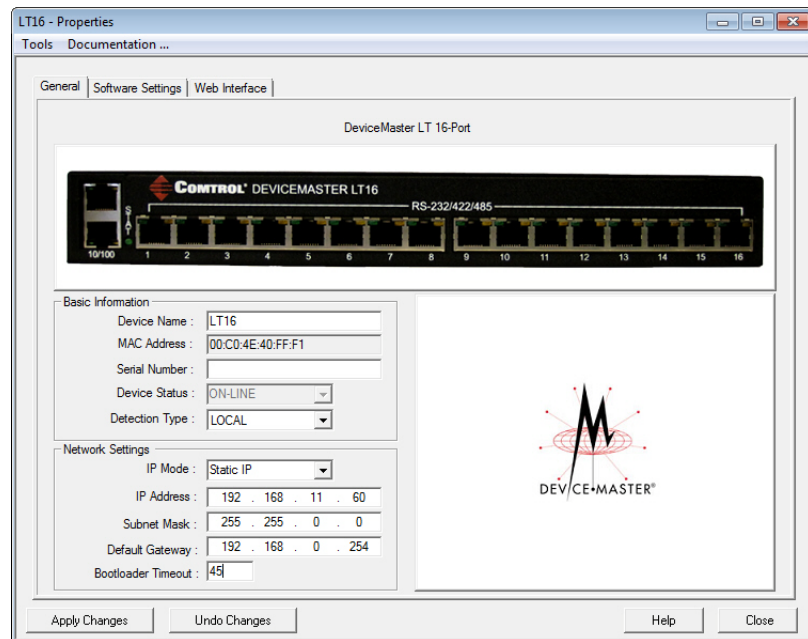
- a. Unzip the tftp server that you downloaded to your host system in a location that you can easily find.
- b. Execute the **tftp.64.exe** (or **tftp32.exe**) file.
- c. Click **Run**.
- d. Depending on your operating system, you may need to click **Unblock**, if you receive a *Windows Security Alert* popup.



The **Tftpd** application opens:

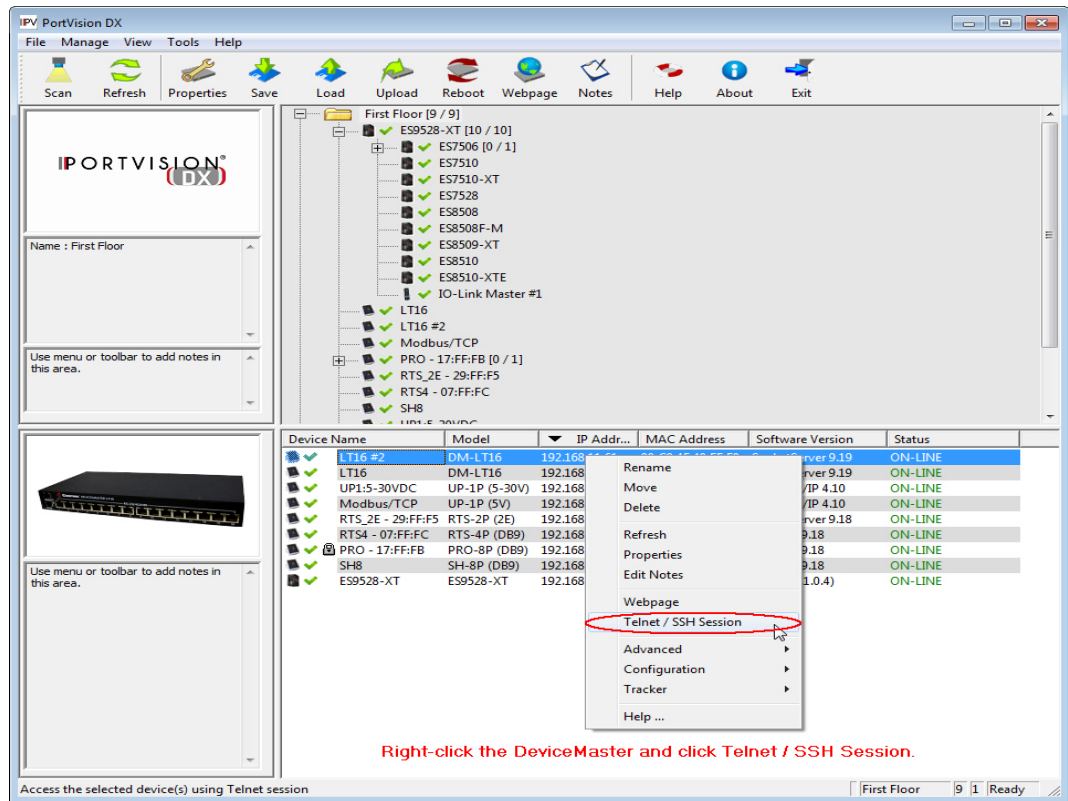


2. Make sure that you have downloaded the latest SocketServer version from: ftp://ftp.control.com/dev_mstr/LT/software/socketserver.
You may want to place SocketServer in the same directory as the Tftpd server.
3. Optionally, rename the **SocketServer-x.xx.bin** file (where x.xx is the version number) to **1.bin** to make the following steps easier.
4. If necessary, open PortVision DX: **Start >Program > Control > PortVision DX > PortVision DX** or the desktop shortcut.
5. Change the Bootloader Timeout value to 60 seconds.
 - a. Right-click the DeviceMaster LT in the *Device List* pane for which you want to upload the latest SocketServer and click **Properties**.
 - b. Change the **Bootloader Timeout** value to 60, click **Apply Changes**, and then **Close**.

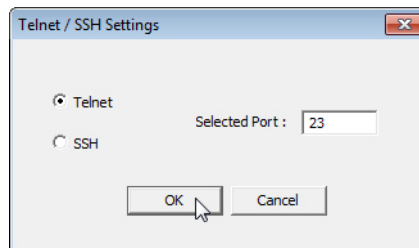


Note: If the PuTTY screen flashes in the background and does not appear as shown above, make sure that **Enable Telnet/ssh** has not been disabled in SocketServer. To check this, return to PortVision DX, right-click the DeviceMaster LT in the Device List pane, and click **Webpage**. Click the **Security**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

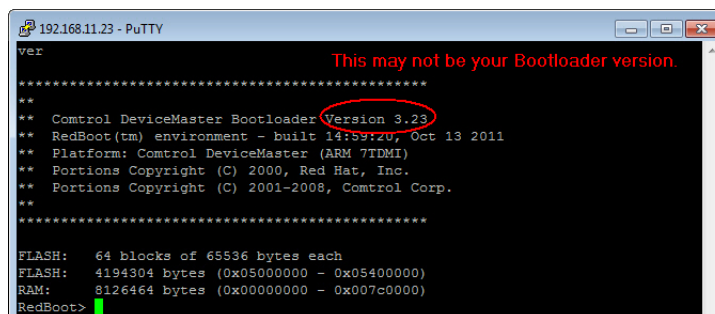
- In PortVision DX, right-click the DeviceMaster LT in the *Device List* pane for which you want to upload the latest SocketServer, and click **Telnet/SSH Session**.



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



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



If the **RedBoot>** prompt does not appear, reboot the DeviceMaster LT and try again. You must be at the **RedBoot>** prompt for the following steps to work. Repeat [Steps 6](#) through 7.

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

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

10. Enter the following command:

```
load -r -b 0x28000000 -h <tftp-Server_IP_Addr> <Download_FileName>
```

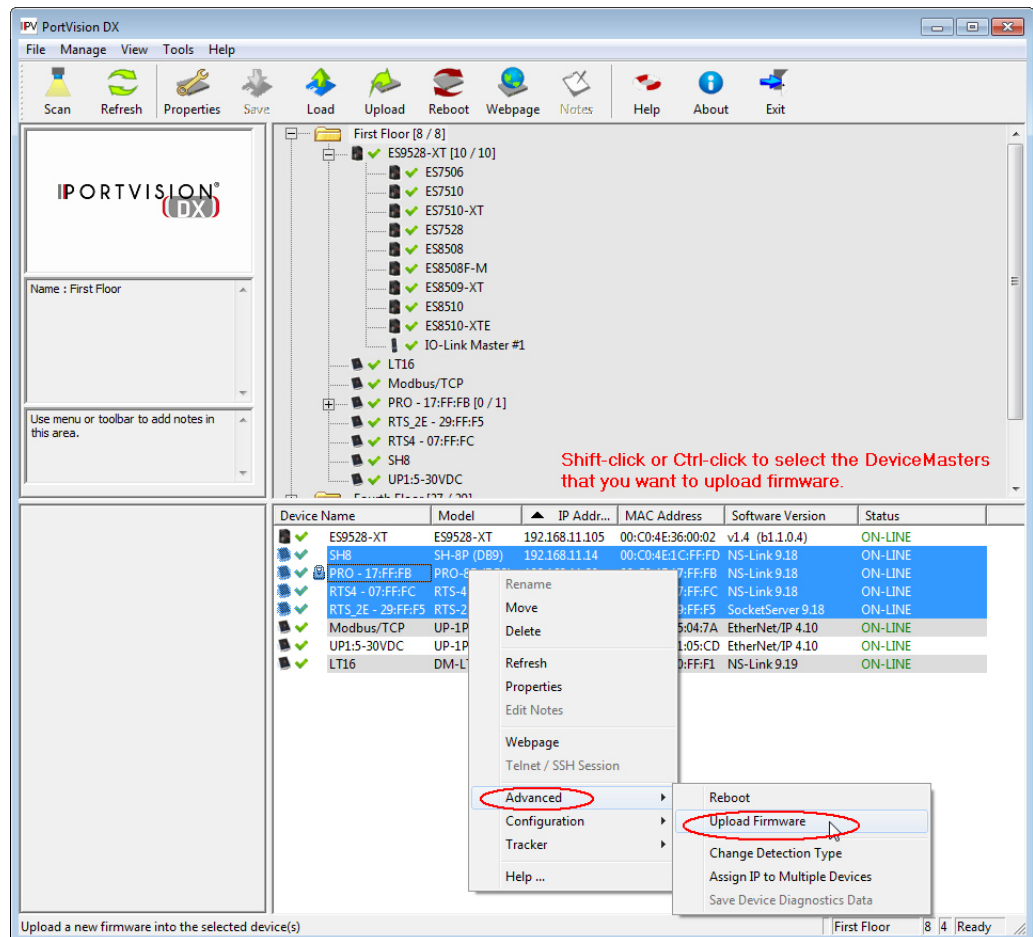
***Note:** The **tftp-Server_IP_Addr** can be viewed in the application (Page 70) and if you renamed the file as suggested, the file name is **1.bin**.*

11. At the **RedBoot>** prompt, type **go** after the *raw* file string appears.
12. Close the PuTTY window and click **Ok**.
13. In PortVision DX, highlight the DeviceMaster LT in the *Device List* pane that you updated and click **Refresh**. You may need to click **Refresh** several times before you see the latest SocketServer version listed under the *Software Version*.

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.



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

It may take a few moments for the firmware to upload onto the 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

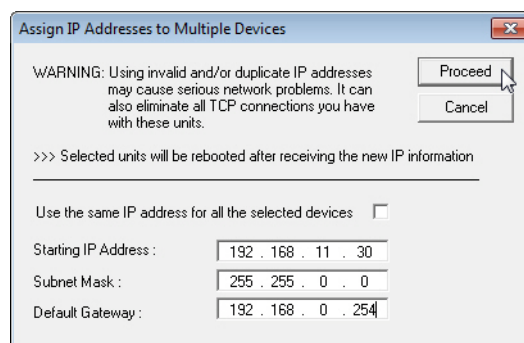
You can configure the network addresses for multiple DeviceMaster LTs using the **Assign IP to Multiple Devices** option.

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 77 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.



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:

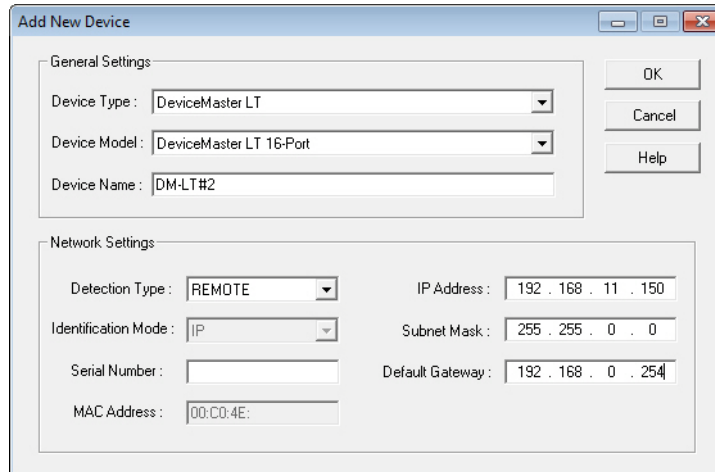
- Configure DeviceMaster LT units that are not on the local network (remote) using [Remote Using the IP Address](#) on Page 75.
- Pre-configure a DeviceMaster LT in PortVision DX (local) using [Local Using the IP Address or MAC Address](#) on Page 76.

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.

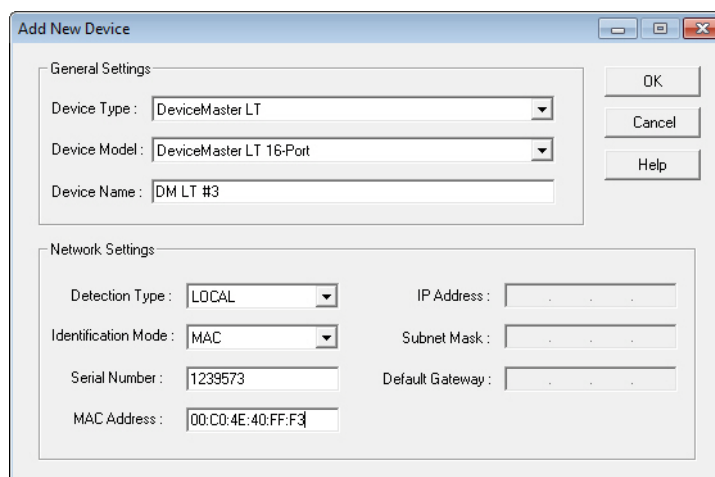


8. Click **Ok** to close the *Add New Device* window. It may take a few moments to save the DeviceMaster LT.
9. If necessary, click **Refresh** for the new DeviceMaster LT to display in the *Device Tree* or *Device List* panes. The DeviceMaster LT shows **OFF-LINE** if it is not attached to the network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



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 the configuration file (.dc) from the *Main* or **Properties > Software Settings** tab in PortVision DX and load that configuration onto other DeviceMaster LT units.

If you save a SocketServer configuration file from the *Main* or **Software Settings** tab on the *Properties* screen, you can choose what settings you want saved or loaded.

You may want to program the network settings in multiple DeviceMaster LTs using [Configuring Multiple DeviceMaster LTs Network Addresses](#) on Page 75.

Saving a SocketServer Configuration File

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

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

1. If you have not done so, install PortVision DX ([Installing PortVision 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.

