



TIGHTROPETM
m e d i a s y s t e m s

Installation Guides

©Tightrope Media Systems

November 1, 2005

Contents

| | |
|---|-----------|
| 1 Quick Start: Everything You Need To Know in Four Pages | 9 |
| 1.1 Introduction | 9 |
| 1.2 Identifying the Servers | 9 |
| 1.3 Passwords | 10 |
| 1.4 Before Power Up: A Note About the Video Output | 10 |
| 1.5 Configuring the Network Settings | 10 |
| 1.6 Network Ports | 10 |
| 1.7 Accessing from the Outside | 11 |
| 1.8 Identifying Serial Ports | 11 |
| 1.9 The IR4 | 11 |
| 1.10 Configuring Carousel Players | 11 |
| 1.11 Configuring Video Servers and Encoders | 12 |
| 1.12 Configuring VOD and LIVE Streaming Servers | 12 |
| 2 Introduction | 13 |
| 2.1 Welcome | 13 |
| 2.2 What Does This Guide Cover? | 13 |
| 2.3 Conventions Used In This Guide | 14 |
| 2.4 About Tightrope | 15 |
| 3 Hardware Installation | 17 |
| 3.1 Unpacking the Server | 17 |
| 3.2 Server Connections | 18 |
| 3.2.1 The Two Rack-Unit Chassis | 18 |
| 3.2.2 The Three Rack-Unit Chassis | 20 |
| 3.2.3 The VS4-Series Breakout Box | 21 |
| 3.2.4 The STRM-Live Breakout Box | 22 |
| 3.3 First Steps for a Cablecast or Carousel System | 22 |
| 3.3.1 Mounting | 22 |
| 3.3.2 Connecting the Video Outputs | 22 |
| 3.3.3 Connect Serial Devices | 23 |

| | | |
|----------|--|-----------|
| 3.3.4 | Power Up the Server | 23 |
| 3.3.5 | Configure the Network Settings | 23 |
| 3.3.6 | Set the System's Time | 23 |
| 3.4 | Installing Rack Rails | 24 |
| 3.5 | Installing Video Servers, Carousel Players and Other Tightrope Servers | 25 |
| 3.5.1 | Carousel Players | 25 |
| 3.5.2 | VS4-Series and ENC-Series Servers | 26 |
| 3.5.3 | STRM-VOD Servers | 26 |
| 3.5.4 | STRM-Live Servers | 27 |
| 4 | Network Configuration | 29 |
| 4.1 | Introduction | 29 |
| 4.2 | Ramblings About Tightrope Servers Over Multiple Networks | 29 |
| 4.3 | Discovering a Computer's Name | 30 |
| 4.4 | Setting the IP Address of a Server | 30 |
| 4.5 | Network Ports | 32 |
| 4.6 | Making Email Work | 36 |
| 4.7 | Making the Weather Plug-in Work | 37 |
| 4.8 | Making Network Time Synchronization Work | 37 |
| 4.9 | Almost All About How To Access The System From Home | 37 |
| 4.10 | How to Make Video Servers and Carousel Players Talk Between Networks | 38 |
| 5 | Carousel Display Engine Video and Setup | 41 |
| 5.1 | Introduction | 41 |
| 5.2 | TV Output | 41 |
| 5.2.1 | Enabling the TV Output | 41 |
| 5.2.2 | Adjusting the TV Output Settings | 43 |
| 5.2.3 | But My Video Is Black and White! | 43 |
| 5.3 | Adjusting the Video Resolution | 43 |
| 5.3.1 | Standard Resolution Adjustments | 45 |
| 5.3.2 | Custom Monitor Adjustments | 45 |
| 5.3.3 | Setting up a 9x16 Display | 48 |
| 6 | Frontdoor Server Settings | 51 |
| 6.1 | Introduction | 51 |
| 6.2 | Logging into the Frontdoor Server | 51 |
| 6.3 | The Frontdoor Main Menu | 52 |
| 6.4 | Changing Your Password | 53 |
| 6.5 | Server Setup | 54 |
| 6.5.1 | Server Setup: Site Name | 54 |
| 6.5.2 | Server Setup: Server Security | 56 |
| 6.5.3 | Server Setup: Mail Settings | 56 |
| 6.5.4 | Server Setup: Time Settings | 58 |
| 6.5.5 | Server Setup: Database Tools | 60 |

| | | |
|----------|--|-----------|
| 7 | Connecting Serial Ports—Cablecast Installations | 63 |
| 7.1 | Introduction | 63 |
| 7.2 | 8-Port Serial Cards | 63 |
| 7.3 | Quatech USB-Serial Converters | 64 |
| 7.3.1 | Third Party USB-Serial Converters | 66 |
| 7.4 | Discovering and Reassigning COM Port Assignments | 66 |
| 7.5 | The Serial Port Tester Application | 68 |
| 7.6 | Changing the 422-232 Configuration on PCI422-232-8PT Cards | 71 |
| 7.7 | A Note About Serial Cables | 72 |
| 8 | The CBL-IR4 | 73 |
| 8.1 | Introduction | 73 |
| 8.2 | Installing the IR4 | 74 |
| 8.3 | Learning IR Commands | 74 |
| 8.4 | Configuring Cablecast | 76 |
| 8.5 | Testing the Control | 77 |
| 9 | The VS4 and ENC Series Video Servers | 79 |
| 9.1 | Introduction | 79 |
| 9.2 | Environmental Considerations | 79 |
| 9.3 | How does Cablecast Communicate with the Server? | 80 |
| 9.4 | Cablecast Setup for the VS4 and ENC Servers | 80 |
| 9.5 | Maintaining the Video Server Storage RAID | 88 |
| 9.5.1 | Determining if Your RAID Has Been Degraded | 88 |
| 9.5.2 | Configuring Email for 3ware controllers | 88 |
| 9.5.3 | Rebuilding the Array | 90 |
| 9.5.4 | Checking Drive Connections | 93 |
| 9.5.5 | Replacing Bad Drives | 93 |
| A | Cablecast Device Control List | 95 |
| A.1 | Denon DVD2900 | 95 |
| A.2 | For Digital Rapids Encoders | 95 |
| A.3 | VS4 Series Video Servers | 96 |
| A.4 | Extron MAV Series Routing Switchers | 96 |
| A.5 | JVC SR-S365U SVHS VTR | 96 |
| A.6 | 8 I/O and Lower Knox RS Series Routing Switcher | 97 |
| A.7 | 16 I/O and Higher Knox RS Series Routing Switchers | 97 |
| A.8 | Knox Pro Switch Series Routing Switchers | 97 |
| A.9 | Leitch Routers (Terminal and Passthru Protocols) | 98 |
| A.10 | Leightronix Mini-T Pro | 98 |
| A.11 | Leightronix MVP-2000 | 99 |
| A.12 | Leightronix Pro 8 | 99 |
| A.13 | Leightronix Pro 16 | 100 |

| | |
|--|------------|
| A.14 Leightronix TCD-1000 | 100 |
| A.15 Leightronix TCD-IP | 101 |
| A.16 Panasonic 232 Protocol Devices (AG7100, 7150, etc.) | 101 |
| A.17 Pioneer DVDV7400 and V5000 | 102 |
| A.18 Pioneer DVDV7400 and V5000 | 102 |
| A.19 Pioneer DV-F07 | 102 |
| A.20 Sierra SVS Series Routing Switchers | 102 |
| A.21 Sigma Routing Switchers | 103 |
| A.22 Sony DVP-CX777ES | 103 |
| A.23 Tascam DVD6500 DVD Player | 103 |
| A.24 Tightrope 422 Control | 103 |
| A.25 Cable Pin-Out Diagrams | 105 |
| A.25.1 RS-232 9-Pin Serial Cable: Straight-Thru | 105 |
| A.25.2 RS-232 9-Pin Serial Cable: Null-Modem | 106 |
| A.25.3 RS-232 9-Pin Serial Cable: Sierra Routers | 107 |
| A.25.4 RS-422 9-Pin Serial Cable: With Internal PCI Serial Cards | 108 |
| A.25.5 RS-422 9-Pin Serial Cable: With Multi-Port USB-Serial Converters | 109 |
| A.25.6 RS-232 9-Pin to 15-Pin Serial Cable: For Most Pioneer | 110 |
| A.25.7 RS-232 9-Pin to 25-Pin Serial Cable: For Leightronix Pro 8/16 | 111 |
| B A Not-So-Short Introduction to Networking | 113 |
| B.1 Introduction | 113 |
| B.2 The Basics: What is a Network? | 113 |
| B.2.1 IP Address | 115 |
| B.2.2 Subnet Mask | 115 |
| B.2.3 Network Router | 116 |
| B.2.4 Domain Name System (DNS) Address | 117 |
| B.2.5 Summary of Basic Network Concepts | 119 |
| B.3 Dynamic Addresses and DHCP | 119 |
| B.4 TCP and UDP Glossed Over | 120 |
| B.5 Network Ports | 121 |
| B.6 Private and Public IP Addresses | 122 |
| B.7 Network Address Translation | 123 |
| B.8 Firewalls | 125 |
| B.8.1 Dire Warning About Firewalls | 126 |
| B.9 Port Forwarding | 126 |
| B.10 Virtual Private Network | 127 |
| B.11 How Do I Access Cablecast or Carousel From Home? | 127 |

| | |
|--|-----|
| B.11.1 Option 1: Hang It Out On the Internet | 128 |
| B.11.2 Option 2: Use Port Forwarding | 128 |
| B.11.3 Option 3: Use VPN | 129 |
| B.11.4 The “Forget the IT Department” Option | 129 |
| B.12 Avoiding The Tyranny of Cable Modem Providers | 130 |
| B.12.1 Dynamic DNS | 130 |
| B.12.2 Change Your Port Number | 131 |
| B.13 Time Synchronization, UDP and NAT | 131 |
| B.14 Summary | 133 |

Chapter 1

Quick Start: Everything You Need To Know in Four Pages

1.1 Introduction

If you are an experienced installer and knowledgeable about networking, this section may be all that you need. It is designed to have all of the critical information needed to install your Tightrope servers.

1.2 Identifying the Servers

If you are unpacking multiple servers, you need to identify each server by looking at the box that it came in. On it, you will find a product number. The most important server to locate is the Cablecast (for Cablecast customers) or Carousel server. Their part number will be any of the following: **“CBL-Cablecast”**, **“CBL-Cablecast-Pro”**, **“CBL-Cablecast-Bundle”**, **“CAR-Carousel”**, **“CAR-Carousel-Pro”**.

See chapter 3 on page 17 for connection diagrams.

Hereinafter, your Cablecast/Carousel machine will be referred to as the “main server”.

1.3 Passwords

Every single password in your system has been set to “trms”. This includes both the software and the Administrator password for Windows. You will want to change this before you are finished.

1.4 Before Power Up: A Note About the Video Output

If you intend to use the composite video output, do not power up the server or any Carousel Players without **first** plugging in a video monitor (or other 75Ω load). If you do, the driver will automatically turn the video output off and you’ll have to visit chapter 5 on page 41 to learn how to turn it back on.