Loading a SocketServer Configuration File

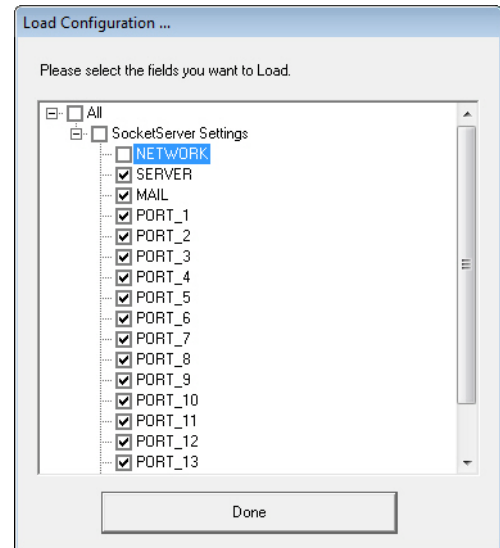
Use the following procedure to load a previously saved a DeviceMaster LT configuration file. Load a configuration file and apply it to a selected DeviceMaster LT or DeviceMaster LTs from the *Device List* pane or **Software Settings** tab on the *Properties* screen.

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**

- Click **Load Settings from a File** on the **Software Settings** tab of the *Properties* screen
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.



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

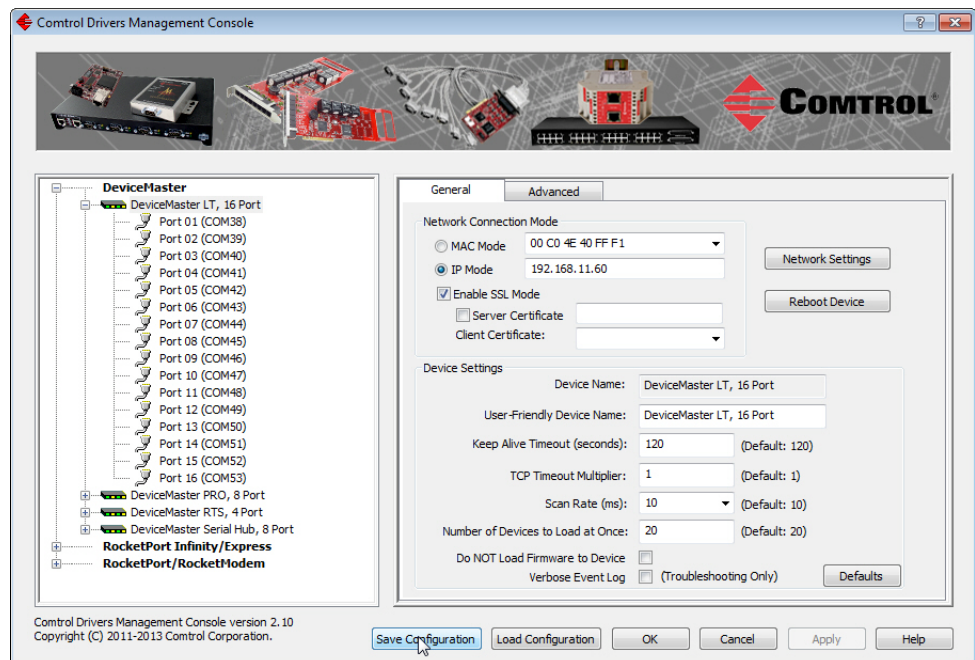
You must save the driver configuration file in portions:

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

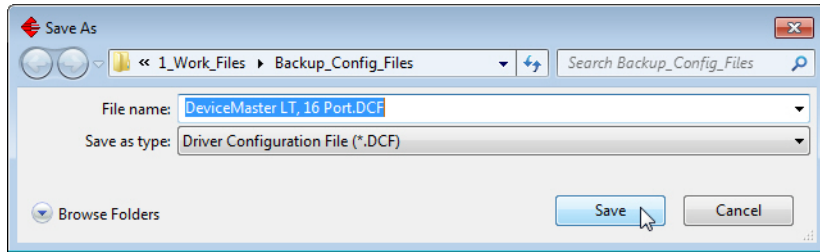
Saving Device-Level Configuration

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

1. If necessary, open the *Control Drivers Management Console* using one of these methods:
 - **Windows Control Panel**; go to your *Control Panel* and click the **Control Drivers Management Console**.
 - **Shortcut**; located under **Start > Program Files > Control > DeviceMaster LT > Control 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**.



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

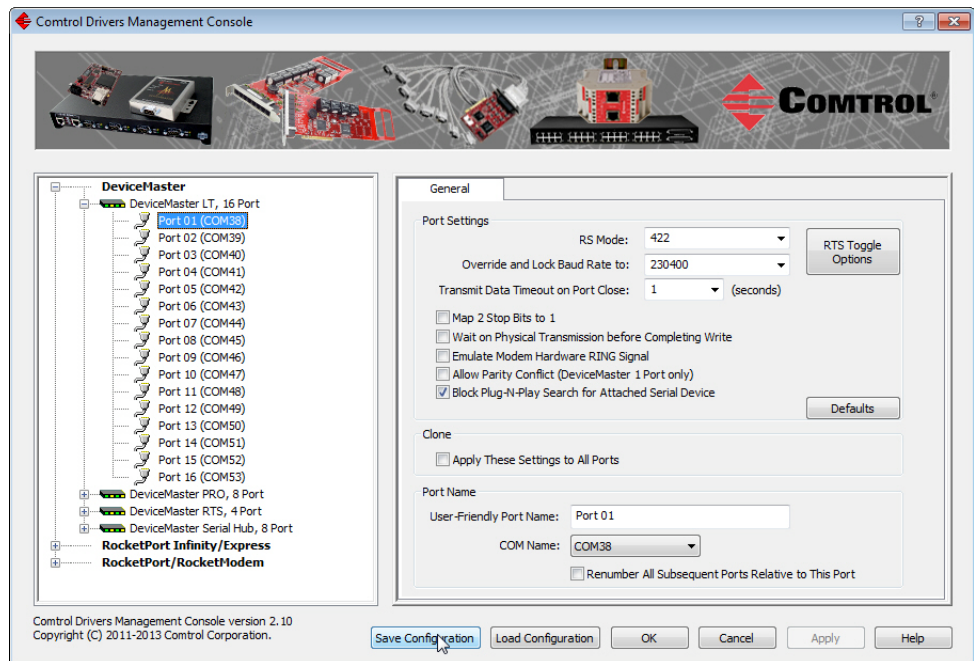


- Repeat the previous steps for each DeviceMaster LT for which you want to save the driver configuration.

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.

- If necessary, open the *Control Drivers Management Console* using one of these methods:
 - Windows Control Panel**; go to your *Control Panel* and click the **Control Drivers Management Console**.
 - Shortcut**; located under **Start > Program Files > Control > DeviceMaster LT > Control Drivers Management Console**.
- 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.
- Highlight the DeviceMaster LT for which you want to save the port-level configuration.
- Highlight the port for which you want to save port configuration.



- Click **Save Configuration**.
- 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.

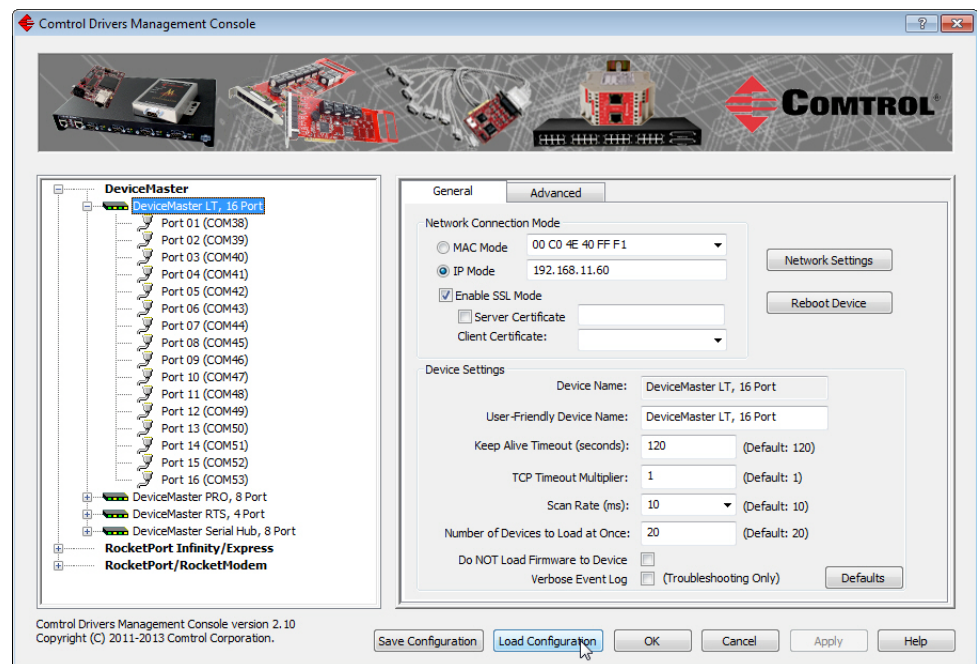
The driver configuration file uploads in portions:

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

Loading Device Configuration

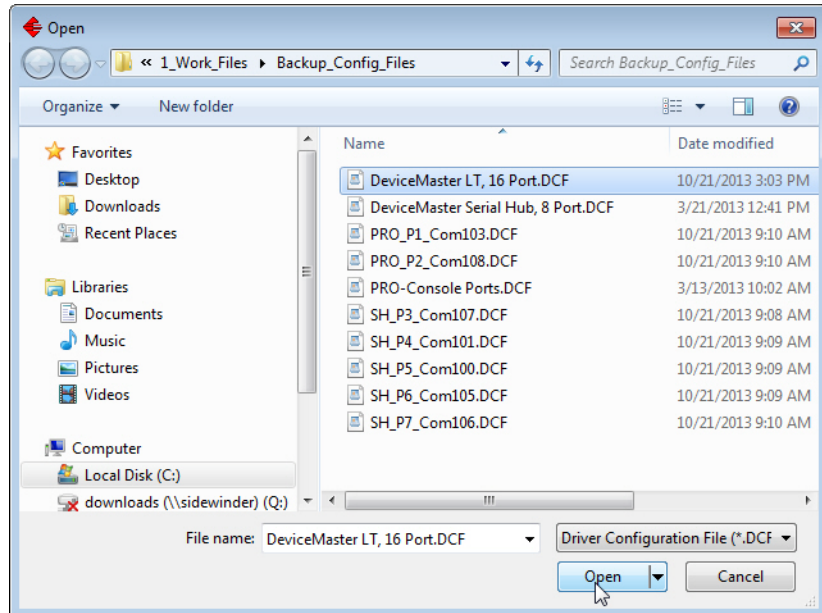
Use the following procedure to load the configuration file for device-level information for your DeviceMaster LT.

1. If necessary, open the *Control Drivers Management Console* using one of these methods:
 - **Windows Control Panel;** go to your *Control Panel* and click on the **Control Drivers Management Console**.
 - **Shortcut;** located under **Start> Program Files> Control> DeviceMaster LT> Control 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.

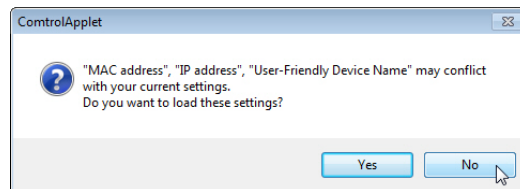


4. Click **Load Configuration**.
5. Browse to the location of the configuration file that you want to load.

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



- Make the appropriate choice for your situation:
 - Click **No** to the *ControlApplet* message, if you are using the file to set up multiple DeviceMaster LTs with the same device-level settings.
 - Click **Yes** to the *ControlApplet* 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.



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

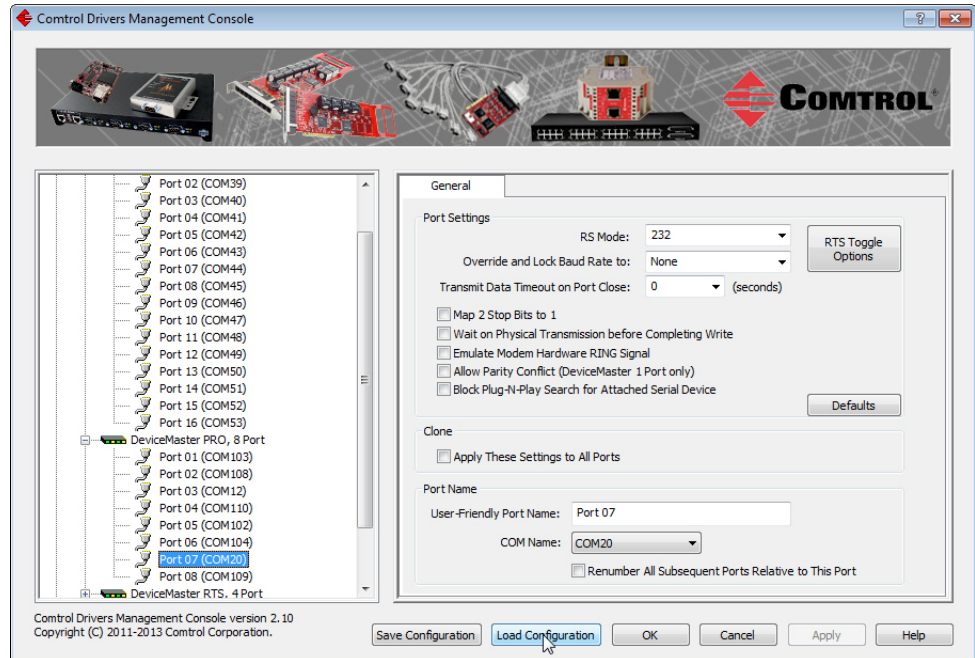
Loading Port Configuration

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

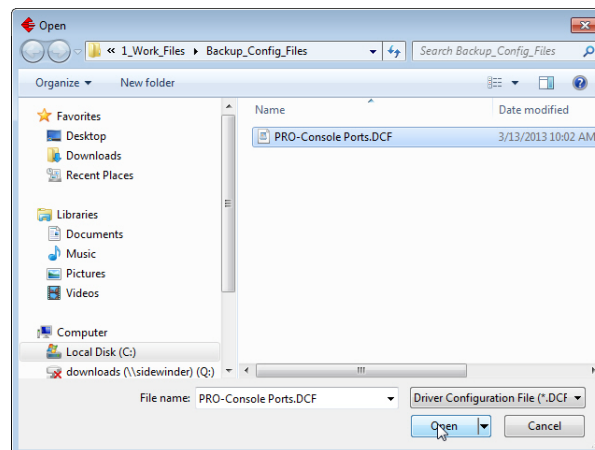
Note: Device driver configuration files must be for the same model with the same port density

- If necessary, open the *Control Drivers Management Console* using one of these methods:
 - Windows Control Panel;** go to your *Control Panel* and click on the **Control Drivers Management Console**.
 - Shortcut;** located under **Start > Program Files > Control > DeviceMaster LT > Control Drivers Management Console**.
- 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.

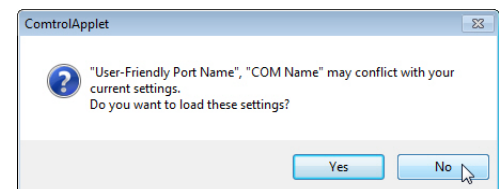
- In the left pane, highlight the port for which you want to load the port-level settings from the configuration file.



- Click **Load Configuration**.
- Browse to the location of the configuration file that you want to load.
- Highlight the configuration file and click **Open**. The configuration file loads in a few moments.



- 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.



- Click **Apply** so that the configuration is saved on the DeviceMaster LT.
- Repeat [Steps 3](#) through 8 for each port that you want to restore.

Changing the Bootloader Timeout

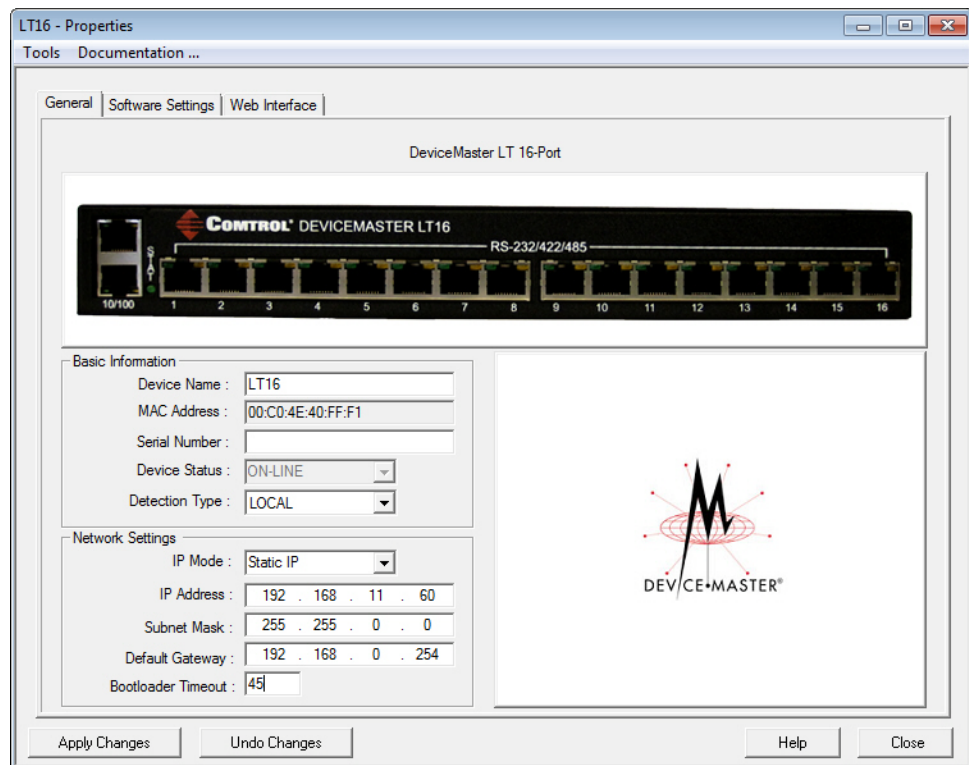
If SocketServer fails during the upload process, you should change the **Bootloader timeout** value to 45 seconds.

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 18.*

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

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.

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



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 Control 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 99 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 103.

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 Control 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 Control 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.*

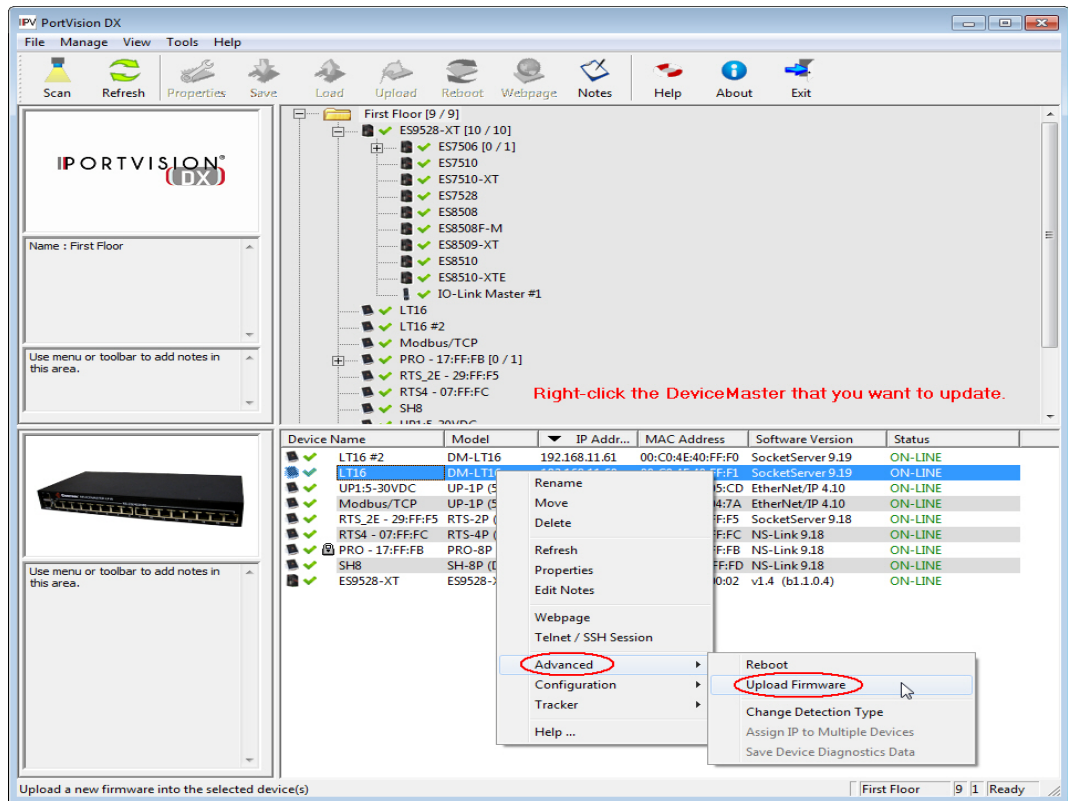
Make sure that power is not interrupted while uploading Bootloader. Power interruption while uploading Bootloader will require that the DeviceMaster LT must be sent into Control so that it can be reflashed.

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

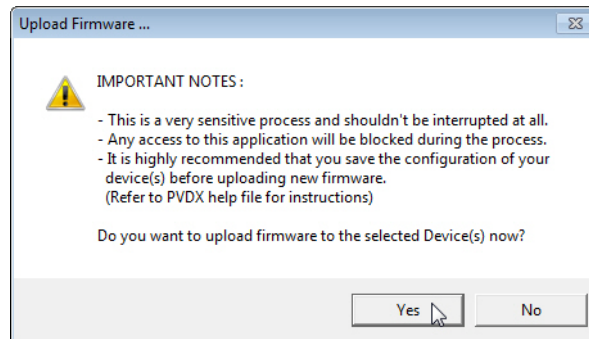


1. If you have not done so, install PortVision DX ([Installing PortVision DX](#) on Page 15) and **Scan** the network.
2. If necessary, check the Bootloader version ([Checking the Bootloader Version](#)) and download the latest version.

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



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



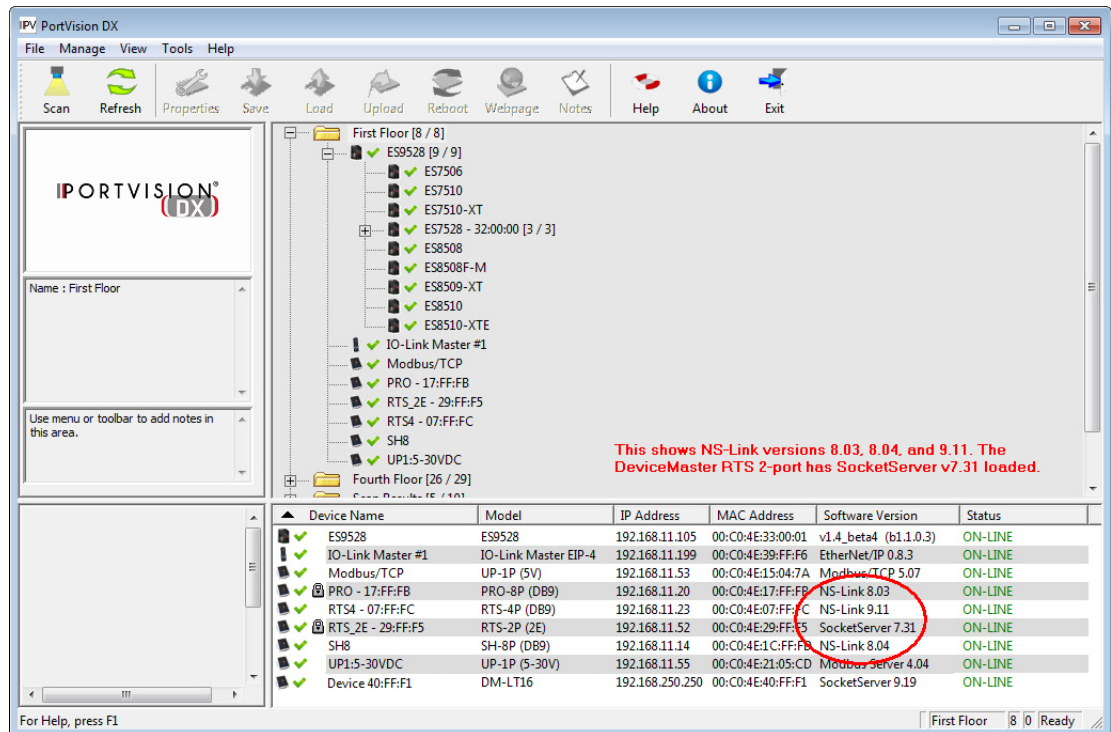
- Click **Ok** to the second *Upload Firmware* message.
- Right-click the DeviceMaster LT and click **Refresh** until the Bootloader version displays in the *Device List* pane and verify that the new version loaded.



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.



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

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

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

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

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

FTP directory /dev_mstr/Lt/software/socketserver/ at ftp.control.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](#)

```
03/11/2013 02:16PM      124,405 1800111\_socketserver\_history.pdf
02/08/2013 10:42AM      Directory help
10/02/2012 10:08AM      1,174,340 socketserver-8.04.bin
```

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 24.
 - 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](#)

08/31/2012 11:38AM	6,775,432	devicemaster_windows_9.06.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 Page 9 or viewed on the Control CD shipped with the DeviceMaster LT.

Restoring Serial Port Settings

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

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

NS-Link COM Port

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

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

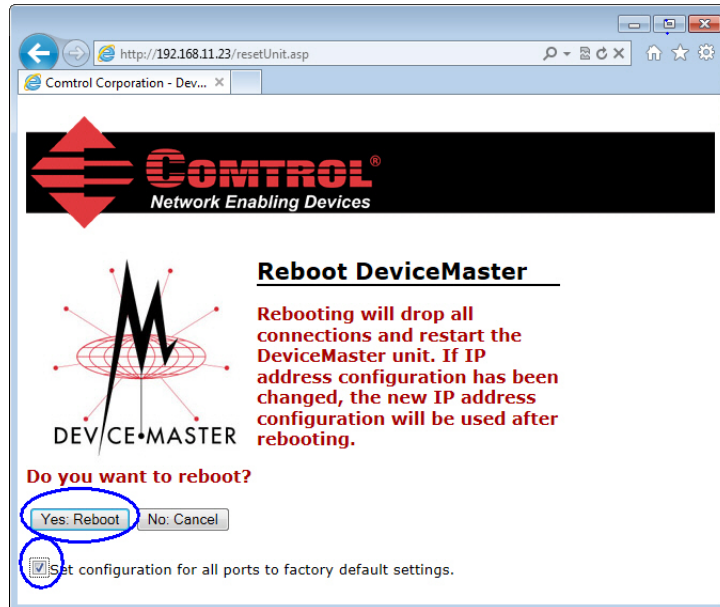
If necessary, you can reset DeviceMaster LT device properties to their defaults on the *Device General* tab using the Defaults button.

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 43).
2. Scroll to the bottom of the *Server Status* page (main) and click **Reboot**.

3. When the **Reboot** page appears, click the **Set configuration for all ports to factory default settings** check box.



4. Click the **Yes, Reboot** button.

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

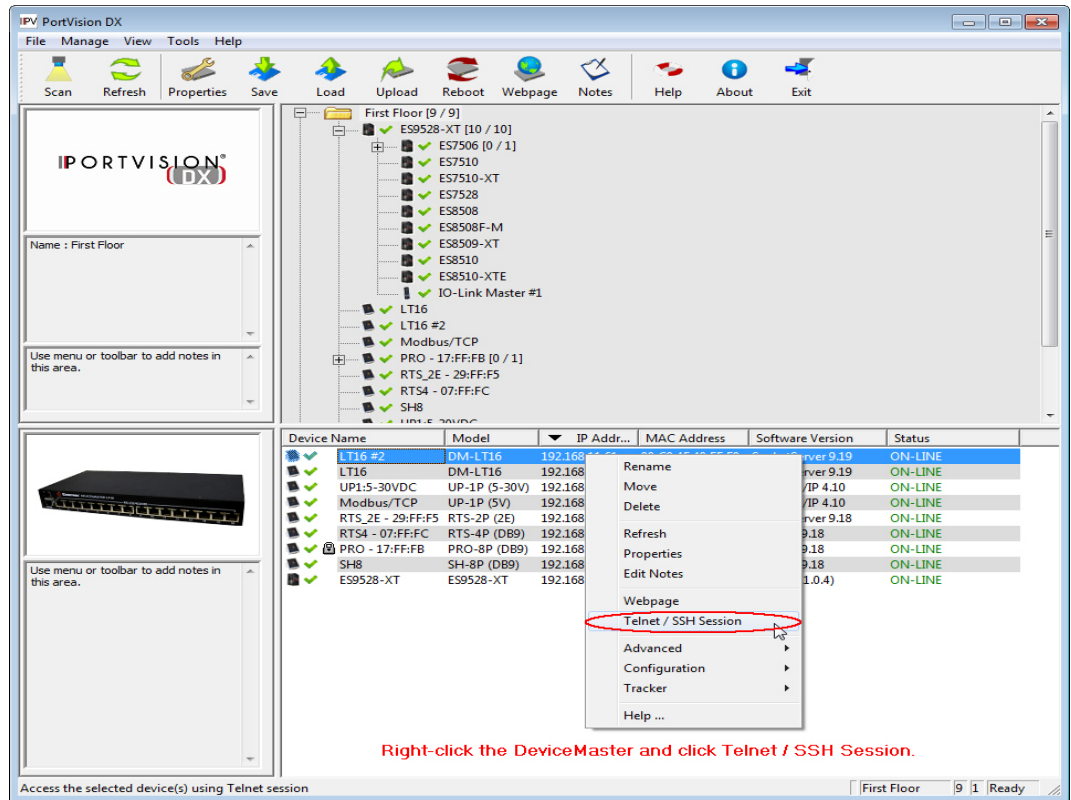
You can open a Telnet or SSH session using PortVision DX. Use the appropriate procedure for your site:

- [Telnet Session](#) (below)
- [SSH Session](#) on Page 92

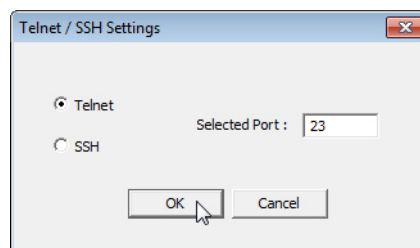
Telnet Session

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

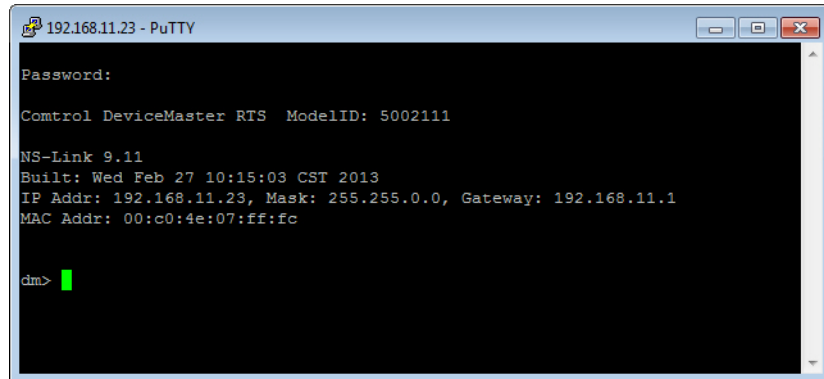
1. In PortVision DX, right-click the DeviceMaster LT in the *Device List* pane for which you want to open a telnet session, and click **Telnet/SSH Session**.