1.5 Configuring the Network Settings

The main server requires a static IP address. VS4-Series video servers, ENC-Series encoders and Carousel Players may use dynamic addresses, provided that you reference them using their Windows Network name. Usually this will be something like “**VS4-1000E-1001**”. If all of your servers shipped together, Cablecast is most likely configured to address any video servers or encoders in this way.



If you do not provide static address to all of your servers, you will *need* to address them using Windows Networking names. Therefore, it is sometimes simpler to get static addresses for all of the servers. That way, even if you join these computers to a domain, the address will still remain valid.

1.6 Network Ports

Tightrope servers communicate with other computers for various required services, such as email, time synchronization, RSS data, weather information and communicating with other servers.

See section 4.5 on page 32 for a chart of required ports.



Remember, you only need to poke a hole through the firewall if: A) you have the products listed in the charts in [4.5](#), and B) you want the services described, and C) the computers that are communicating with each other are on separate networks.

If this is confusing see the appendix on networking in appendix [B](#) on page [113](#) and chapter [4](#) on page [29](#), which is about setting up your Tigtrope servers.

1.7 Accessing from the Outside

As mentioned in the previous section, if you wish to access the main server from outside your network, you will need to have your IT department port-forward TCP port 80 to your main server. You may set IIS on the main server to a higher port if this simplifies things.

For more information see chapter [4](#) on page [29](#).

1.8 Identifying Serial Ports

Locate the yellow card-stock paper with the title “*Serial Port Configuration for This Server*”. On it you will see a picture of two servers, one of which matches yours. Your server will have 0-4 8-port serial cards installed. Consult the diagram and the table below it when configuring Cablecast.

If you need to switch a port between RS-232 and RS-422, see section [7.6](#) on page [71](#).

1.9 The IR4

See chapter [8](#) on page [73](#) for instructions on programming the IR4.

1.10 Configuring Carousel Players

When the Display Engine boots, a splash screen appears with a “**Configure**” button. Click it before the counter runs down to ‘0’. Enter the address into the “**Carousel**

Server” field. Enter the channel number that you want this display engine to point at¹.

Typically, the monitor offset will be zero, as most players do not have two monitors. If yours is different, see the full text on this subject in chapter 5 on page 41.

1.11 Configuring Video Servers and Encoders

See section 3.5.2 on page 26 for information about connecting the VS4-Series breakout box and connecting the audiovisual inputs for both the VS4-Series servers and the ENC-Series encoders.

Cablecast addresses these video servers and encoders through the network either by their IP address or their network name. Therefore, no additional configuration is necessary beyond marking the unit’s address information for entry into Cablecast².

1.12 Configuring VOD and LIVE Streaming Servers

Apart from connecting the audiovisual connections, covered in section 3.5.3 on page 26, the STRM-VOD and STRM-LIVE Series servers come pre-configured. Like the VS4-Series servers, the Cablecast machine usually comes shipped with the network name of these servers pre-entered. All quality and control settings for these servers is handled through Cablecast’s web interface.

For further details, see the Cablecast Guide or call Tightrope technical support.

¹Channels are enumerated in Carousel in ascending order starting from 1. The left most tab is channel 1, and so on.

²Often, the network name is entered into Cablecast before the unit ships. Unless you change this name or wish to address the machine via its IP address, you can simply leave this setting alone.

Chapter 2

Introduction

2.1 Welcome

Thank you for purchasing products from Tightrope Media Systems! We have worked hard to make your new system versatile, easy to use and reliable.

2.2 What Does This Guide Cover?

This guide covers the installation and maintenance of Tightrope's entire family of servers. These include:

Carousel Web-centric digital signage system

Carousel Pro High-availability and high-capacity digital signage for enterprise applications

Carousel Player Carousel channel player

Cablecast Web-centric audiovisual head end management system

Cablecast Pro High-availability channel automation system for multi-location systems

VS4 Series Video Servers 4-channel decode, 1-channel encode MPEG-2 video servers for Cablecast

ENC Series Encoders MPEG-2 Encoders for Cablecast

STRM-LIVE IP Video Encoder Real-time encoder for IP channel streaming

STRM-VOD Series IP Video On Demand Server Video On Demand server for Cablecast

This guide will step you through the process of installing, configuring and maintaining the systems listed above. Topics include:

- Hardware installation and connections
- Network requirements and configuration
- Configuring Carousel's video output
- Serial port configurations for Cablecast
- Configuring the IR4 four-port IR controller
- Configuring Video Servers
- Backing up the data on your systems



Detailed software setup is covered in the Cablecast and Carousel documentation.

In addition, you'll want to check out the appendix of this guide, as it contains helpful background information about networking, Pin-Out diagrams and answers to frequently asked questions.

2.3 Conventions Used In This Guide

Throughout this guide, the following conventions will be used:



This is a note. Notes are used to call attention to special information that may be helpful to keep in mind.



This is a warning. Warnings call attention to actions that may result in unforeseen consequences, such as batch functions that delete large amounts of data or configurations that might have network security implications.



This is a tip. Tips show unique ways to use the software, and tricks that have been picked up by other users.

When the text references a particular menu item, field or label within the software, that text will be quoted in bold.

Example: Click on the "**Main Menu**" button.

When the text references user input, "this format" will appear.

Example: When logging into Front Door from the main server, enter "localhost" into the browser's address field.

When quotes are used, do not include them in your input unless specifically told to.

When it is necessary to navigate to a menu, this documentation will represent each menu level with a colon (":").

2.4 About Tightrope

Tightrope Media Systems is a manufacturer of web centric media delivery and display systems. We strive to provide integrated solutions designed specifically for the markets we choose to address, with a web centric interface as a core design of everything we do.

For more information on Tightrope Media Systems, please visit our web site: www.trms.com

Email us at: info@trms.com

Our Address is:

Tightrope Media Systems
800 Transfer Road, Suite 17
Saint Paul, Minnesota 55114

For customer service, please contact your dealer or:

Customer Support Email: support@trms.com

Support Forum: <http://forum.trms.com>



This forum requires a free registration.

Phone Number: (866) 866-4118 / (612) 866-4118 ext. 255

Chapter 3

Hardware Installation

3.1 Unpacking the Server

Cablecast and Carousel servers are shipped in one box, which includes:

- This guide on CD-ROM
- The 2-Rack unit or 3-Rack unit computer
- A standard PC keyboard
- A standard PC mouse
- Power Cord
- The Microsoft Windows XP Professional Installation CD
- The motherboard's driver disk
- One or more 8-Port serial card breakout cable(s)—*optional*
- Serial Port Loopback Adaptor—*Cablecast servers only*
- Rack rails—*3RU Servers Only*

Video servers will include a separate box with the 1-rack unit breakout box and two high-density audiovisual cables.

Video servers and encoders will include a bag of adaptors for the encoder card. It includes (2) 1/8 inch to two RCA adaptors and a RCA to BNC adaptor.

The STRM-LIVE series server ships in two boxes with the breakout box shipped apart from the server.

3.2 Server Connections

Tightrope has standardized on two computer platforms that the company uses to build all of its hardware: the two (2) rack-unit machine (2RU) and the three (3) rack unit machine (3RU). The three 3RU chassis comes in two varieties: one for the Carousel and Cablecast Pro systems and one for the VS4-Series video servers¹.

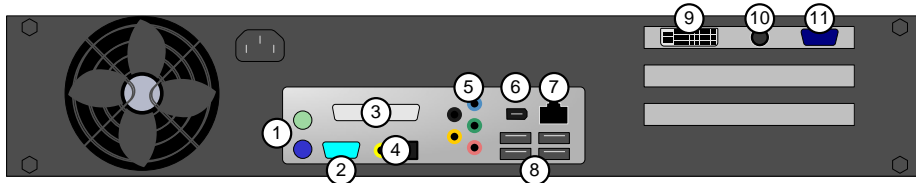
The 2RU is used for the following equipment:

- Cablecast
- The Cablecast Bundle
- Carousel
- The Carousel Player

The 3RU is used for the following equipment:

- Cablecast Pro
- The VS4-Series Video Servers
- The ENC-Series MPEG-2 Encoders
- Carousel Pro

3.2.1 The Two Rack-Unit Chassis



1. Keyboard / Mouse (PS/2 Style)
2. RS-232 (9-pin male Connector)
3. Parallel (*unused*)
4. Digital audio out (Coaxial S/PDIF (RCA female) and Optical (TOSLINK))
5. Analog audio connectors (1/8 female connector):
Black Rear left/right out (*unused*)
Yellow Center/Low frequency effects (LFE) out (*unused*)

¹The difference between them is not material for the configuration process, as both chassis have the same dimensions. It is only mentioned here because the front of each chassis looks different.

Blue Line in left/right

Green Line out left/right

Red Mic in (*unused*)

6. Firewire IEEE 1394 (6-Pin male)
7. Ethernet 10/100 (RJ45 female)
8. USB 2.0 × 4 (male, keyboard and mouse compatible)
9. DVI Connector (female, dual channel)
10. Composite Video Output (female, RCA)
11. VGA (HD 15 Pin female)

Physical and Electrical Properties

Width 19 inches; rack ears included

Height 3.5 inches (two rack units)

Depth 21 inches; rails are not required and not included; *rails are required for shipping in rack cabinet*

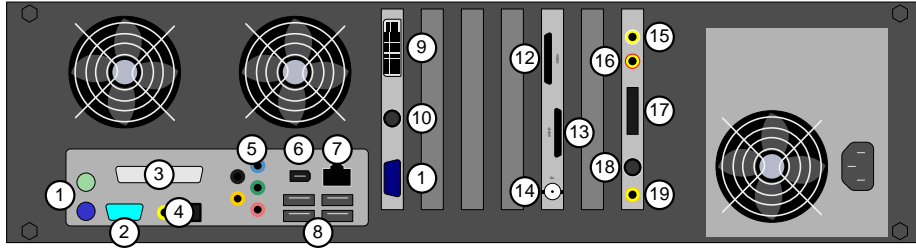
Shipping Weight Approximately 40 lbs, configuration dependant.

Ventilation Left side, front and back are vented. Top and bottom are not vented.

Ambient Operating Temperature +50 - +78 degrees Fahrenheit

Maximum Power Consumption Less than 250 watts; 180 watts average

3.2.2 The Three Rack-Unit Chassis



1. Keyboard / Mouse (PS/2 Style)
2. RS-232 (9-pin male Connector)
3. Parallel (*unused*)
4. Digital audio out (Coaxial S/PDIF (RCA female) and Optical (TOSLINK))
5. Analog audio connectors (1/8 female connector):
 - Black** Rear left/right out (*unused*)
 - Yellow** Center/Low frequency effects (LFE) out (*unused*)
 - Blue** Line in left/right
 - Green** Line out left/right
 - Red** Mic in (*unused*)
6. Firewire IEEE 1394 (6-Pin male)
7. Ethernet 10/100/1000 (RJ45 female)
8. USB 2.0 x 4 (male, keyboard and mouse compatible)
9. DVI Connector (female, dual-channel)
10. Composite Video Output (female, RCA)
11. VGA (HD 15 Pin female) optcbl
12. Multi-channel MPEG video out (included custom cable, 3 inches)
13. Multi-channel MPEG audio out (included custom cable, 3 inches)
14. Genlock in (all MPEG channels lock to this source, BNC female)
15. Encoder audio input **left** (RCA female)
16. Encoder audio input **right** (RCA female)
17. Four channel audio in (included pigtail cable, 4 XLR female)
18. Encoder video input (S-Video, Mini)
19. Encoder video input (composite, RCA female)

Physical and Electrical Properties

Width 19 inches; rack ears included

Height 5.25 inches (three rack units)

Depth 29 inches; rails are required and included

Shipping Weight Approximately 70 lbs, configuration dependant.