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**.



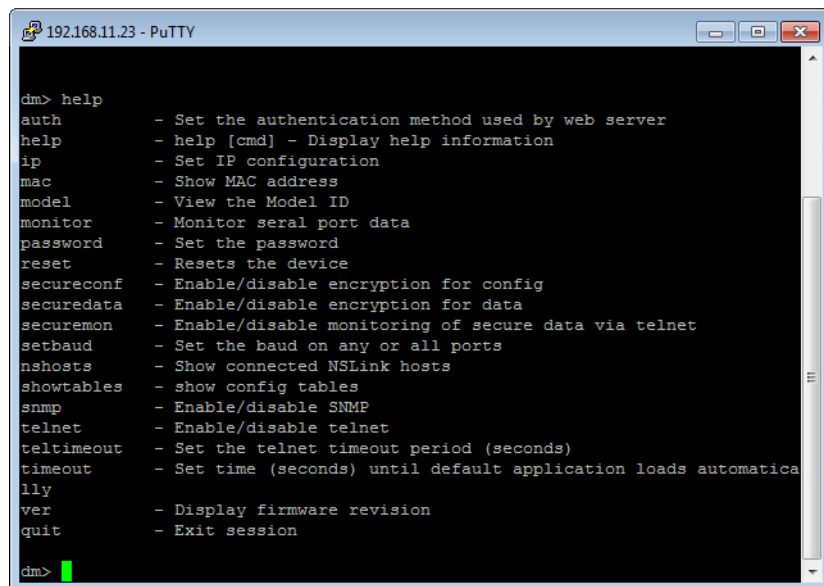
```
192.168.11.23 - PuTTY
Password:

Comtrol DeviceMaster RTS ModelID: 5002111

NS-Link 9.11
Built: Wed Feb 27 10:15:03 CST 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>
```

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



```
192.168.11.23 - PuTTY

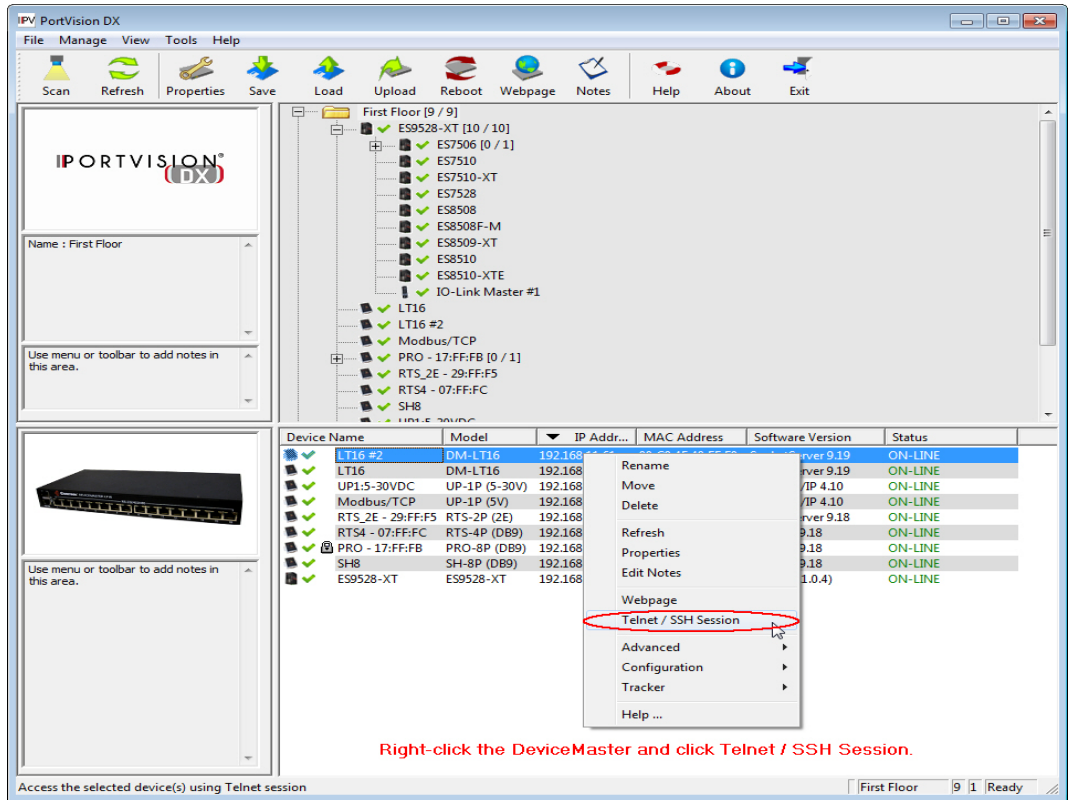
dm> help
auth          - Set the authentication method used by web server
help          - help [cmd] - Display help information
ip            - Set IP configuration
mac           - Show MAC address
model         - View the Model ID
monitor       - Monitor serial port data
password      - Set the password
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 automatica
lly
ver           - Display firmware revision
quit          - Exit session

dm>
```

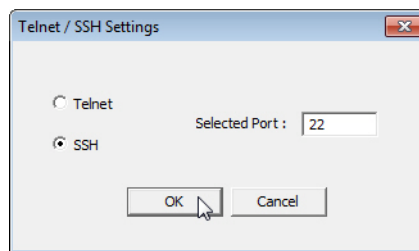

SSH Session

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

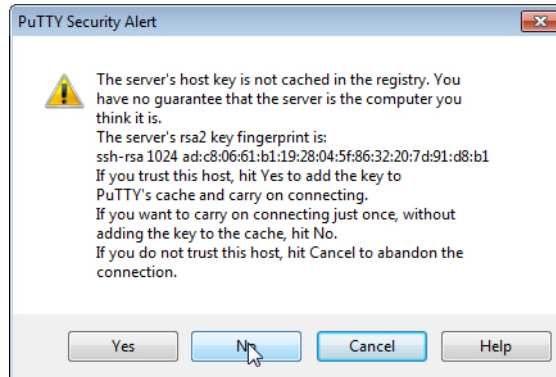
1. In PortVision DX, PortVision DX, right-click the DeviceMaster LT in the *Device List* pane for which you want to open an SSH session, and click **Telnet/SSH Session**.



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



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



- Press **Enter**.

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

- If necessary, enter the password and press **Enter**. If a password has not been set, press **Enter**.
- You can type **help** to refer to available SocketServer/NS-Link commands.

```

192.168.11.23 - PuTTY
login as:
Please log in. Unauthenticated use prohibited.
@192.168.11.23's password:

Control DeviceMaster RTS ModelID: 5002111

NS-Link 9.11
Built: Wed Feb 27 10:15:03 CST 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> help
auth          - Set the authentication method used by web server
help          - help [cmd] - Display help information
ip            - Set IP configuration
mac           - Show MAC address
model         - View the Model ID
monitor       - Monitor serial 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>

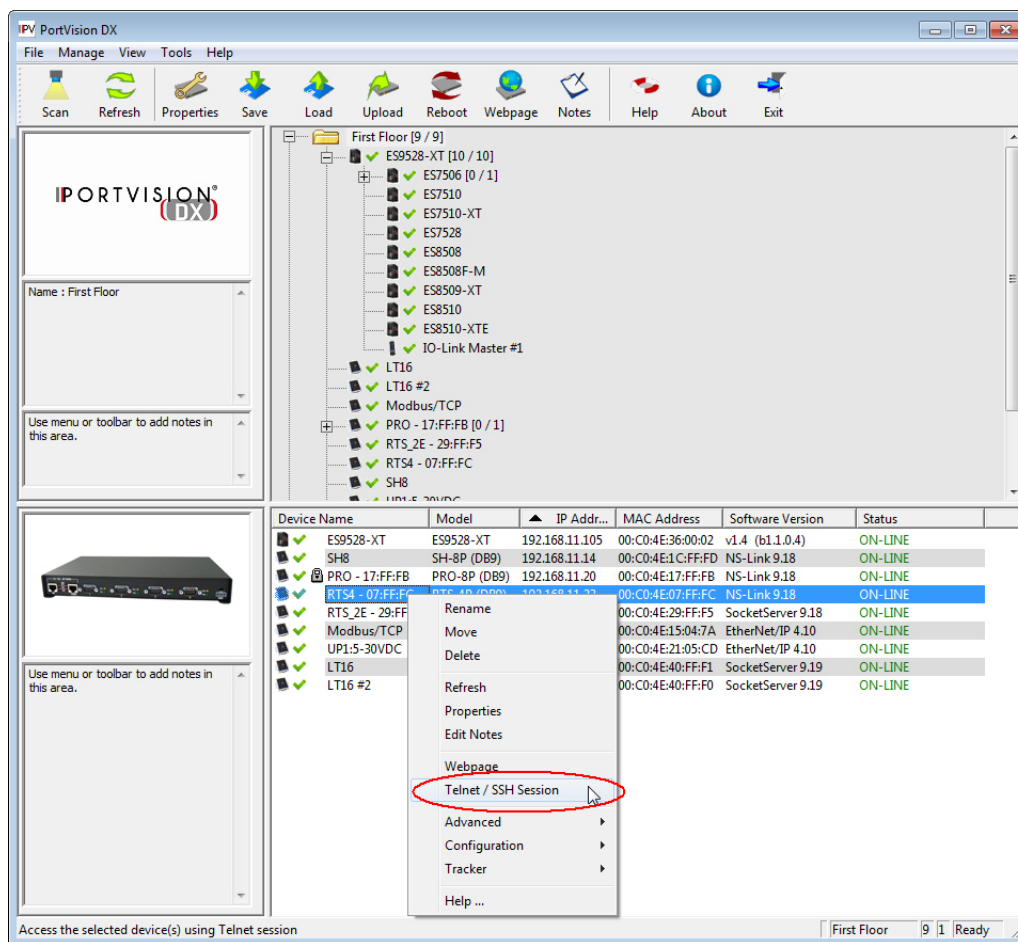
```

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

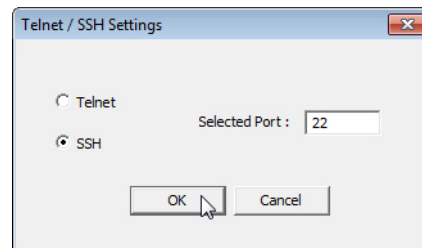
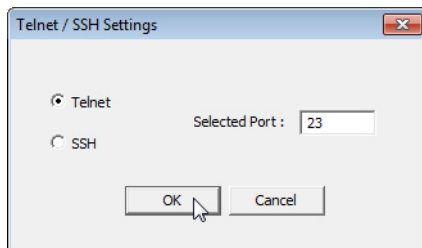
You can open a Telnet or SSH session using PortVision DX to access RedBoot commands.

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

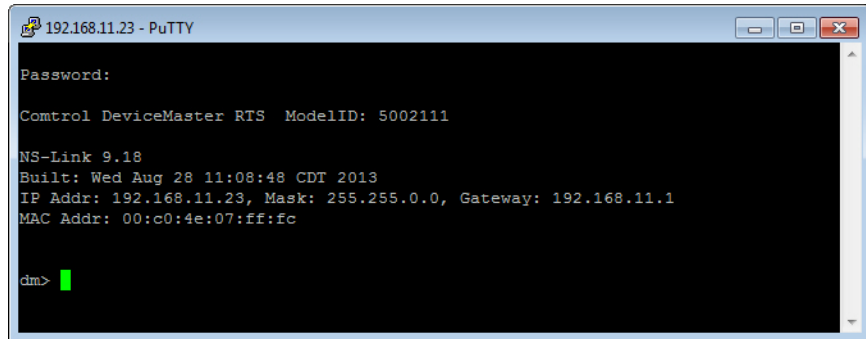
1. In PortVision DX, right-click the DeviceMaster LT in the *Device List* pane for which you want to open a telnet session, and click **Telnet/SSH Session**.



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



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.



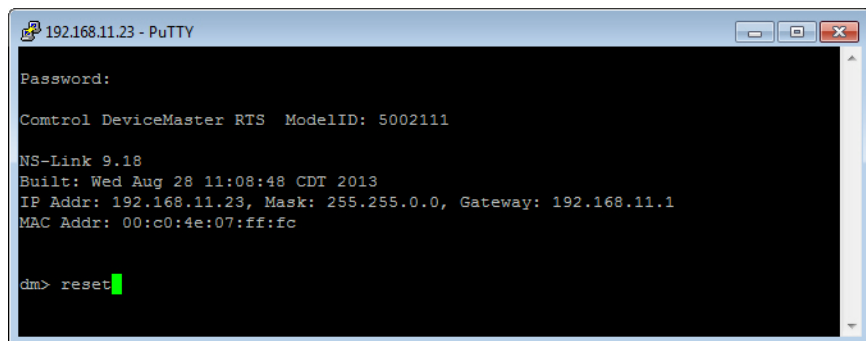
```

192.168.11.23 - PuTTY
Password:
Control 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.

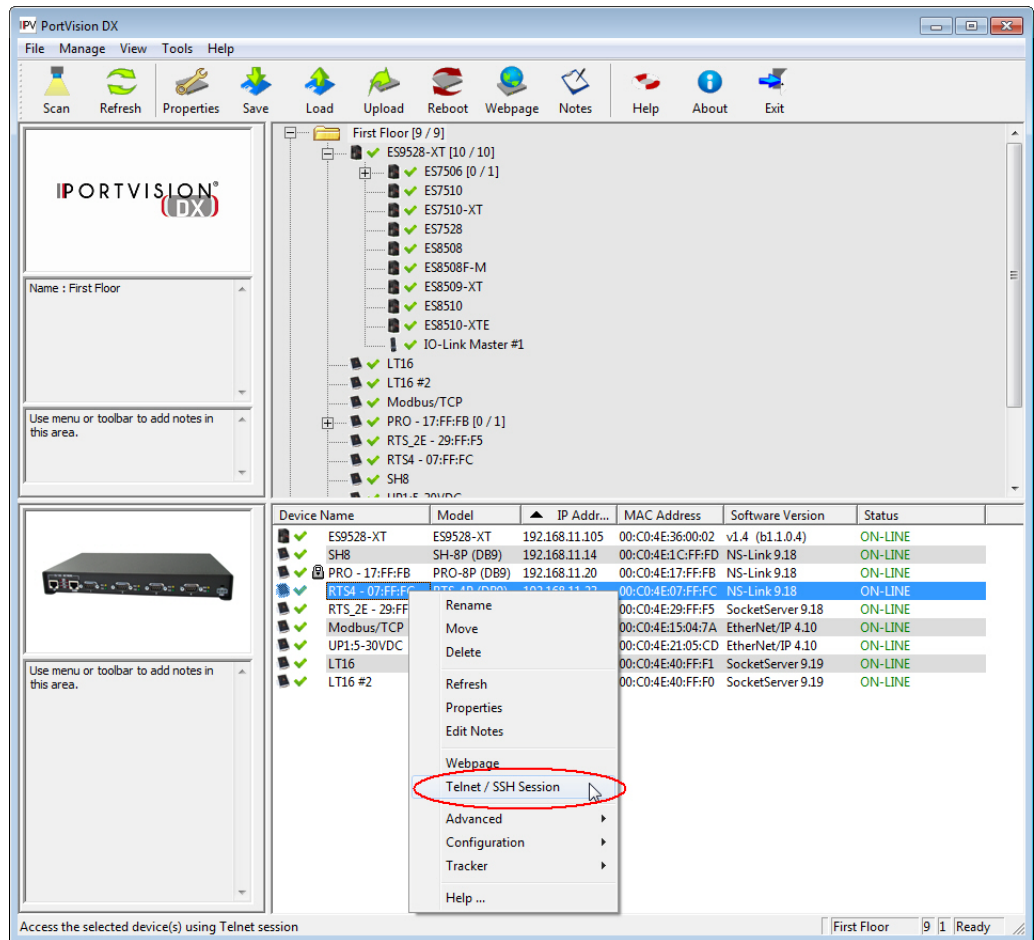


```

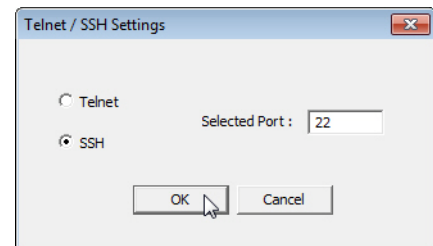
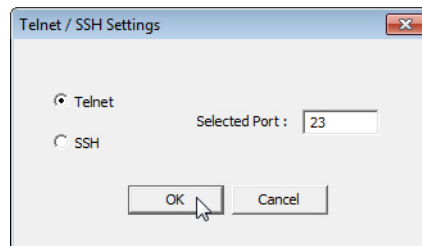
192.168.11.23 - PuTTY
Password:
Control DeviceMaster RTS ModelID: 5002111
NS-Link 9.18
Built: Wed Aug 28 11:08:48 CDT 2013
IP Addr: 192.168.11.23, Mask: 255.255.0.0, Gateway: 192.168.11.1
MAC Addr: 00:c0:4e:07:ff:fc

dm> reset
    
```

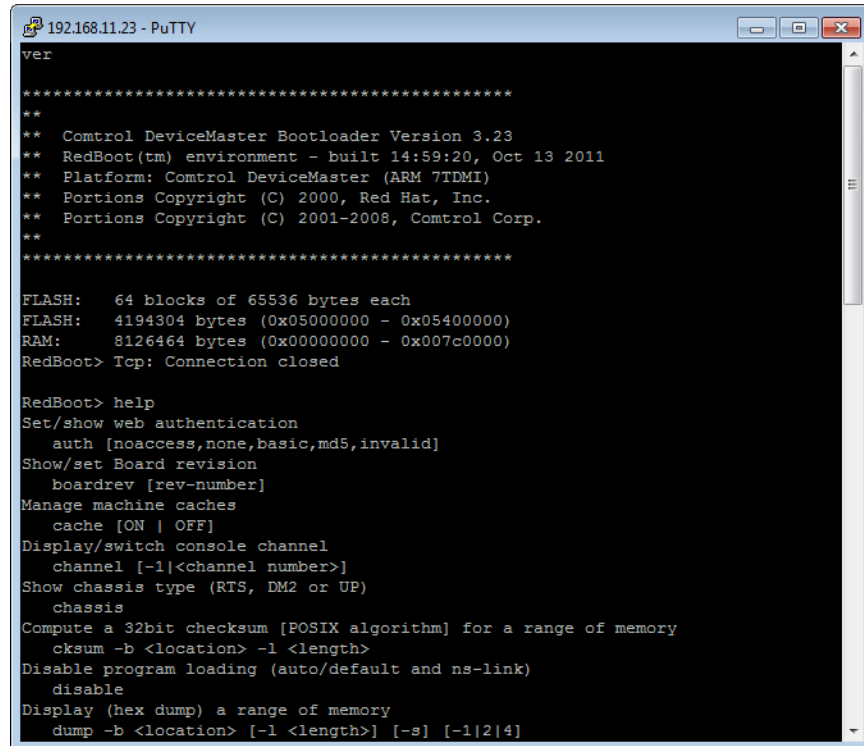
5. Quickly re-open the telnet or SSH session using the previous steps.



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



7. Press **Enter**. You can type **help** to review the RedBoot commands. You can also refer to [RedBoot Command Overview](#) on Page 107.



```
192.168.11.23 - PuTTY
ver
*****
**
** Control DeviceMaster Bootloader Version 3.23
** RedBoot(tm) environment - built 14:59:20, Oct 13 2011
** Platform: Control DeviceMaster (ARM 7TDMI)
** Portions Copyright (C) 2000, Red Hat, Inc.
** Portions Copyright (C) 2001-2008, Control Corp.
**
*****
FLASH: 64 blocks of 65536 bytes each
FLASH: 4194304 bytes (0x05000000 - 0x05400000)
RAM: 8126464 bytes (0x00000000 - 0x007c0000)
RedBoot> Tcp: Connection closed

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 [-l]<channel number>]
Show chassis type (RTS, DM2 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] [-l|2|4]
```

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.

- [Accessing RedBoot Overview](#) on Page 99
- [Establishing a Serial Connection](#) on Page 100
- [Establishing a Telnet Connection](#) on Page 101
- [Determining the Network Settings](#) on Page 102
- [Configuring the Network Settings](#) on Page 102
- [Changing the Bootloader Timeout](#), Page 103
- [Determining the Bootloader Version](#) on Page 103
- [Resetting the DeviceMaster LT](#) on Page 104
- [Uploading Firmware - Telnet Method \(Linux\)](#) on Page 104
- [Configuring Passwords](#) on Page 106
- [RedBoot Command Overview](#) on Page 107.

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 94.

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 100). 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 101), 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 65, 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 99 or use the [RedBoot Command Overview](#) on Page 107 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, open a **Command** window and type **telnet [ip_address]**
2. Press the **Enter** key if you did not program a password or type the password and press **Enter**.

```

♥♦
Password:

Control DeviceMaster RTS Model ID: 5002535

SocketServer 9.18
Built: Wed Aug 28 11:08:48 CST 2013
IP Addr: 192.168.11.52, Mask: 255.255.0.0, Gateway: 192.168.0.254
MAC Addr: 00:c0:4e:29:ff:f5

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.

```

*****
**
** Control DeviceMaster Bootloader Version 3.23
** RedBoot(tm) environment - built 14:59:20, Oct 13 2011
** Platform: Control DeviceMaster (ARM 7TDMI)
** Portions Copyright (C) 2000. Red Hat, Inc.
** Portions Copyright (C) 2001-2008 Control Corp.
*****

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

```

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

Determining the Network Settings

Default Network Settings

IP address:
192.168.250.250

Subnet mask:
255.255.0.0

Gateway address:
192.168.250.1

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

1. Establish communications with the DeviceMaster LT using the serial (Page 100) or telnet (Page 101) method.
2. At the **RedBoot** prompt, type **ip**.

```
RedBoot>dis
Loading disabled
RedBoot> ip
IP:      192.168.250.250
Mask:    255.255.0.0
Gateway: 192.168.50.1
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 100) or telnet (Page 101) 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:    255.255.0.0
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 100) or telnet (Page 101) 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 100) or telnet (Page 101) method.
2. At the **RedBoot** prompt, type **version**.

```
RedBoot> ver
*****
**
** Control DeviceMaster Bootloader Version 3.23
** RedBoot(tm) environment - built 14:59:20, Oct 13 2011
** Platform: Control DeviceMaster (ARM 7TDMI)
** Portions Copyright (C) 2000. Red Hat, Inc.
** Portions Copyright (C) 2001-2008 Control Corp.
*****

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

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
```

Uploading Firmware - Telnet Method (Linux)

Optionally, you can install PortVision DX on a Windows system on the network and upload firmware. PortVision DX is the recommended method for uploading firmware. See [Installing PortVision DX](#) on Page 15 and [Uploading SocketServer with PortVision DX](#) on Page 24.

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

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

- If you are using Windows, see [Updating Firmware Across WANs \(Windows\)](#) on Page 70 to install and use a TFTP server with PortVision DX.
- If you are using Linux and do not have a TFTP server installed, you can use [Setting Up a TFTP Server in Linux](#) (below). If you have a TFTP server installed, you can skip to [Uploading the Firmware](#) on Page 105.

Setting Up a TFTP Server in Linux

Use this procedure to set up a TFTP server.

1. Install and enable the tftp server software:

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

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

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

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

```
IPTABLES_MODULES="ip_conntrack_tftp"
```

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

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

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

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

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

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

```
/sbin/service iptables restart
```
6. Add the proper lines to **/etc/hosts.allow**:

```
in.tftpd: 192.168.250.250
```
7. Go to [Uploading the Firmware](#) on Page 105 to load the firmware.

Uploading the Firmware

This Linux procedure requires that a TFTP server is installed.

1. Verify that you have the **.bin** file ([Locating Software and Documentation](#) on Page 9) and place the **.bin** file in **/tftpboot** so that you can retrieve it with the DeviceMaster LT.
2. Open a telnet session, enter the DeviceMaster LT IP address.
3. Press the **Enter** key, if you did not program a password or type the password and press **Enter**.
Note: The DeviceMaster LT does not come pre-programmed with a password.
4. Type **reset**, and close the session.
5. Open a new telnet session and enter the DeviceMaster LT IP address.

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

```

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

```
Password:
*****
**
** Control DeviceMaster Bootloader Version 3.23
** RedBoot(tm) environment - built 18:59:20 Oct 13 2011
** Platform: Control DeviceMaster (ARM 7TDMI)
** Portions Copyright (C) 2000. Red Hat, Inc.
** Portions Copyright (C) 2001-2008 Control Corp.
*****

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

```

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

```
RedBoot>dis
Loading disabled

```

8. Verify that the system responds with an **Loading disabled** message.
9. Load the file from a TFTP server using the following command and then press **Enter**:

```
load -r -b 0x28000000 -h <TFTP-Server_IP_Addr> <Downloaded_File_Name>
```
10. When the RedBoot> prompt appears (after approximately one minute if you are uploading the Bootloader and approximately three minutes if you are uploading SocketServer, type **go**.

```
RedBoot>go

```

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

If uploading SocketServer:

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

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

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

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

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

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

Configuring Passwords

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

Note: See the *PortVision 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 100) or telnet method (Page 101).
2. Type **password [your_password]** and press **Enter**.