Ventilation Front and back are vented. Top and bottom are not vented.

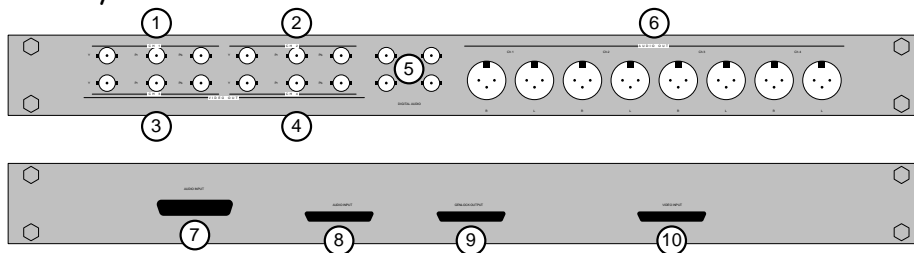
Ambient Operating Temperature +40 - +78 degrees Fahrenheit

Maximum Power Consumption Less than 350 watts; 220 watts average

Redundant Power Option Servers ordered with the redundant power supply require two power outlets.

3.2.3 The VS4-Series Breakout Box

Front / Back



1. MPEG video output **channel 1** (BNC female x 3: Y/P, Pr, composit/Luma/Pb)
2. MPEG video output **channel 2** (BNC female x 3: Y/P, Pr, composit/Luma/Pb)
3. MPEG video output **channel 3** (BNC female x 3: Y/P, Pr, composit/Luma/Pb)
4. MPEG video output **channel 4** (BNC female x 3: Y/P, Pr, composit/Luma/Pb)
5. Digital audio pass-through (BNC female, genlock mode not supported)
6. MPEG audio output (XLR male, outputs 1-4 alternate left-right)
7. *unused*
8. Audio input from server (included 50-pin HD cable)
9. *unused*
10. Video input from server (included 50-pin HD cable)

3.2.4 The STRM-Live Breakout Box

Front / Back



1. Audio Input (XLR female)
2. Audio Input (RCA female)
3. Video Input (S-Video female, BNC female)

Each breakout box can handle two STRM-LIVE servers.

3.3 First Steps for a Cablecast or Carousel System

3.3.1 Mounting

If the server is a 2RU machine, install the system in its rack. Connect the supplied keyboard and mouse to the appropriate connectors on the back.

If the server is a 3RU machine, consult section 3.4 on page 24 for information on installing the required rack rails prior to mounting the server in your rack.



Do not plug the unit's power in at this step. Since the machine automatically turns on when power is supplied, plugging it in will boot the system. This will reset the system's video settings.

3.3.2 Connecting the Video Outputs

If you are connecting Carousel to an NTSC or PAL video system, you will use the video output connector, marked '10' in sections 3.2.1 and 3.2.2 on page 18.

If you are using a VGA distribution system, then you will use the system's VGA connector, marked '2' in the same diagrams.

Connect it to your video distribution system or routing switcher at this time. If you are using the video output, you may also connect a VGA monitor² for maintenance

²Not included.

purposes³.



If your video distribution system or routing switcher is not yet ready, you may wish to temporarily install a 75Ω terminator on the server's video output. This will force the system to recognize a television connected to its output and prevent you from having to reconfigure the output later. Reconfiguring the video output is covered in chapter 5 on page 41.

3.3.3 Connect Serial Devices

The next step is to connect your serial devices. If you have more than one serial device in your installation, consult chapter 7 on page 63.

If you have only one device that is controlled via serial port, connect it to the Cablecast unit and note that it will be addressed as "1" in Cablecast.

3.3.4 Power Up the Server

Plug the power cable into the unit. If the unit does not power up automatically, press the power button on the front.

Once the system boots, it will automatically start the Carousel Display engine, if Carousel is installed. To stop it, click the "cancel" button when the Carousel splash screen appears.

3.3.5 Configure the Network Settings

Connect the system to your network using the Ethernet port ('7') on the back of the server. This server *requires* a static IP address. See chapter 4 on page 29 for details on how to set the IP address in Windows XP and 2003.

3.3.6 Set the System's Time

All Tightrope servers will automatically attempt to synchronize their system clock using the Network Time Protocol (NTP). At this point, we'll assume that this is working and only worry about setting the time zone.

³The VGA and video output ports are active at the same time and display the same video. It's sometimes nice to have a VGA monitor when performing maintenance on the server, as it has a clearer text display

From the server's desktop, double-click on the time in the lower right of the screen⁴. This will open the “**Date and Time Properties**” dialog box. Click on the “**Time Zone**” tab to reveal the windows shown in figure 3.1.

Select your time zone from the list.



It is important that you set the time zone for all servers, including any Carousel Players, video servers, encoders or streaming servers. We'll cover that later in this chapter.

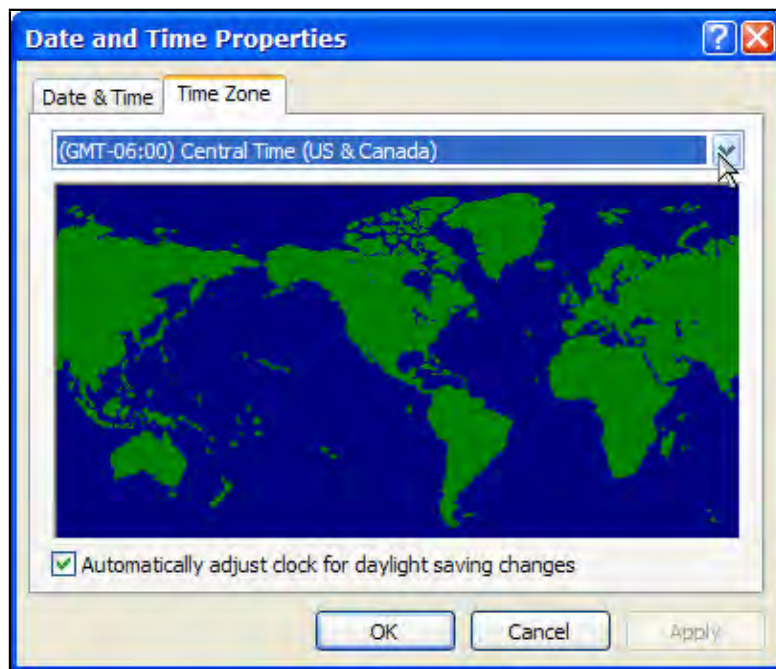


Figure 3.1: Select the time zone that you are in from the pop-down list and “OK”.

3.4 Installing Rack Rails

When mounting servers that are in the 3RU chassis, you must first install the included rack rails.

Each side has a two-piece rail. Install the ‘C’ shaped rail in your rack and install the flat rail to your server, using all of the included screws.

⁴This is region of the screen is called the system tray.

Once the four pieces of the rail are securely installed, you may mount the server in the rack.



These servers are heavy, especially when you are trying to hold them perfectly flat and slide them precisely into the rack rails. This is a job that is best accomplished with two people.

3.5 Installing Video Servers, Carousel Players and Other Tightrope Servers

Setting up additional Tightrope servers is similar to setting up the main server.

Mainly, just plug the keyboard, mouse, VGA and Ethernet cables into each unit.

For units that are running the Carousel Display Engine, be sure to connect the video output before plugging in the power cable, as discussed in section 3.3.2 on page 22 and in detail in chapter 5 on page 41.

For specific information regarding each type of Tightrope server and its networking configuration, read the following sections of this chapter.

3.5.1 Carousel Players

Follow the instructions in section 3.3.2 on page 22 and chapter 5 on page 41 for configuring the player's video output.

Note that you will need to point this server at the main Carousel machine. To do this, click on the “**Configure**” button and enter the address into the IP address into the “**Carousel Server**” field.

As discussed in chapter 5, you will have to ‘point’ this display engine at the desired Carousel channel. When logging into Carousel, you will notice that there are tabs at the top of the user interface. These tabs represent the channels on the Carousel system and they are enumerated from 1 to the number of channels on the server.

Carousel Players do not require a static IP address and may have a dynamic address like any other machine on your network.

See chapter 4 on page 29 for information regarding network port requirements for display engines, especially if you are operating a player that is separated from a Carousel server by a network router.

3.5.2 VS4-Series and ENC-Series Servers

Install the rack rails as discussed in section 3.4 on page 24.

The VS4-Series video servers include a separate 1 rack unit, illustrated in section 3.2.3 on page 21. It includes two cables, one for audio and one for video.

Locate the cable labeled **“Video”** and plug it into the decoder card’s video connector, labeled **“12”** in section 3.2.2 on page 20. Plug the other end into the breakout box, labeled **“10”** in section 3.2.3 on page 21.

Do the same for the cable labeled **“Audio”**, plugging it into the connector labeled **“13”** on the server and **“8”** on the breakout box.

Mount the breakout box on the back of your rack and connect the audio and video inputs to its connectors.



Each video output has three connectors, with the right most being the connector used for composite. Consult the diagram of the breakout box for reference.

For both VS4 and ENC Series servers, the encoder card is located on the right as you are looking at the back of the computer. Consult the diagram in section 3.2.2 on page 20 in determining the audio and video connections.



Be sure that when using XLR connectors that you take care to wire them correctly. If they are not wired correctly, it will often be as though your audio levels are extremely low.

These servers do not require a static IP address, so long as they are addressed by the system’s network name. To learn how to find the server’s network name, see section 4.3 on page 30.

You may wish to give the server a static IP address. To learn how to do this, see section 4.4 on page 30.

3.5.3 STRM-VOD Servers

Install the rack rails as discussed in section 3.4 on page 24.

There are no audiovisual connections for these servers, but they do require a static IP address. See section 4.4 on page 30 for information on assigning a static address.

3.5.4 STRM-Live Servers

Each STRM-Live server includes a breakout box, illustrated in section [3.2.4](#) on page [22](#).

Connect one side of the breakout box to the STRM-Live server.

Each of these breakout boxes is able to handle two STRM-Live servers.

Only connect one source to each side. That is, do not use the composite and S-Video or the XLR and RCA connectors at the same time.

These servers require a static IP address. Consult section [4.4](#) on page [30](#) for information on setting the IP address on this computer.

Chapter 4

Network Configuration

4.1 Introduction

Everything that Tightrope makes is based on a web-centric design. This means that day-to-day operation and most of the configuration of these systems is accomplished through a web browser interface.

As you can imagine, this design requires a network. Configuring your network to use Cablecast and Carousel is at the heart of your installation.

This chapter covers basic setup procedures, such as setting IP addresses. It also covers advanced topics, such as: configuring Carousel and Cablecast to be accessed from outside your network, making Tightrope servers work across networks, joining Tightrope servers to a domain, and many other topics.