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

```
Password:
*****
**
** Control DeviceMaster Bootloader Version 3.23
** RedBoot(tm) environment - built 14:59:20, Oct 13 2011
** Platform: Control DeviceMaster (ARM 7TDMI)
** Portions Copyright (C) 2000. Red Hat, Inc.
** Portions Copyright (C) 2001-2008 Control Corp.
*****

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

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

See the **auth** command in the [RedBoot Command Overview](#) on Page 107, 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 is located on the *Control Software and Documentation* CD or you can download it 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.)
boardrev †	Displays the board revision.
cache [ON OFF]	Manages machine caches.
channel [-1]<channel number>	Displays or switches the console channel.
chassis	Displays chassis information.
cksum -b <location> -l <length>	Computes a 32-bit checksum [POSIX algorithm] for a range of memory.
disable	Disables automatic load of the default application.
dump -b <location> [-l <length>] [-s] [-1 2 4]	Displays (hex dump) of a range of memory.
fis {cmds}	Manages flash images. See Chapter 2 of the eCos Reference Manual for {cmds} information.
flash	Shows flash information.
go [-w <timeout>] [-c] [-n] [entry]	Executes code at a location.
help <topic>	Displays available RedBoot commands.
history	Displays command history.
ip [addr mask gateway]	Displays or sets the IP address configuration.
load [-r] [-v] [-h <host>] [-p <TCP port>] [-m <TFTP xyzmodem>] [-c <channel_number>] [-b <base_address>] <file_name>	Loads a file from TFTP server or XModem.
loop 232 422 int port-number	Runs loopback test on port. The DeviceMaster Serial Hub does not support this command.
mac †	Displays ethernet MAC address.
mcmp -s <location> -d <location> -l <length> [-1 -2 -4]	Compares two blocks of memory.

RedBoot Commands (Continued)	
mcopy -s <location> -d <location> -l <length> [-1 -2 -4]	Copies memory from one address to another.
mfill -b <location> -l <length> -p <pattern> [-1 -2 -4]	Fills a block of memory with a pattern.
model †	Shows model number.
password {password}	Sets or deletes the password.
ping [-v] [-n <count>] [-l <length>] [-t <timeout>] [-r <rate>] [-i <IP_addr>] -h <IP_addr>	Network connectivity test.
reset	Resets the DeviceMaster LT.
secureconf [disable enable]	Sets or displays secure config enable.
securedata [disable enable]	Sets or displays secure data enable.
?	Displays short help.
snmp [disable enable]	Sets or displays SNMP enable.
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.
† Do not use these commands to change the values. Doing so would cause the DeviceMaster LT to stop functioning.	

Hardware Specifications

Locating DeviceMaster LT Specifications

Specifications can be found on the Control web site.

External Power Supply Specifications

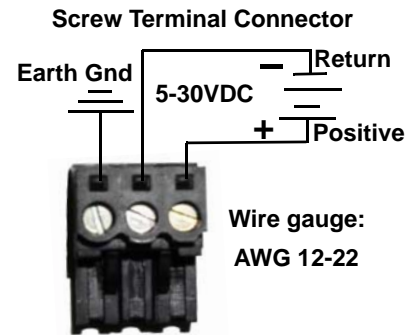
This subsection discusses information that you may need if you wish to use your own external power supplies.

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

Control Power Supply: 5-30VDC	
Input line frequency	43-63 Hz
Input line voltage	90-260 VAC
Output voltage	5-30VDC
Output current	275 mA @ 24VDC

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

External Power Supply: 5-30VDC	
Output voltage†	5-30VDC
Current†	200 mA (Min) @ 24VDC
Power	4.5 W
† Any power supply that meets current consumption, voltage, power, and connector pinouts requirements can be used.	



Notices

Radio Frequency Interference (RFI) (FCC 15.105)

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

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

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

Labeling Requirements (FCC 15.19)

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

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

Modifications (FCC 15.21)

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

Serial Cables (FCC 15.27)

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

Underwriters Laboratory

This equipment is Underwriters Laboratory "UL" listed.

Important Safety Information



To avoid contact with electrical current:

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

Troubleshooting and Technical Support

This section contains troubleshooting information for your DeviceMaster 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 111
- [General Troubleshooting](#) on Page 113
- [Testing Ports Using Port Monitor \(PMon2\)](#) on Page 115
- [Testing Ports Using Test Terminal](#) on Page 118
- [Socket Mode Serial Port Testing](#) on Page 124
- [DeviceMaster LT LEDs](#) on Page 129
- [Removing DeviceMaster LT Security Features](#) on Page 131
- [Returning the DeviceMaster LT to Factory Defaults](#) on Page 133

If you cannot diagnose the problem, you can contact [Technical Support](#) on Page 136.

Troubleshooting Checklist

The following checklist may help you diagnose your problem:

- Verify that you are using the correct types of cables on the correct connectors and that all cables are connected securely.
Note: Most customer problems reported to Control Technical Support are eventually traced to cabling or network problems.
- 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 Control tools.
 - *Advanced* tab in the *Control 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 118 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 115 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 129) 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 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 111.

General Condition	Explanation/Action
Status LED flashing	<p>Indicates that the bootloader has not downloaded to the DeviceMaster LT.</p> <ol style="list-style-type: none"> 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 29 for procedures. <p>Note: If the Status LED is still flashing, contact Technical Support.</p>
Status LED not lit	<p>Indicates that power has not been applied or there is a hardware failure. Contact Technical Support.</p>
Can ping the Control device, but cannot open the ports from a remote location. (You must have previously programmed the IP address, subnet mask, and IP gateway.)	<p>The NS-Link driver uses Port 4606 (11FE h) to communicate with the DeviceMaster LT.</p> <p>When using a <i>sniffer</i> to track NS-Link packets, filtering for Port 4606 will easily track the packet. The packet should also contain the MAC address of the device and the originating PC so that it can be determined if the packet is able to travel the full distance one way or not.</p> <p>If the 4606 packet is found on one side of a firewall or router, using sniffer, and not on the other side, then that port needs to be opened up to allow the 4606 to pass.</p> <p>This will most often be seen with firewalls, but is also seen in some routers.</p>
Cannot ping the device through Ethernet hub	<p>Isolate the DeviceMaster LT from the network. Connect the device directly to the NIC in the host system.</p>
Cannot ping or connect to the DeviceMaster LT	<p>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.</p> <p>In most cases, it will be necessary to program in an address that conforms to your network. See Configuring the Network Settings on Page 18 to use PortVision DX to program the IP address.</p> <p>If you do not use PortVision DX (or the NS-Link driver for Windows) to program the IP address, you can use RedBoot.</p> <p>If you use RedBoot, you only have 15 seconds to disable the Bootloader with RedBoot to get into the setup utility. See RedBoot Procedures on Page 99 for the RedBoot method of programming an IP address.</p>

General Condition	Explanation/Action
<p>DeviceMaster LT continuously reboots when connected to some Ethernet switches with the NS-Link driver</p>	<p>The problem is caused by a L2 bridging feature called Spanning Tree Algorithm (STA) in the switch. This feature is enabled by default in some switches. This feature causes time-out problems on certain L2 protocols, such as our MAC mode.</p> <p><i>Resolution:</i> There will be no firmware fix for this problem. Only one of the following fixes is required for resolution.</p> <ol style="list-style-type: none"> 1. Disable STA in the switch. 2. Enable STA fast forwarding on the port. 3. Change the STA Forward Delay and Message Age to minimum time values. 4. On the device, set the time-out value to 0 (to disable loading of SocketServer) or 120. The command from the redboot prompt is "Timeout 120" without the quotes. <p><i>Problem Details:</i> STA by default blocks packets for 30 seconds after an ethernet port auto negotiates. Blocking of these packets causes the NS-Link driver load process to fail.</p> <p>The normal NS-Link driver load process is:</p> <ol style="list-style-type: none"> 1. If NS-Link determines that it needs to load a device, it resets the device. It does this to get the device into RedBoot mode. Only RedBoot accepts load binary commands, which are needed to load the NS-Link binary into the DeviceMaster 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. <p>If the device is not loaded after timeout seconds (default 15), it loads SocketServer.</p> <p>The above process fails when STA is running because the switch blocks packets for 30 seconds after the DeviceMaster 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.</p>
<p>DeviceMaster LT continuously reboots when connected to some Ethernet switches or routers</p>	<p>Invalid IP information may also cause the switch or router to check for a gateway address. Lack of a gateway address is a common cause.</p>