If you are new to networking or some are unfamiliar with some of the jargon used in this chapter, please visit [appendix B](#) on page [113](#) for a not-so-short introduction to networking.

4.2 Ramblings About Tightrope Servers Over Multiple Networks

As discussed in [appendix B](#), a network is a pool of IP addresses in the same subnet. If two computers want to talk across two networks, they do it via a network router. In most networks, a router is accompanied by a firewall, which is able to block network traffic on certain TCP or UDP ports. Therefore, considerations must be

made when attempting to configure a system to work across two networks or when attempting to access a system from outside the network.

Specifically, the correct ports must be opened, proxy servers bypassed and holy water sprinkled. If your network is simple, then these issues may be easy to resolve on your own. If you are part of a larger organization, then coordination with your IT department will be important¹.

It is important to understand, however, that simply accessing a Cablecast or Carousel machine from within your network only requires a static IP address, which *should* be easy to obtain. If all of the system equipment is in the same rack and on the same network, no special considerations will need to be made in order for the majority of your system to operate.

4.3 Discovering a Computer's Name

Often, you can address a Tightrope server by its network name. This may be easier than obtaining a static IP address, although it is less reliable since the network name will point the computer at its address and if that address changes, you're at the mercy of Windows Networking and its ability to 'rediscover' the address.

To find the network name:

1. From the Windows desktop, right click on **"My Computer"**. In Windows XP, right click on **"My Computer"** from the **"Start"** menu.
2. Click **"Properties"**.
3. Click the **"Computer Name"** tab at the top.
4. The name to the left of **"Full computer name"** is the name of this computer. (figure 4.1 on the next page)

You can use this name when addressing computers within Cablecast and for Carousel's remote servers list.



It is extremely unlikely that these names will work across networks. If you are using Cablecast or Carousel across a WAN or the Internet, use IP addressing.

4.4 Setting the IP Address of a Server

Cablecast, Carousel, STRM-VOD and STRM-LIVE servers *require* static IP addresses. For all other servers a static address is recommended but optional.

¹Bring cookies.

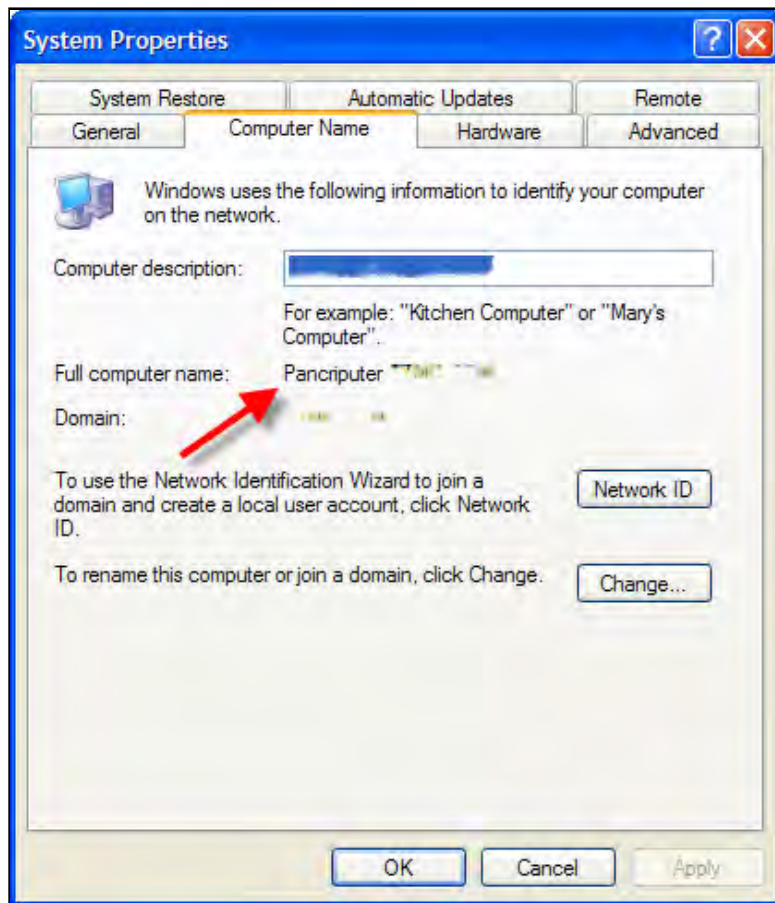


Figure 4.1: The Red Arrow is pointing at this computer's name.

By designating a static address, you may address the machine using its IP address instead of its network name. This gives you some flexibility in how the computer is named². It may even be necessary, especially if your organization uses a domain controller and restricts access to computers outside your domain.

To set the IP address to a static number:

1. From the Windows desktop, navigate to the control panel by clicking on the “**Start**” menu.
2. If the Control Panel is in “category view”, select “**Networking and Internet Connections**”, then click “**Network Connections**”. If the Control Panel is in “classic view”, double-click on the “Network Connections” icon.
3. Right-click on the ‘Ethernet’ icon and select “**Properties**”.
4. Double-click “Internet Protocol (TCP/IP)” to open its properties dialog. (figure 4.2 on the facing page)
5. Flip the radio buttons to “**Use the following IP address**” and “**Use the following DNS server addresses**”.
6. Enter your servers network settings into the provided fields. If you are unsure about the required settings, consult your network administrator or read appendix B on page 113.
7. Click “**OK**” to save your settings.

4.5 Network Ports

As discussed in section B.8 on page 125, the term “outgoing network ports” refers to requests originated from within your network that go to the outside world. They are what make common, desktop network interactions with the Internet possible.

The term “incoming network ports” refers to services that are inside your network that others from the Internet may want to reach. These are a Big Deal from a security and configuration standpoint.

Most often, the outgoing ports that you need to operate Cablecast and Carousel are already open and full use of the system from within your network may be accomplished without any incoming network access.

It is only in these scenarios where incoming network ports must be configured:

- When you want to access Cablecast or Carousel’s web interface from outside your network.

²... useful when joining it to a domain...

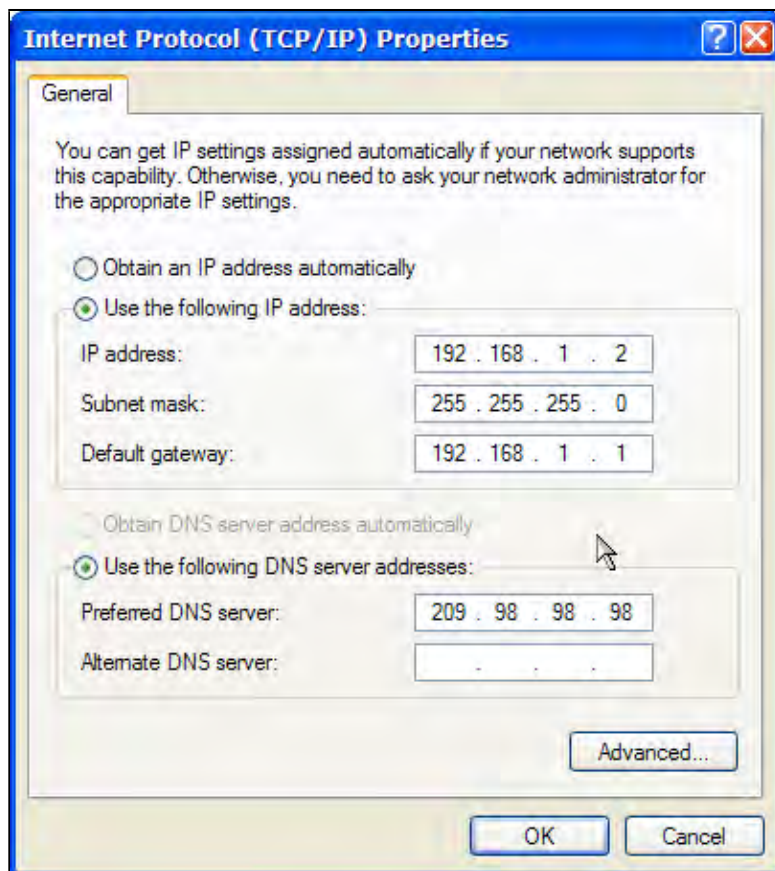


Figure 4.2: This is the TCP/IP settings dialog in Windows.

- You want web traffic to be able to browse your Carousel or Cablecast public web interface³.
- You want to be able to use Cablecast and Carousel's RSS or iCal data output.
- You want Cablecast to control equipment that is located on another network.
- You have remote Carousel display engines that need to access the Carousel server across networks.

³...to see the schedule or current messages...

Study the following tables, which describe the required ports and their usage within a Tightrope system.

Table 4.1: Outgoing Ports: These are ports where the server needs to contact a service outside the network. For a further explanation of incoming versus outgoing ports, see section [B.8](#) on page [125](#).

| Products | Port | Usage |
|-----------------------|---------|---|
| All Tightrope Servers | UDP 123 | NTP Time Synchronization ⁴ |
| All Tightrope Servers | TCP 80 | RSS Reader Plug-in for Carousel; Windows Update |
| Carousel | TCP 25 | Email for Carousel notification; Server must allow relaying for this server |
| Carousel | TCP 21 | Weather plug-in; contacts ftp://tgftp.nws.noaa.gov |

⁴This may be redirected to an internal server.

Table 4.2: Incoming Ports: These are ports where a computer *may* need to contact your from outside your network. For a further explanation of incoming versus outgoing ports, see section [B.8](#) on page [125](#).

| Products | Port | Usage |
|--|----------------------------|--|
| Cablecast, Carousel | TCP 80 | The Front Door user interface ⁵ , RSS Output for Cablecast and Carousel, iCal output from Cablecast |
| Carousel Player, Carousel display engine, Carousel | TCP Ports 56901, 56903, 80 | Any display engine communications; does not support proxy server authentication |
| Cablecast Control Modules | TCP 56700 | Used for computers that have the Cablecast control module package installed, such as VS4-Series Video Servers, ENC-Series Encoders, or any tightrope server with the Cablecast Control Module package installed. |
| DSK Plug-in | TCP 56904 | Communication between Cablecast and the server that is acting as the DSK overlay CG |

4.6 Making Email Work

Follow the steps outlined in section [6.5.3](#) on page [56](#). If you fail to get a test email, ask your email administrator to allow relaying from this server.

⁵This is the key port for accessing Carousel and Cablecast from outside your network.

4.7 Making the Weather Plug-in Work

Of all the outgoing ports that might be blocked, the two most likely are FTP and NTP.

FTP is used for downloading weather information from the National Weather Service. If FTP access is normally blocked and you would like to use this feature, then you need to tell your network administrators to open FTP access to your server. If they want to limit access to a single address, then use the address listed in the table from section 4.5 on page 32. The Weather Plug-In for Carousel works in passive mode, so it will work with network firewalls.

4.8 Making Network Time Synchronization Work

If your firewall does not allow access to network time protocol servers (NTP), then your servers will not be able to synchronize their clocks.

Even without NTP access, multiple servers will periodically synchronize their clocks with the main server. While the main server's clock will not be in sync with the world, the players and video servers in contact with your main server will be in sync with.