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

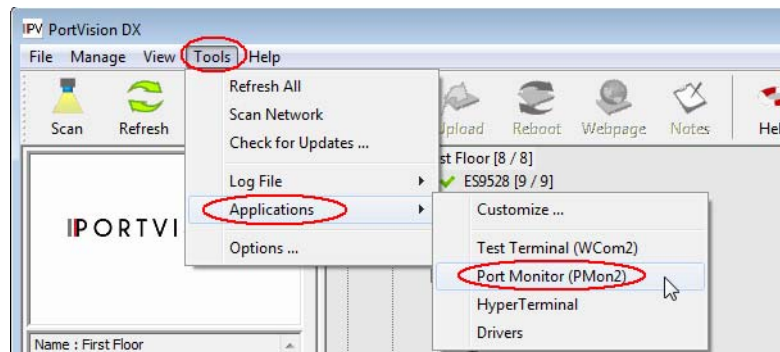
This procedure will check whether the DeviceMaster LT can:

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

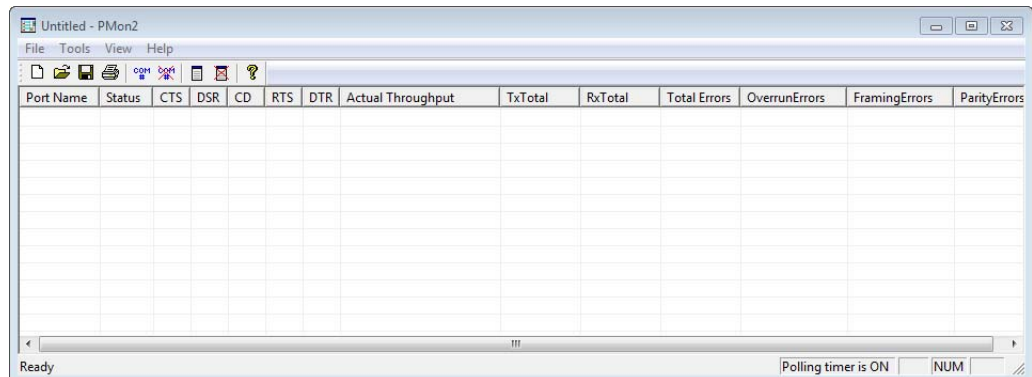
Testing Control COM Ports

If necessary, [Installing PortVision DX](#) on Page 15 to install PortVision DX, which contains Port Monitor.

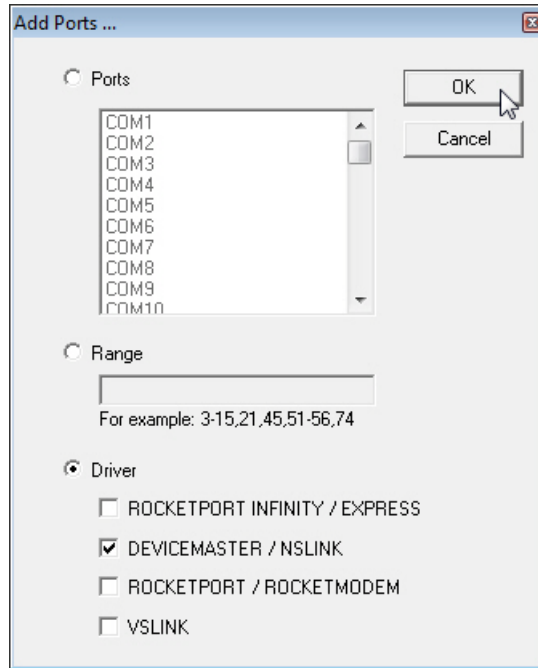
1. Start PortVision DX from the **Start** menu, select **Programs > Control > PortVision DX > PortVision DX** or click the desktop shortcut.
2. Select **Tools > Applications > Port Monitor (PMon2)**.



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



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



- 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.

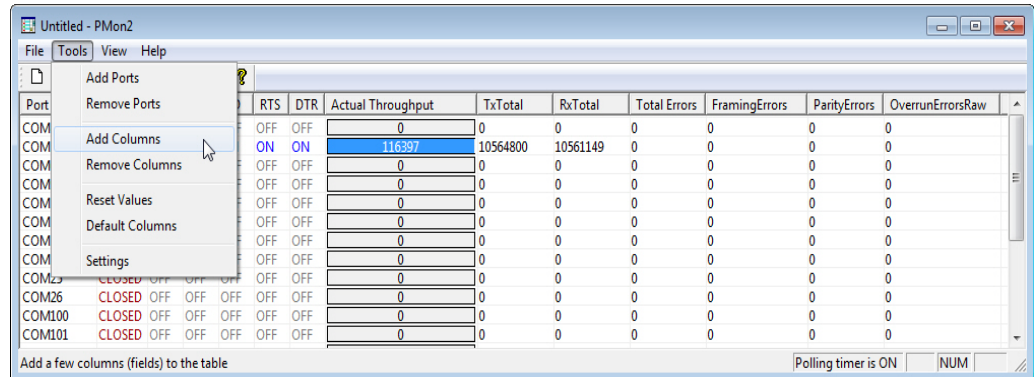
Port Name	Status	CTS	DSR	CD	RTS	DTR	Actual Throughput	TxTotal	RxTotal	Total Errors	FramingErrors	ParityErrors	OverrunErrorsRaw
COM4	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM5	OPEN	ON	ON	ON	ON	ON	115800	9105348	9101707	0	0	0	0
COM6	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM9	CLOSED	OFF	OFF	OFF	OFF	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

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**.

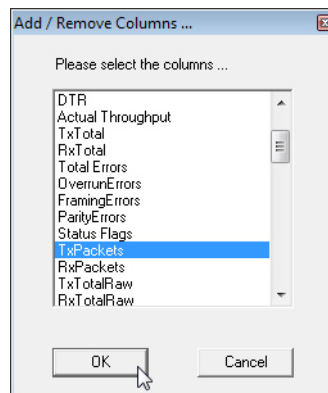
If the errors are:

- 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**.

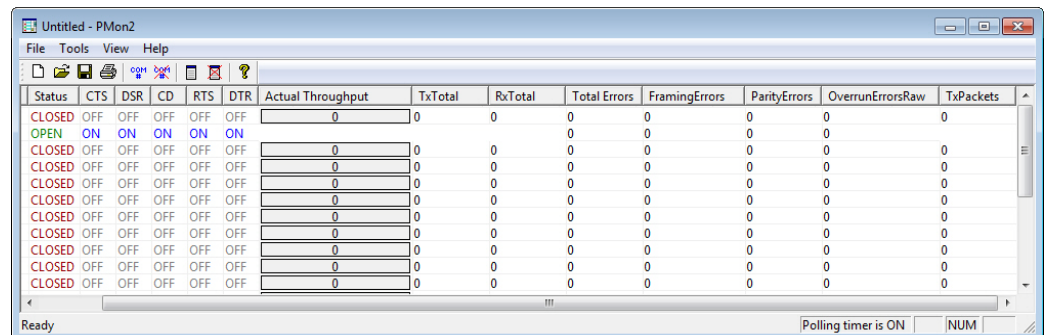


7. Highlight or shift-click to add multiple statistics and click **Ok**.




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


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



9. If you want to capture this session, you can save a current session as a report. To do this, select one of the following save options:

- **File > Save As**
- **File > Save** - if the report already exists in an older format
- **Save Active Session**  button

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

- a. **Select File > Open** or the **Open Existing Session**  button. The *Open Session* dialog appears.
 - b. Locate the session (table), you want to open and click the **Open** button. Optionally, if you want to continue monitoring for an existing session, you need to activate the *Polling Interval*.
 - **Select Tools > Settings** to access the PMon2 *Settings* dialog
 - Change the **Polling Interval** field to a value other than zero (0)
10. Leave Port Monitor open so that you can review events when using *Test Terminal* to test a port or ports.

Testing Ports Using Test Terminal

You can use the following procedure to test COM ports. If you need to install the DeviceMaster 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 65.

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.

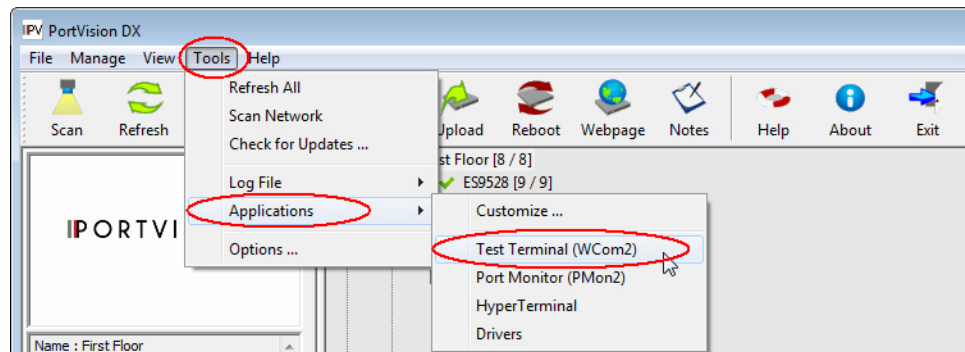
Opening Ports

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 > Control > PortVision DX > PortVision DX** or click the desktop shortcut.
3. Select **Tools > Applications > Test Terminal (WCom2)**.

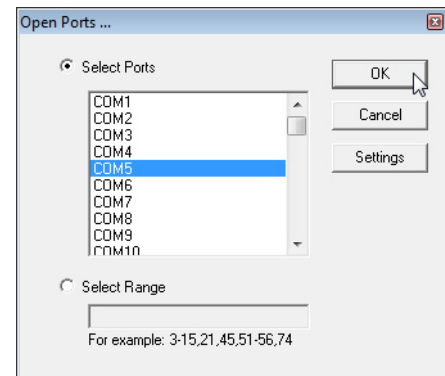


4. Select **File > Open Port**, the appropriate port (or ports) from the *Open Ports* drop list and **Ok**.

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 121



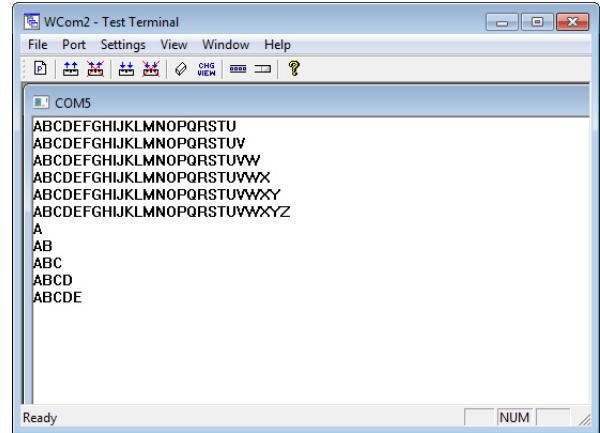
Sending and Receiving Test Data (RS-232/422/485: 4-Wire)

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 119.
2. Install the loopback plug onto the port (or ports) that you want to test. See [Connecting Serial Devices](#) on Page 65, if you need to build loopback plugs.
3. Select **Port > Send and Receive Test Data**.

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

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



4. Select **Port > Send and Receive Test Data** to stop the scrolling data.
5. You can go to the next procedure to run the *Loopback Test* on Page 120 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 119, [Steps 1](#) through [2](#)).
2. Click **Port > Loopback Test**.

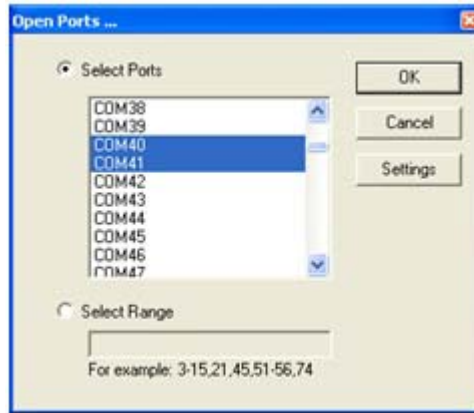
This is a pass fail test and will take a second or two to complete. Repeat for each port that needs testing.

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

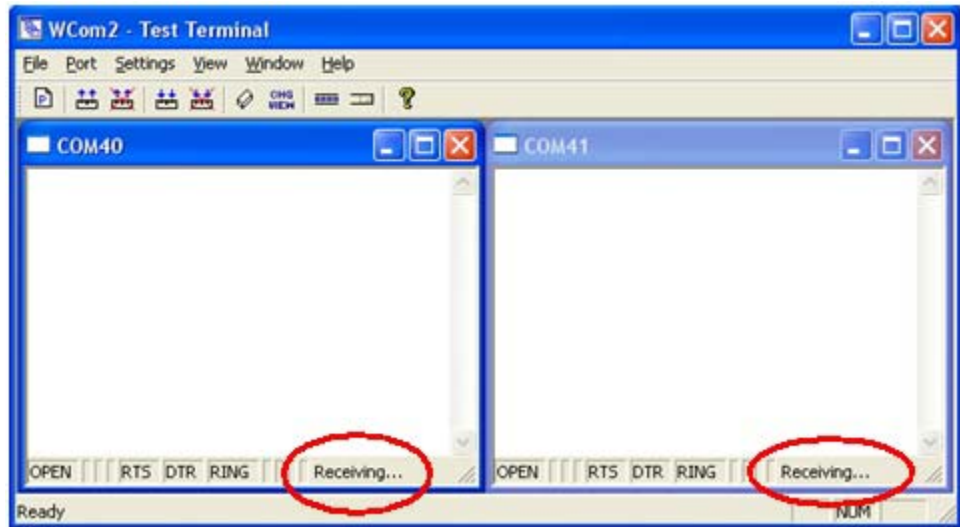
Sending and Receiving Data (RS-485: 2-Wire)

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

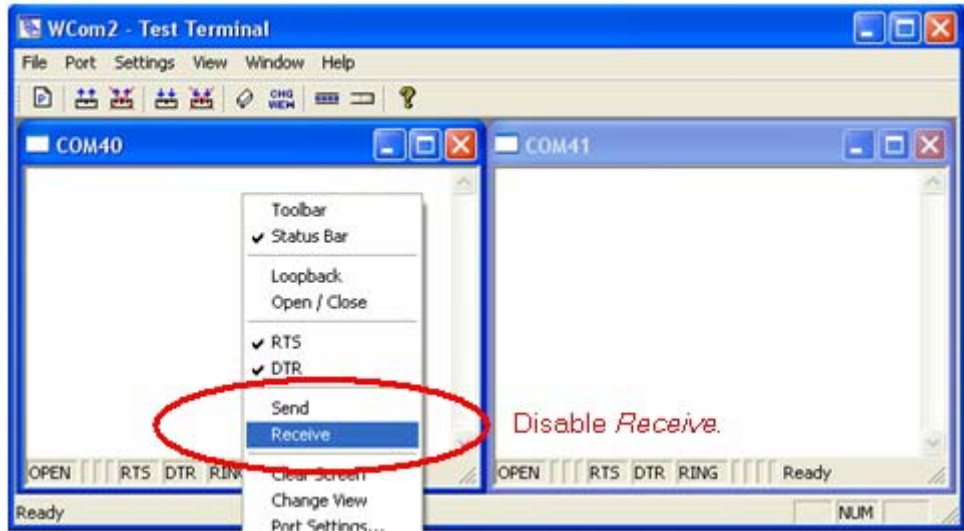
1. In PortVision DX, click **Tools > Applications > Test Terminal (WCom2)** to start Test Terminal.
2. Open two ports RS-485 ports. This example uses COM40 and COM41.



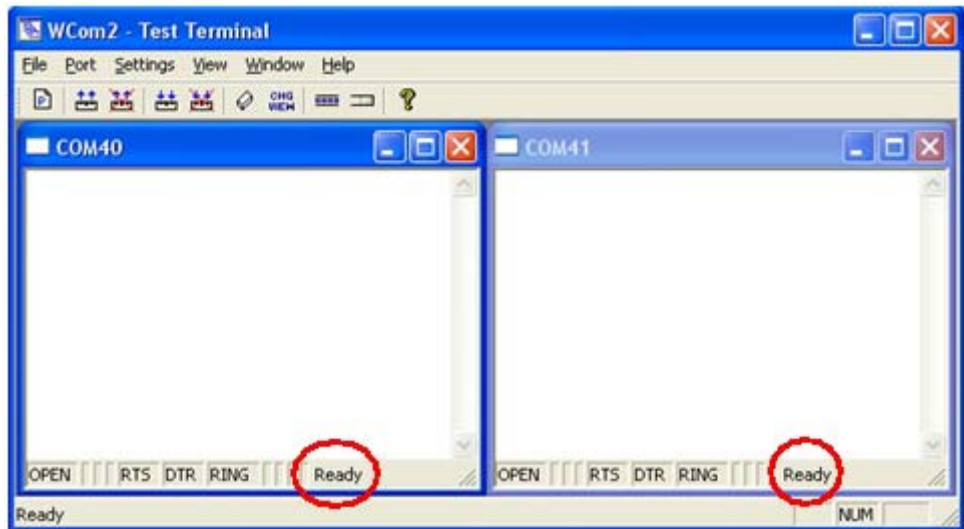
Test Terminal will open two windows, note that both ports show *Receiving* on the status bar.



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

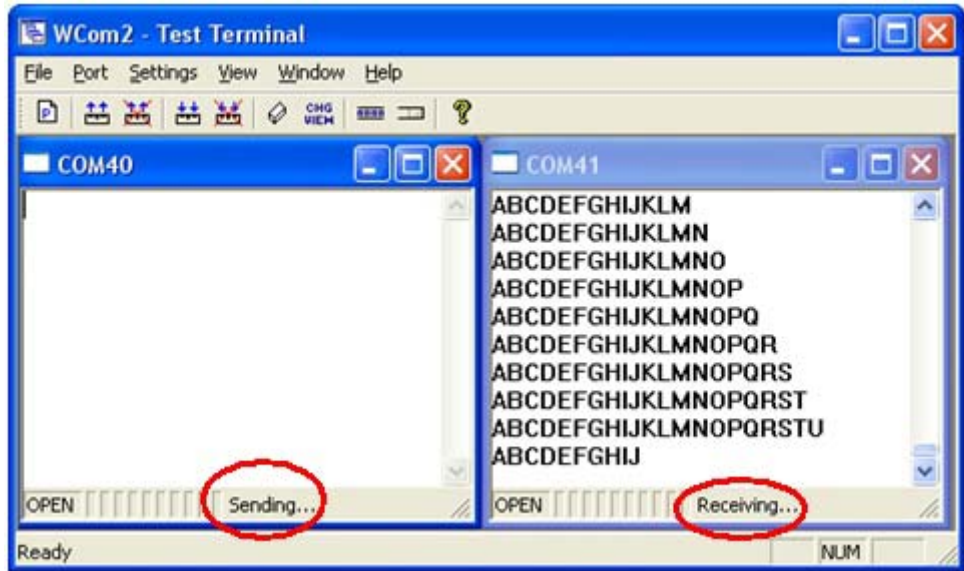


Both COM ports show *Ready* on the status bar.



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

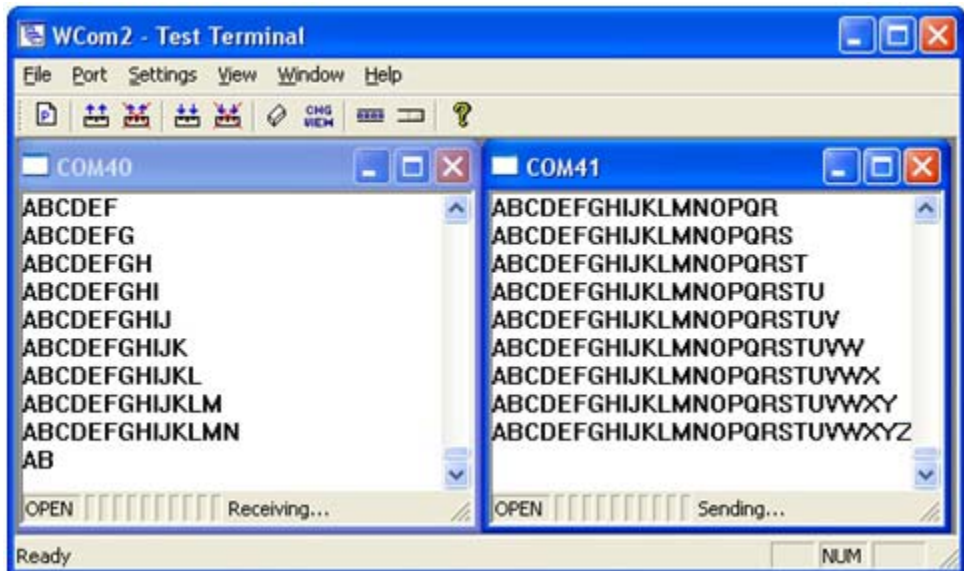
- Right-click the OPPOSITE window and click Send.



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

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

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



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

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

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

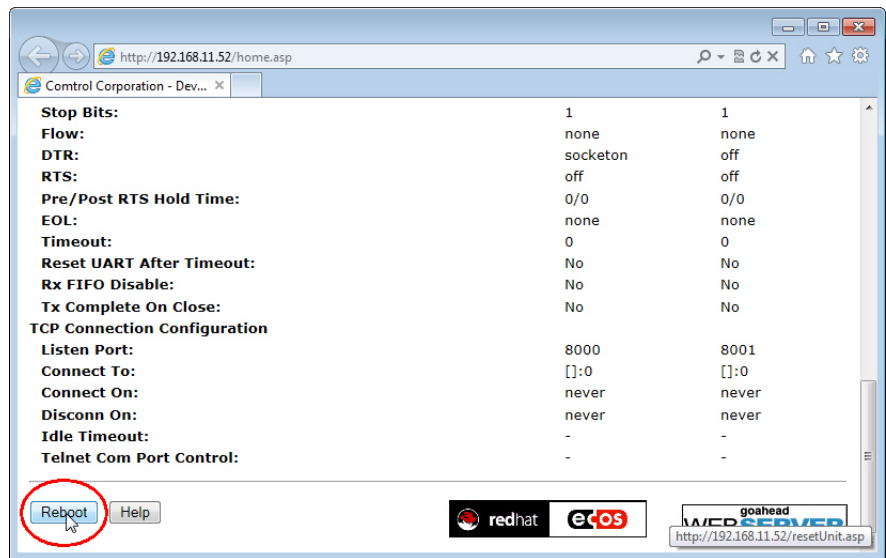
Data is now scrolling in the COM40 window. COM41 is static as it is not receiving data but transmitting data.

Socket Mode Serial Port Testing

This procedure illustrates using 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 [Saving a SocketServer Configuration File](#) on Page 77.

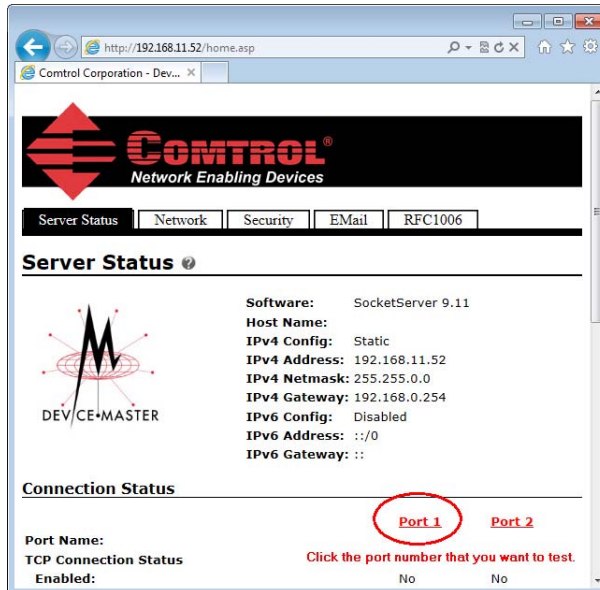
1. If necessary, install PortVision DX using [Installing PortVision DX](#) on Page 15 and scan the network to locate the DeviceMaster LT that you want to test.
2. Right-click the DeviceMaster LT and click **Webpage**.
3. Scroll to the bottom of the home page and click **Reboot**.



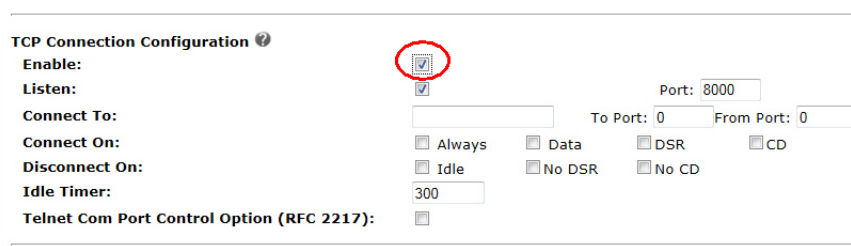
4. Click the **Set configuration for all ports to factory default settings** option and then click the **Yes Reboot** button.



- If necessary, re-open the web pages and click on the port that you want to test. The following example tests Port 1.

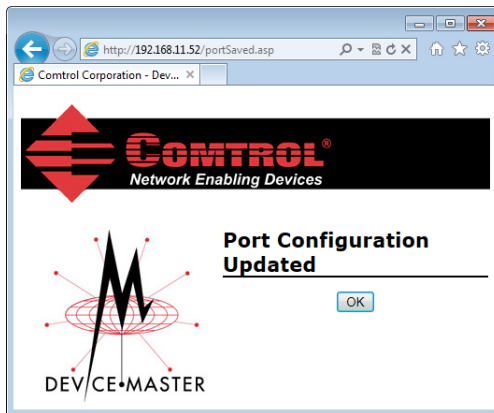


- Scroll down *TCP Connection Configuration* options, click the **Enable** option, and leave all other settings on this page at their default values.

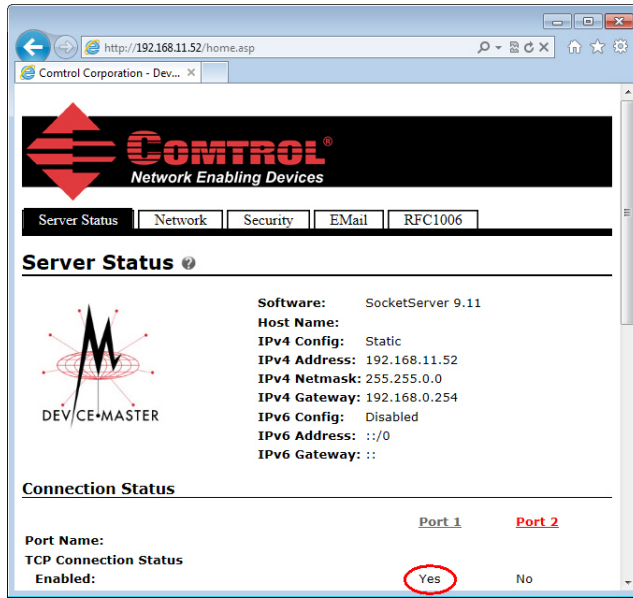


Note the Port number as it is needed later in this procedure. In this example, the port number is 8000.

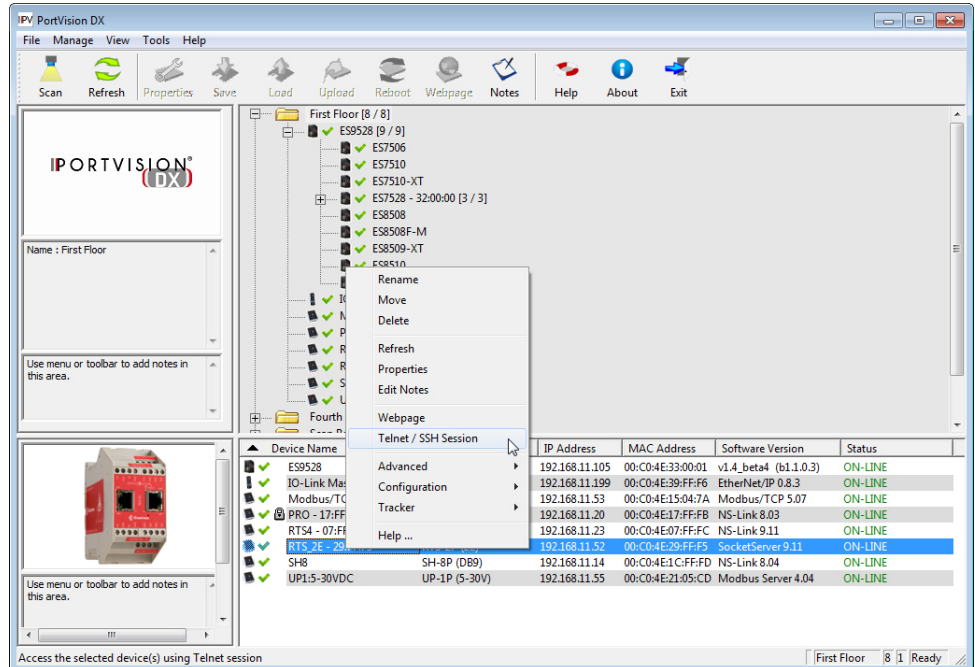
- Scroll to the bottom of the page and click the **Save** button.
- Click **Ok** when the *Port Configuration Updated* page appears.



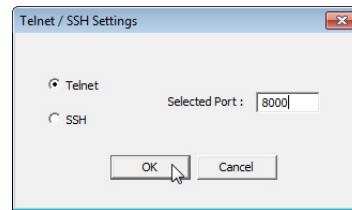
- Verify that the port has been enabled.



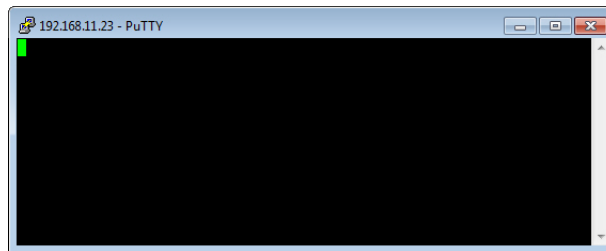
- Leave the web page open.
- Attach the loopback plug that was shipped with the DeviceMaster LT to the serial port of the DeviceMaster LT. See [Connecting Serial Devices](#) on Page 65 if you need to build a loopback plug.
- Right-click the DeviceMaster LT in the *Device List* pane and click **Telnet / SSH Session**.



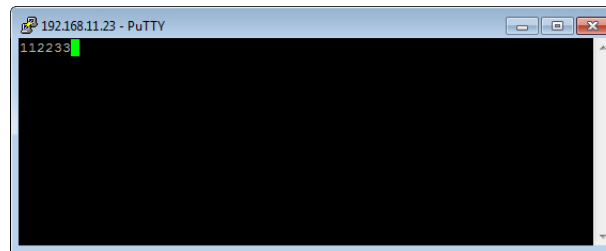
13. Enter the socket number of the port that you are testing ([Step 6](#)) and click **Ok**.



PuTTY loads.

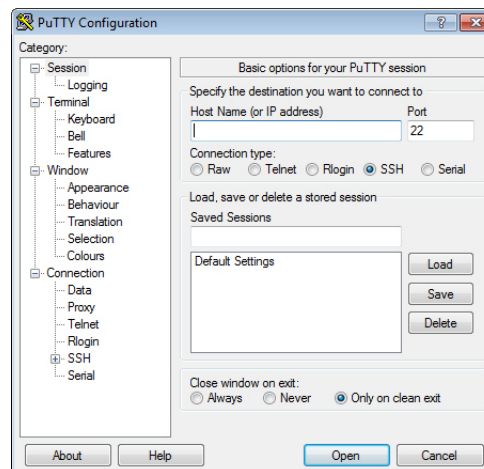


14. Type 123.

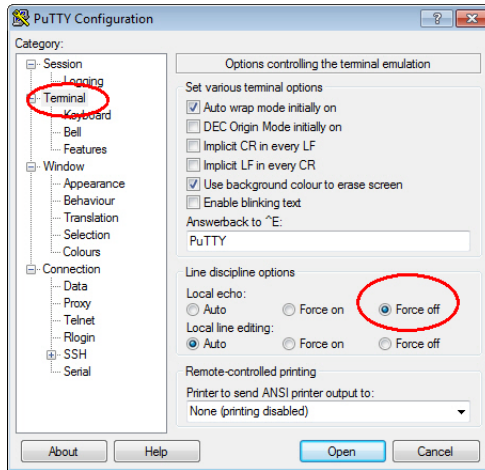


If 112233 displays, you need to disable local echo. Use the following steps to disable local echo.

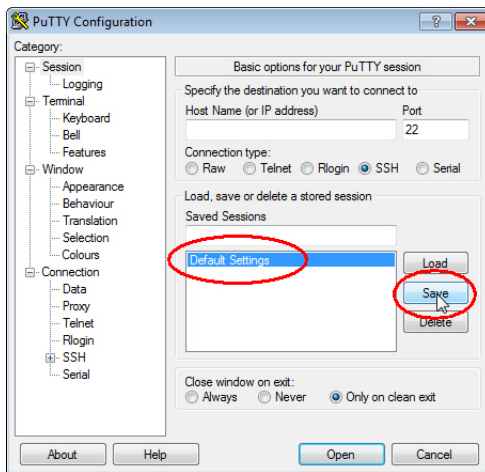
- Go to `c:\Program Files (x86)\Control\PortVision DX`.
- Execute **PUTTY.EXE** to open the application.



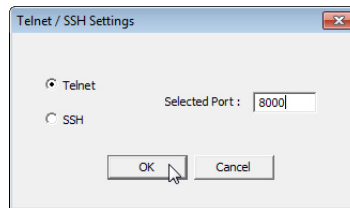
- c. Click **Terminal** and click **Force off** for the *Local echo* option.



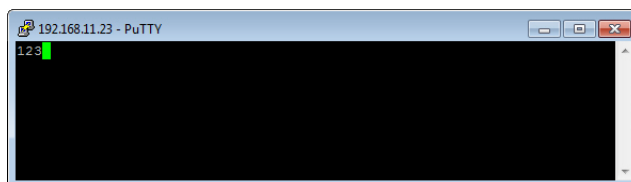
- d. Return to the **Session** menu, highlight **Default Settings** and then click **Save**.



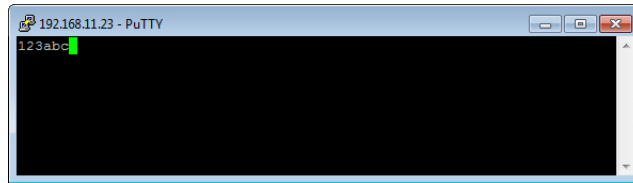
- e. Click **Cancel** to close PuTTY.
- f. Close the telnet (PuTTY) session that you opened from PortVision DX.
- g. Re-open the telnet session by right-clicking the DeviceMaster LT, and select the **Telnet / SSH Session** option.
- h. Enter the Socket Port number and then click **Ok**.



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



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



17. If you want to test additional ports, simply repeat this procedure on that port or ports.
18. 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 130

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
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 Control after obtaining an return material authorization (RMA) so that Control 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 43 [Connecting Serial Devices](#) on Page 65 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.
5. At the **RedBoot>** prompt, type **dis**, and press **Enter**.

Note: *If you do not disable the loading feature of*

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

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 Control for re-flashing.

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

Note: If necessary, see [Installing PortVision DX](#) on Page 15.

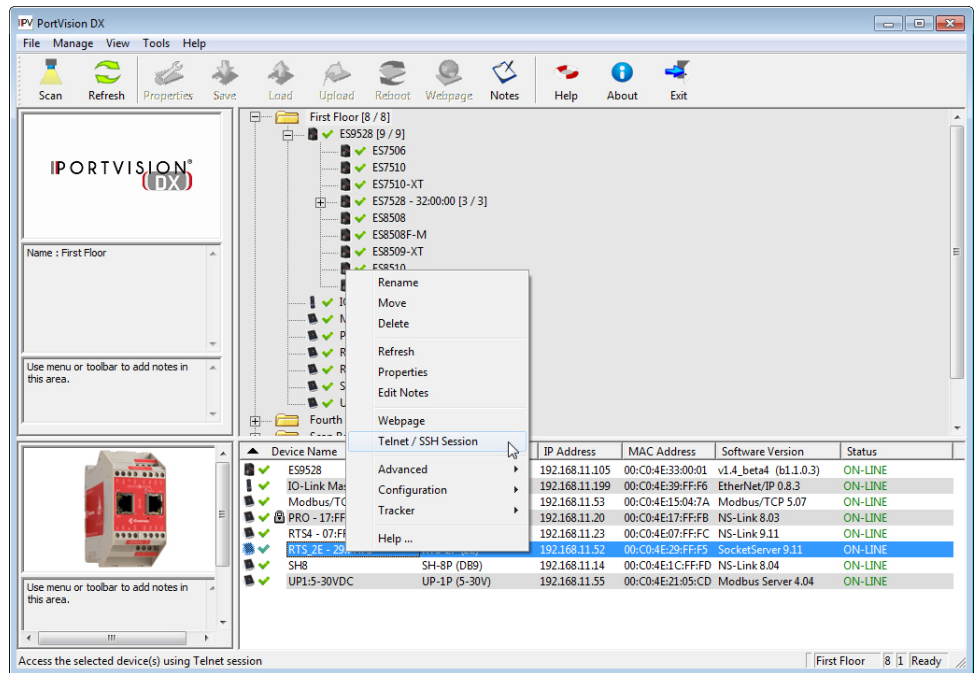
11. Open PortVision DX.
12. Scan the network so that PortVision DX discovers the DeviceMaster LT.
13. Right-click the DeviceMaster LT and then click **Telnet/SSH Session**.