If your organization has an internal NTP server, you may use this by entering the servers address into the "**Time (NTP) Server**" field in the "**Time Settings**" form from the main administrator menu. See section 6.5.4 on page 58.

4.9 Almost All About How To Access The System From Home

Cablecast and Carousel operate their user interface from a web server that is included with the system⁶. By default, the web server uses TCP port 80 for communications, which is the industry standard for HTTP and what most people associate with web surfing.

If you want to access your system from outside your network, you will have to do one of the following:

- Give your server an external IP address.
- Leave your server behind a firewall with a private IP address, but set your firewall up to forward port 80 to your server.
- Access your system through a virtual private network.

⁶Internet Information Server 5 or 6

Each of the above methods has its advantages and disadvantages.

Generally, hanging your computer out on the Internet without a firewall in front of it is generally not necessary and inadvisable, at least from a security standpoint. In the distant past, this was common practice because people had an egalitarian sense that every computer should have a public IP address. It was an optimistic age.

Today, a cheap 'firewall' can be had for about 80 dollars, so people generally use the port forwarding method, which blocks all incoming traffic that is not explicitly setup within the firewall. The downside to this method is that it is not as secure as blocking all traffic to the Cablecast or Carousel server. Theoretically, if there is an exploit that is discovered in the system's web server, the computer could be compromised and a worm, virus or attacker could gain access to other computers within your network.

The third option, virtual private networking (VPN) is the most secure option because it establishes a single, secure point of encrypted access between the server and the client that is on the Internet. As discussed in section [B.10](#) on page [127](#), VPN's basically establish a network connection on top of your standard Internet access that is a secure link to your organization's internal network. Typically with these connections, you have the same access to your internal network that you would have if you were sitting at your desk.

The downside to the VPN method is that nobody except those with a VPN account will be able to access your server. This means that the RSS, iCal and public web features of Cablecast or Carousel will be inaccessible to the public.

How do I make it so that people can see my Cablecast schedule or view my Carousel announcements? *Not by using the VPN method.*

If you need further information about networking and how to configure your network for external access, see section [B.11](#) on page [127](#).

4.10 How to Make Video Servers and Carousel Players Talk Between Networks

The first step is to know the ports that need to opening. Study section [4.5](#) on page [32](#).

No Proxy Support in
Carousel Players!

Carousel Players utilize TCP port 80 when downloading content from the main server. They do not support proxy server authentication and therefore proxy servers must be bypassed in order for them to work.

Once the required ports are open you will use the web interface within Cablecast to address remote control modules and the "**Carousel Server**" field in the display engine. See chapter [5](#) on page [41](#) for information on configuring Carousel Players and

Carousel Display Engines. See the Cablecast Guide for information on addressing remote Control Modules.

Chapter 5

Carousel Display Engine Video and Setup

5.1 Introduction

In this chapter we cover the setup of a Carousel Player and Carousel Display Engine. Specifically, how to adjust and activate the video output on a Carousel system and how to point the display engine at a Carousel server.

5.2 TV Output

There are a few procedures related to television output which are relevant only if you are using the composite output on your Carousel server or player. The composite output is located on the back of the server, illustrated in section 3.2.2 on page 20 and section 3.2.1 on page 18, number 10.

5.2.1 Enabling the TV Output

By far, the most common technical support question that we receive is “I’ve got no video output! What happened?”

The answer is that your system automatically disabled the video output because it did not sense a monitor or other 75Ω load.

To re-enable your video output:

1. Plug in a 75Ω ¹ load.

¹...monitor, routing switcher, etc...

2. Restart your server *or* . . .
3. Right-click on the NVidia Settings icon in the system tray.
4. Select “**nView Display Settings**”
5. Select “**Clone**”
6. Select the option that shows your VGA monitor + TV. Your monitor may be named by its vendor or it will be called “**Analog Display**”.(figure 5.1)
7. The video output will now be active.

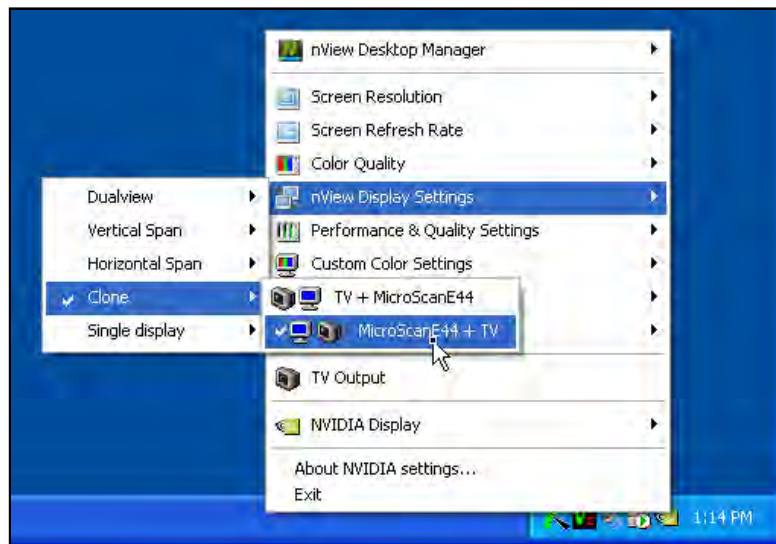


Figure 5.1: Right-click the NVidia icon from the system tray and navigate to the menu through the menu to select Analog + TV

If “**nView Display Options**” is not available, it is probably because the graphics card does not sense a connection on its video output. Check your cabling.

5.2.2 Adjusting the TV Output Settings

Carousel machine's video output is adjusted by the factory to produce acceptable video levels for TV applications. If these become lost or need to be adjusted, follow the steps in this section.

1. Select "**TV Output**" by right-clicking on the Nvidia icon in the server's system tray.
2. The dialog box appears, shown in figure 5.2 on the next page.
3. Use the sliders to adjust the video levels. The "**Overdrive**" option locks the brightness and contrast together. By default, this is option is activated and the adjustment is set to about one third. This setting produces a video signal where pure white is about 90% IRE.
4. Use the arrows in the "**Screen positioning**" tool to adjust the size and position of the TV output.



Use "**Overdrive**" to keep video levels legal

5.2.3 But My Video Is Black and White!

If this happens, follow the instructions from section 5.2.2 for navigating to the "**TV Output**" dialog. Note the settings that are there and click on the "**Restore Defaults**" button.

This will clear out any misconceptions that the graphics card may have gotten about your setup and restore the color to your display. You will have to restore your settings once you have done this, because this procedure will revert your system back to Nvidia's defaults, which are generally set to a video level that is too hot for broadcast.

5.3 Adjusting the Video Resolution

This section covers two major topics: adjusting the video resolution for plug and play monitors and adjusting the resolution for monitors that do not provide accurate settings for the graphic card driver.

If you are operating your system with a standard television monitor in 4x3 mode, then the default setting (800x600 pixels) is the most optimum for this configuration.

No need to adjust 4x3 monitors.

If you plan to operate your system in 16x9 mode, then you will have to consult with your monitor's guide for the display's optimum resolution. If you plug your monitor into Carousel and it does not allow you to select the correct resolution using the "**Display Properties**" resolution slider, you will have to hand enter your monitor's resolution and sync rates. This process is covered in section 5.3.2 on page 45.



Figure 5.2: The NView TV Output dialog box. Notice that the “Overdrive” box is checked.

5.3.1 Standard Resolution Adjustments



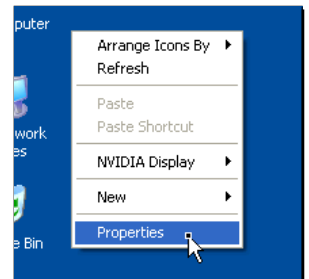
Generally, if you are running Carousel in 4x3 mode there is no need to adjust the display's resolution. It runs in 800x600 and this is optimal for all applications.

Before you proceed, be sure that your display is *directly* plugged into the Carousel system. Do not plug it in through an active balun or other video distribution system.

If you need to adjust Carousel's screen resolution, you may do so by right-click on Carousel's desktop² and clicking on "**Properties**".

This opens the "**Display Properties**" dialog box. Click and drag the "**Screen Resolution**" slider until the native resolution of your display appears, as shown in section 5.3 on the next page

During setup, plug the monitor directly into the server.



5.3.2 Custom Monitor Adjustments



Tightrope is not responsible for any damages to your display as a result of following the procedures outlined in this section. Manually entering sync and resolution settings has the potential to permanently damage your display if it is done incorrectly!

If you are utilizing an LCD or plasma monitor, chances are that you may need to specify a resolution that is not selectable using the procedure outlined in the previous section.



Check to see if there is any software that came with your LCD or Plasma display. This may include the monitor definitions for your display and prevent you from having to set a custom resolution.

Check with the display's documentation for the specifications related to the monitors resolution and sync. Take careful note to look for the *native* resolution of the display. All displays are able to sync and display a variety of resolutions. If you select a non-native resolution, the display's processor will have to re-scale the image, which will degrade its quality.

Armed with this information, open the "**Display Properties**" dialog, as we did in previous section. Click on the "**Advanced**" button.

²If the display engine is running, double-click until it closes.

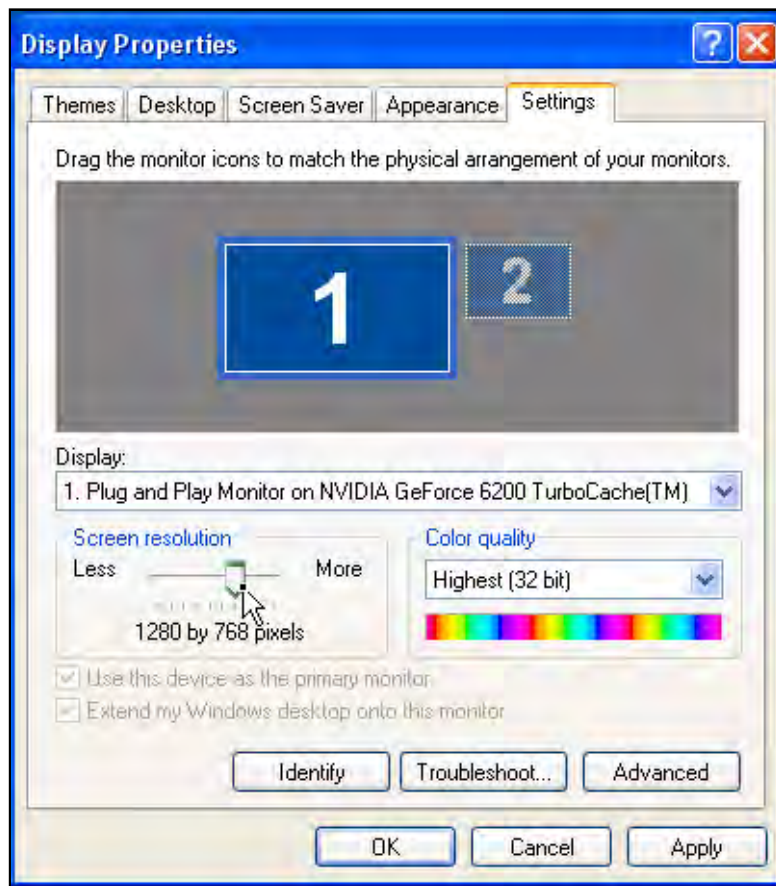


Figure 5.3: Loading the Display Properties Dialog.

You will see tabs at the top of the dialog box. Click on the tab that starts with the word “**GeForce**”. On the left you will see a tab slide out, providing additional menu options. Select “**Screen Resolutions & Refresh Rates**”. (figure 5.4)

Click the “**Add**” button. You will get a tremendously wordy warning about how you can *destroy* your monitor’s display if you enter the wrong information into the next dialog box. *Heed this warning!* Generally, monitors have built-in safe guards to protect them against “out-of-bounds” monitor resolutions and sync rates, but do not rely on these. *Tightrope is not responsible for any damages to your display.*

BE CAREFUL WHEN
ADDING CUSTOM RES-
OLUTIONS!!

The dialog shown in figure 5.5 on the next page will appear. Enter your display’s resolution information into this dialog box. After clicking “**OK**”, you may wish to click the “**Only show custom modes**” checkbox, which will make it easier to pick the resolution that you just added.

Select the new resolution using the “**Screen Resolution**” slider at the top. Click “**Apply**” to view the results.

The display should look centered and fill the screen. If it does not, try using the monitor’s positioning controls to center it. If it still seems out of adjustment or the display is corrupted, you may need to use the “**Advanced Timing**” dialog to adjust some of the sync properties. This is very rare and should not need to be changed, but it is the last option if you are unable to get the display to appear correctly.

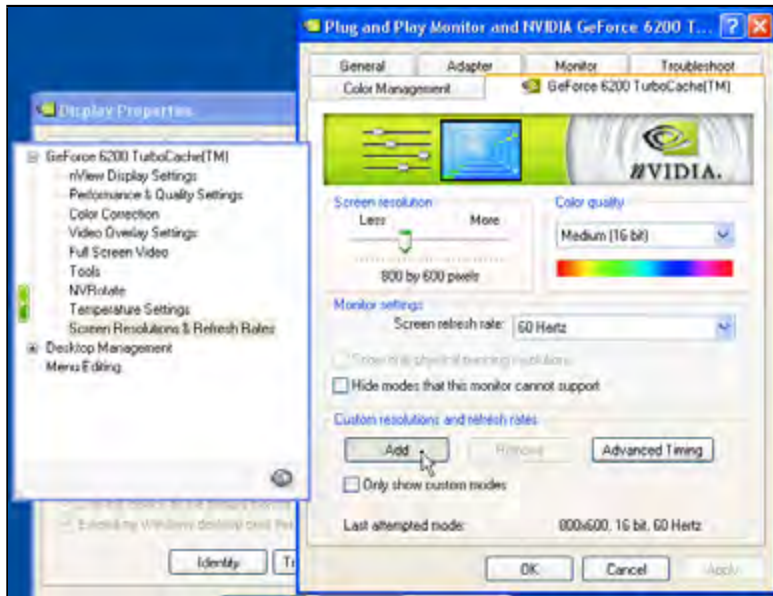


Figure 5.4: The nVidia Advanced Menu

5.3.3 Setting up a 9x16 Display

Carousel may be configured for 9x16 display, where the LCD or plasma monitor is put on its side for a portrait display.

To accomplish this, simply navigate to the “**NVRotate**” menu from the “**Advanced**” settings in “**Display Properties**”. (figure 5.6 on the facing page)

Use the arrows to rotate the display until the illustration looks the way that your monitors will be mounted. After you click “**OK**” the video output will be adjusted so that everything will appear right-side up when the monitor is rotated.

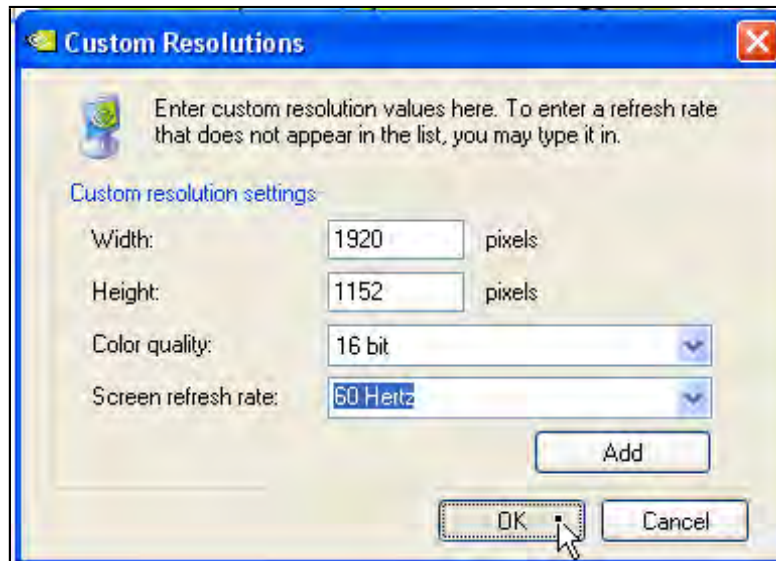


Figure 5.5: Adding a Resolution

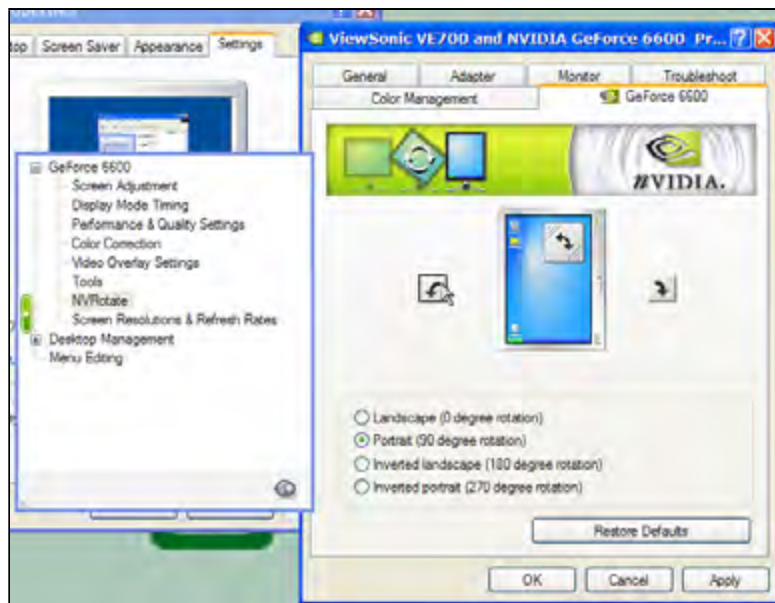


Figure 5.6: Rotating the display

Chapter 6

Frontdoor Server Settings

6.1 Introduction

Part of the installation of your system is to perform basic system settings that are located within the web interface of the system. In this chapter, we'll cover such things as logging in and adjusting the Frontdoor server settings.

6.2 Logging into the Frontdoor Server

Remember, your system operates as a web application. This means that its interface is created from a web server that is running on your server (figure 6.1 on the next page). You can access the software directly from the server, but more often you will access it from a computer that is on your network.

Your system comes with a built-in account called the "Admin" account.

The username for the Administrator account is: "Admin"

The default password is: "trms"



The Admin and Manager Usernames are not case sensitive. You may type "Admin" or "admin" and log in successfully.

You will use this account when following the instructions in this chapter. The "Admin" always has access to all of the features of the system, in both Cablecast and Carousel and includes a "Server Setup" menu that is not available while logged in using any other account.

In addition to the “**Admin**” account, every server comes with a “**Manager**” account. The “**Manager**” account is used to manage the user accounts of all Tightrope products and is the only account that has access to the “**Frontdoor User Manager**”.



We will touch on some activities within the Frontdoor User Manager in this chapter. For complete instructions on using the Frontdoor User Manager, please see the Frontdoor User Manager guide.



All accounts are shipped from Tightrope Media Systems with the default password of “**trms**”. You should change this password as soon as possible.



Every system that Tightrope ships includes “**trms**” as the password! Be sure that you change this password!

6.3 The Frontdoor Main Menu

The Frontdoor Main menu, which appears after you successfully log in, is common to both the administrator and user-level accounts, except for the “**Server Setup**” option. The list of menu options is as follows:

Frontdoor Applications This is the list of Frontdoor applications, such as Carousel and Cablecast, which are installed on the system. While the ad-

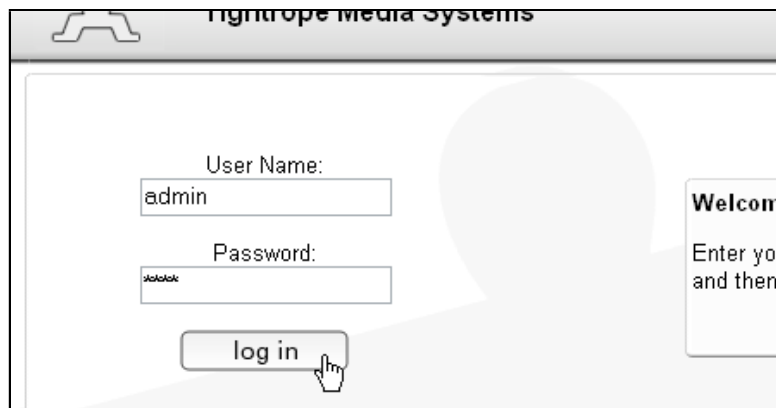


Figure 6.1: Logging into the server

administrator always sees the complete list, user-level accounts may only see a subset of tools depending on privileges assigned in the Frontdoor User Manager.

Change Password Change the account's password from here.

Server Setup *Unique to the administrator account*, this menu option gives the administrator control over email server setup, the banner title, and clock synchronization settings. It is the primary subject of this chapter.

Logout Ends the current session.

6.4 Changing Your Password

All users may change their account's password by selecting the Change Password button. Simply type the new password into the **"Password"** and **"Verify fields"**.

If the account has the **"Require Secure Passwords"** field checked (accessible from the Frontdoor User Manager) then the account must have a secure password. These passwords must be at least six characters long, two of which must be non-alpha. For example "hello12" is valid, but "Me12" is not because it is too short. "hello#@" is valid, whereas "helloAB" is not because it contains no non-alpha characters.

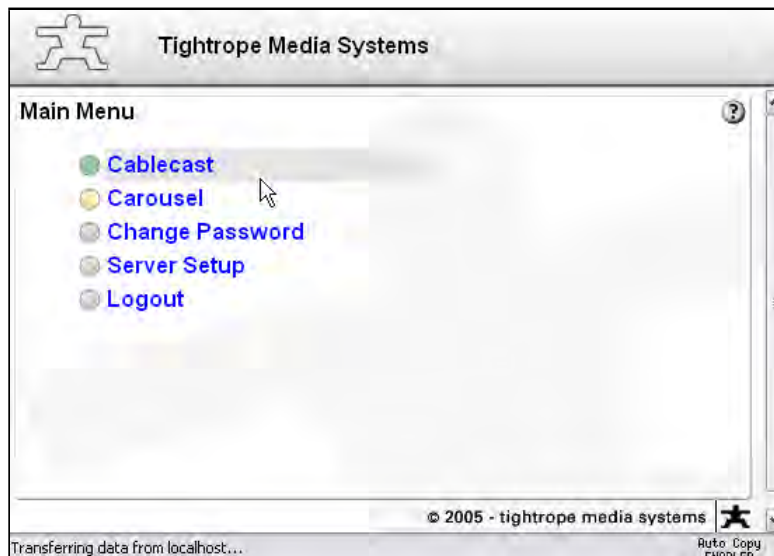


Figure 6.2: Frontdoor Main Menu

Users are required to change their password upon first login if the User Manager¹ has set their account to “**User must change password on next login**” within the Frontdoor User Manager.