```

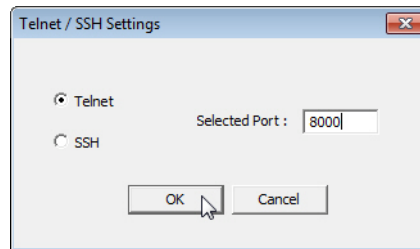
RedBoot> dis
Loading disabled
RedBoot> password
Cleared
RedBoot> auth none
Auth: none
RedBoot> IP

IP:      192.168.11.40
Mask:    255.255.255.0
Gateway: 192.168.11.1

RedBoot> timeout 15
Timeout 15 seconds
RedBoot>
    
```



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



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

```

192.168.11.40 - PuTTY
Password:
Control 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 100 ([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 135
- [Web Server Access](#) on Page 135

Telnet Access

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

Note: To reset authentication, see [Serial Port Access](#) on Page 135 or use the [RedBoot Command Overview](#) on Page 107.

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 100. 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 135 or use the [RedBoot Command Overview](#) on Page 107.

To reset the password, see [Configuring Passwords](#) on Page 106 or [Telnet Access](#) on Page 134.

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

	Security Configuration	
a. Verify that the Enable Secure Data Mode option is not checked.	Enable Secure Data Mode	<input type="checkbox"/>
b. Verify that the Enable Secure Config Mode option is not checked.	Enable Secure Config Mode	<input type="checkbox"/>
c. Verify that the Enable Telnet/SSH option is checked.	Enable Telnet/ssh	<input checked="" type="checkbox"/>
d. Verify that the Enable Monitoring Secure Data via Telnet option is not checked.	Enable Monitoring Secure Data via Telnet	<input type="checkbox"/>
e. Verify that the Enable SNMP option is checked.	Enable SNMP	<input type="checkbox"/>
- 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.

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