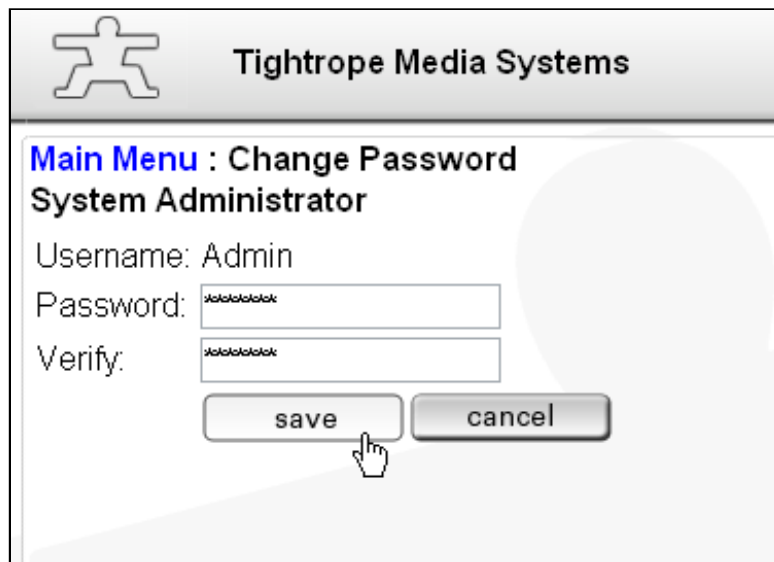
6.5 Server Setup

When you log in as the administrator, the Frontdoor main menu includes the “**Server Setup**” menu item. As you can see in figure 6.4 on the facing page This menu gives you control over global settings of the Server that apply to all Frontdoor tools. Each submenu contains a single form. These forms are outlined below:

6.5.1 Server Setup: Site Name

The bold-text banner at the top of the Frontdoor is set within this submenu (figure 6.5 on the next page). Usually this is the organization’s name. Changing this field changes what is displayed on the banner.

¹The User Manager is a special, built-in account on the system that manages user accounts



The screenshot shows a web interface for 'Tightrope Media Systems'. At the top left is a stick figure icon. The main header reads 'Tightrope Media Systems'. Below this is a section titled 'Main Menu : Change Password System Administrator'. The form contains the following fields and controls:

- Username: Admin
- Password: [password field with asterisks]
- Verify: [password field with asterisks]
- Buttons: 'save' and 'cancel'.

A mouse cursor is pointing at the 'save' button.

Figure 6.3: When changing your password, make sure you enter it in the Password and Verify fields.

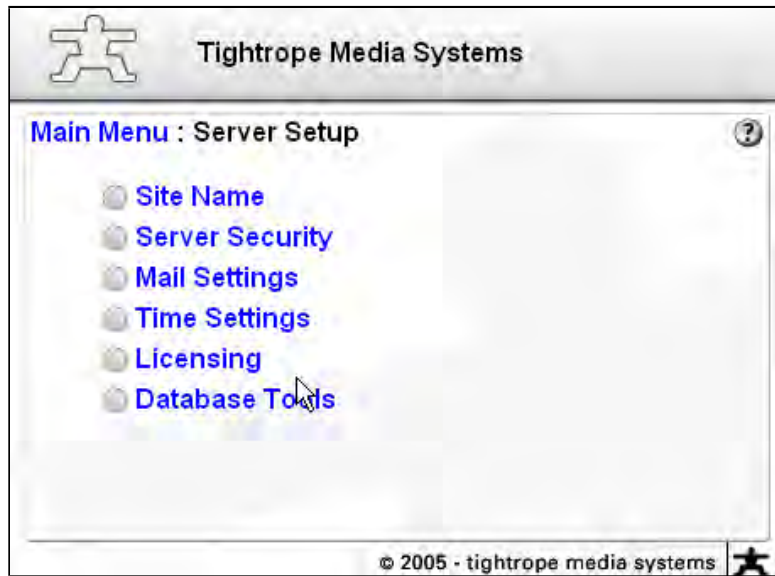


Figure 6.4: The Server Setup Menu



Figure 6.5: The arrow points to the banner.



The banner at the top of the page will not change until you log out. In some cases, you may need to close your browser and re-open it in order for the change to be displayed on your computer.

6.5.2 Server Setup: Server Security

Every time a user interacts with the system, it resets a timer. If they haven't interacted with it before the maximum number of minutes that are allowed, set within this menu using the **"minutes"** field, the system will close their session and force them to log back in.



If the **"minutes"** value is set too high, there will be a significant period that a malicious person could access the system if a user's computer is left unattended. Usually 20 minutes is a good number, but your environment and security needs may vary.

6.5.3 Server Setup: Mail Settings

Frontdoor applications make use of email to notify administrators and users of different events. In order to use these features, you must enter the address of an email server that the Server can use to distribute email. An example may be "mail.yourdomain.org". Enter that name in the Mail Server field. (figure 6.6 on the facing page)

In the **"Mail Bounce Address"** field, enter the email address that should receive notices of bounced mail. It is very important to enter a valid address because most email servers will bounce the email if it is invalid.



This may be the person in charge of your server.

When everything is set, be sure to use the test function. Simply enter your email address into the **"Test Address"** field and click the **"test"** button. This will send a test email to your account. (figure 6.7 on page 58)

If the test fails, it is probably because of one of these three reasons:

- The system uses SMTP, which is not compatible with some proprietary email servers. Check with your IT administrator.

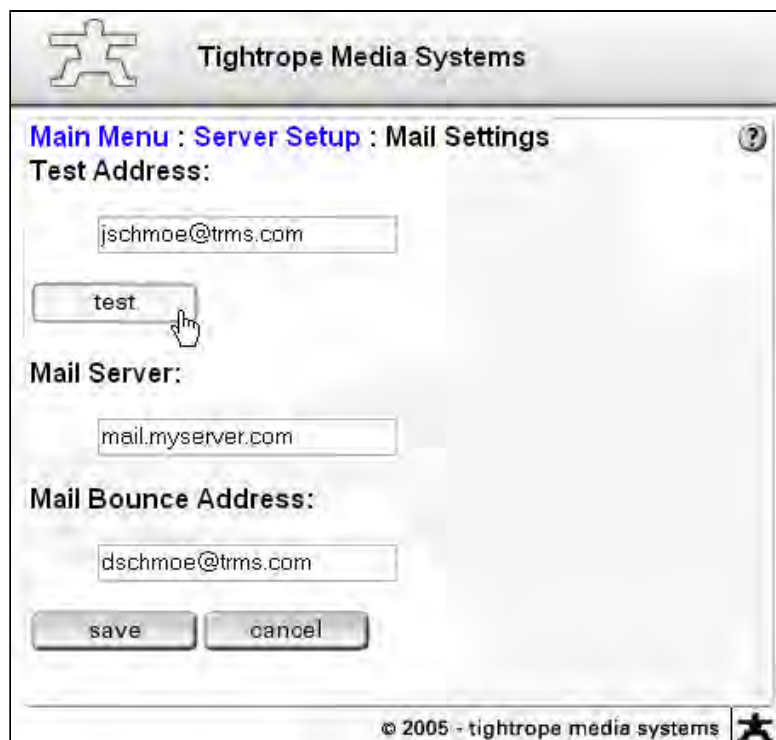


Figure 6.6: Be sure to test your settings by entering your own email account. If set correctly, you'll receive a test email within a few minutes.

- If your email server requires authentication in order to send mail, you're out of luck because the Frontdoor system in this server doesn't support it.
- You may need to setup relaying for this server, especially if you have your system on a separate network from your mail server. If you do not setup relaying, your email server will assume that your server is a spammer.

6.5.4 Server Setup: Time Settings

The server has a service that synchronizes the system clock at an interval that you establish in the **"Synchronize"** field. (figure 6.8 on the facing page)

Enter the location of the network timeserver in the **"Time (NTP) Server"** field.



The default setting of "time.trms.com" will work fine if your network has UDP port 123 open to the Internet. If it does not, or you are not sure, contact your network administrator. Hopefully there is an internal NTP server that your system can synchronize to.

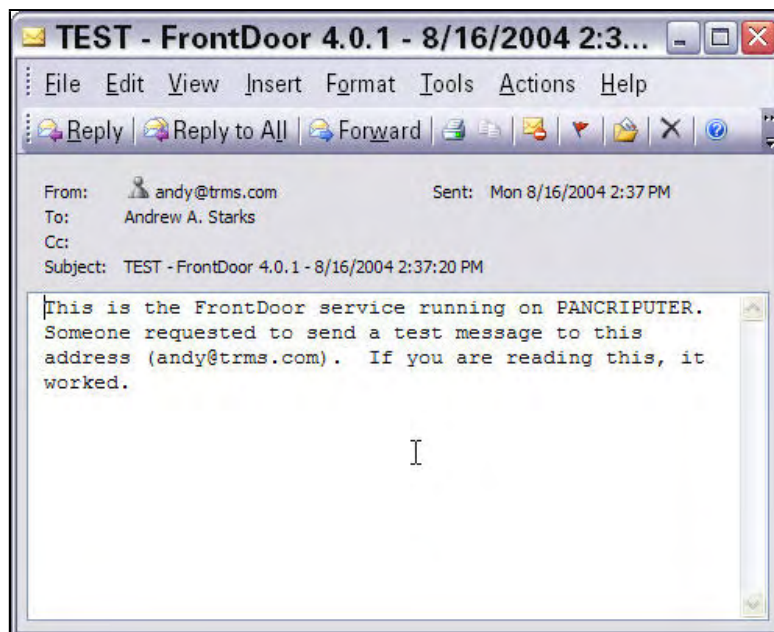


Figure 6.7: The email that you will receive when your email is set correctly.

The screenshot shows a dialog box titled "Tightrope Media Systems". The breadcrumb path is "Main Menu : Server Setup : Time Settings". The "Time Synchronization Service" is checked and "Enabled". The "Time (NTP) Server" is set to "time.trms.com". The "Synchronize" section shows "Every 10 minutes" with an "update now" button. Status information at the bottom indicates the next update is on 1/21/2005 at 11:47:36 PM and the last correction was -1364 ms at 1/21/2005 11:37:36 PM. There are "save" and "cancel" buttons at the bottom left, and a copyright notice "© 2005 - tightrope media systems" with a logo at the bottom right.

Tightrope Media Systems

Main Menu : Server Setup : Time Settings

Time Synchronization Service:

Enabled

Time (NTP) Server:

time.trms.com

Synchronize:

Every 10 minutes **update now**

Next Update: 1/21/2005 11:47:36 PM
Last Correction: -1364 ms at 1/21/2005 11:37:36 PM

save **cancel**

© 2005 - tightrope media systems

Figure 6.8: Notice the information at the bottom of this form. You can see when the last successful time synchronization took place.

6.5.5 Server Setup: Database Tools

Your system has up to three primary databases. This is where you maintain the Frontdoor Database. It holds all of the general settings and user account information. Within this menu, you can backup and update the database.

If the current and required versions do not match, your database is out of date. To update the database, click the **“update”** button.

To backup the database, select the type of backup that you wish to perform. (figure 6.9 on the next page)

The first option backs it up to the server’s hard disk at **“D:\TRMS\Database\Backup”**.

To copy it to a Window’s share, type the share name into the **“UNC”** field. UNC names in the Windows world begin with two back slashes (\\).

Example: `“\\myServer\myServerShare\SubDirectory”`

To attach a backup of your database to an email that is forwarded to you, choose the **“Backup and Email”** option. Enter your email address in the **“Address”** field.



Before you can email the database, you need to set up the email server settings, as shown in section 6.5.3 on page 56.



Many email systems limit the size of attachments. If you’re having trouble emailing your database, be sure you are not up against this limitation.

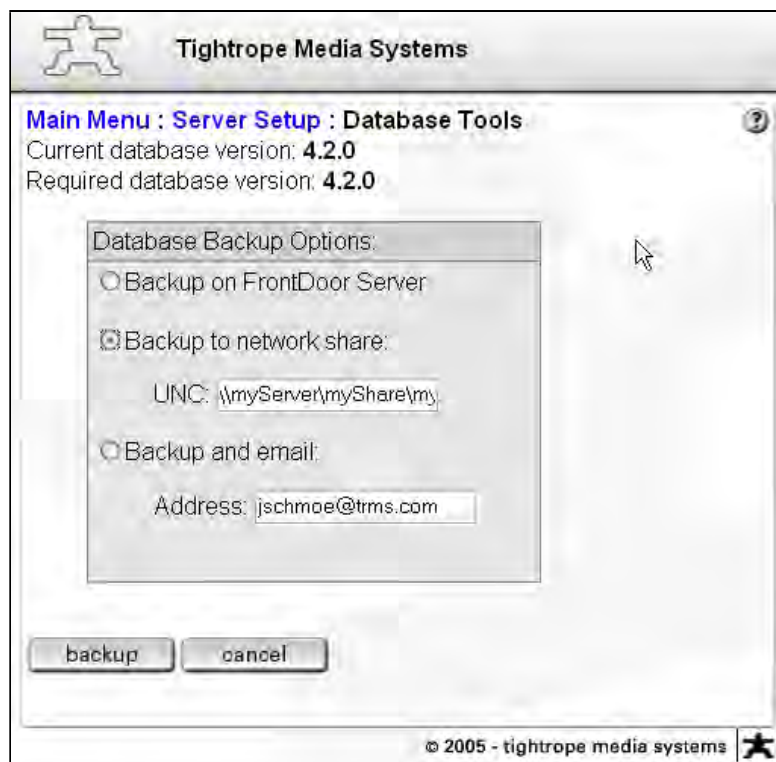


Figure 6.9: The Database Tools form in Server Setup.

Chapter 7

Connecting Serial Ports—Cablecast Installations

7.1 Introduction

Cablecast utilizes serial ports for communicating with a wide variety of devices. The first step in communicating with these devices is identifying, addressing and configuring the ports that are to be used with your specific device.

Included with your Cablecast server is a yellow sheet of paper that enumerates the serial ports included with your system. If this default configuration is suitable to your application, then you may use this sheet as a guide for configuring Cablecast.

If you wish to adjust the port assignments, add serial ports or need to change a port type from 422 to 232 (or the other-way-around) use this chapter as your guide.

7.2 8-Port Serial Cards

Cablecast configurations vary and your installation may include one or more 8-port serial cards installed in any of the servers purchased with your system. These cards are identified by a multi-row 80-pin connector on the back of the server.



Typically, the Cablecast server will include all of the serial ports that will be used in your system. Tightrope will install these cards in other servers only when the Cablecast server does not have space for the additional cards.

Serial cards utilize an octopus cable with 8 9-pin female serial ports. If you have more than one card, note that all octopus cables are identical and plug into the back of your server using any available 80-pin connector.

Included with your server is a yellow form that diagrams the configuration of your serial port cards including: the cable's label, the COM port number, and the port configuration (422 or 232).

Use this chart to connect the serial equipment in your head end. As long as the correct type of port is used on the device, the specific order that devices are plugged in does not matter to Cablecast. Obviously you will want to choose a logical configuration.

If you do not have the correct 422-232 configuration (you need more of one or the other), consult section 7.6 on page 71 for instructions on how to reconfigure the PCI232-422-8PT.

The PCI serial cards used by Tightrope are wired for video use when set to 422 mode. Therefore, BVW protocol devices will utilize a straight-through cable, as illustrated in figure 7.1 on the next page.

422 ports are wired for BVW serial ports. Use straight-through cables.



If you ordered the PCI232-8PT, it is not possible to reconfigure any of the ports for 422 operation.

7.3 Quatech USB-Serial Converters

If your purchase includes Quatech USB to Serial converters, the driver was installed on your Cablecast server. Simply plug the Quatech box into any USB port on the back of the Cablecast machine.

Quatech 422 USB-Serial devices use a different wiring scheme than the 8-Port PCI serial cards sold by Tightrope. They are wired for standard computer use, not for video use. See figure 7.2 on the facing page.

When you plug the Quatech converter into the system, Windows will automatically and arbitrarily assign each serial port a COM port number. See section 7.4 on page 66 for information about discovering the COM port assignments of your USB-Serial converter.

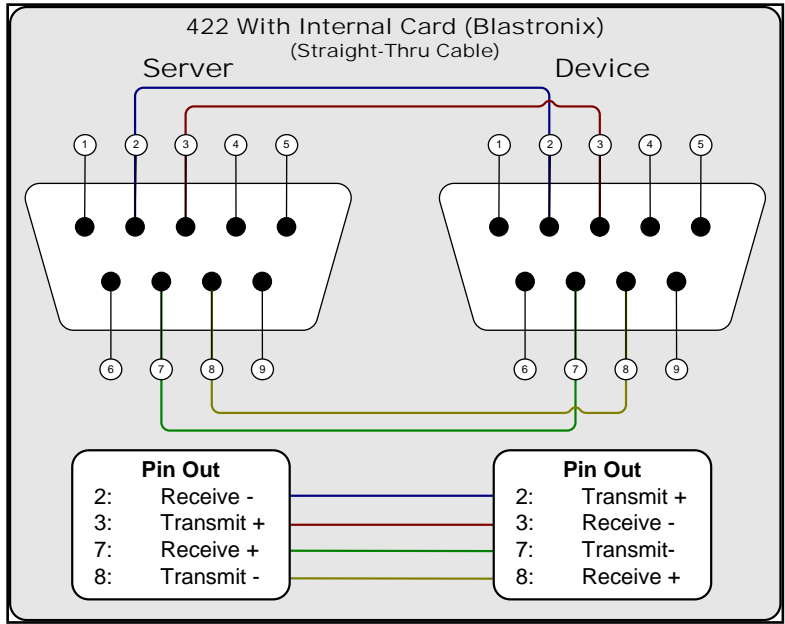


Figure 7.1: PCI 422 cable wiring.

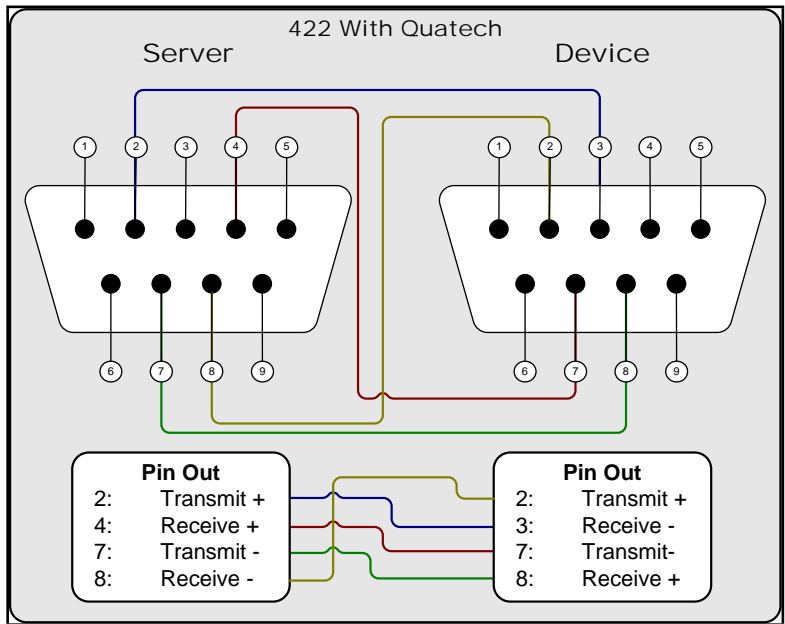


Figure 7.2: Quatech 422 cable wiring.

7.3.1 Third Party USB-Serial Converters

You may use third party USB-Serial converters with Cablecast. Follow the manufacturers instructions for driver installation, making careful note that most manufacturers require driver installation *before* the converter is installed.

Windows will automatically assign a COM port number to these devices. See section 7.4 for information about discovering the COM port assignments of your USB-Serial converter.

7.4 Discovering and Reassigning COM Port Assignments

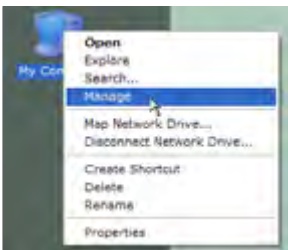
Windows automatically assigns COM port numbers to serial ports that are added to the system. Most often, the assignment is simply the next available number. All servers have one COM port, so if your system has additional COM ports, they will probably start at COM '2'.

If your system includes internal PCI serial adapters, then there is a yellow sheet of paper included with the server that lists the COM port settings. Consult this sheet and decide whether or not you need to reassign your serial ports.

If you are utilizing USB-Serial converters, there are two ways to discover the port assignment. The easy way is to use the TRMS Serial Port Tester program, which also has facilities for testing the COM Port assignment for each adaptor. See section 7.5 on page 68 for information on how to use this program.

However, if you want the ability to reassign COM Port numbers, then you'll have to use the second way of discovering COM Port assignments, which is covered in this section.

From the desktop, right-click on "**My Computer**" and select "**Manage**".



The Computer Management console will appear. Click on "**Device Manager**". In the left pane you will see a list of device categories. Expand the "**Ports (COM&LPT)**" category. Within, you will see all of the COM ports that are recognized by the Windows system. (figure 7.3 on the facing page)

If you need to change any of these COM port assignments, double-click on the port, select the "**Settings**" tab, click the "**Advanced...**" button at the bottom of the dialog box, then select the comport number from the "**COM Port Number**" pop-down list. Click "**OK**" to save your settings. (figure 7.4 on the next page)

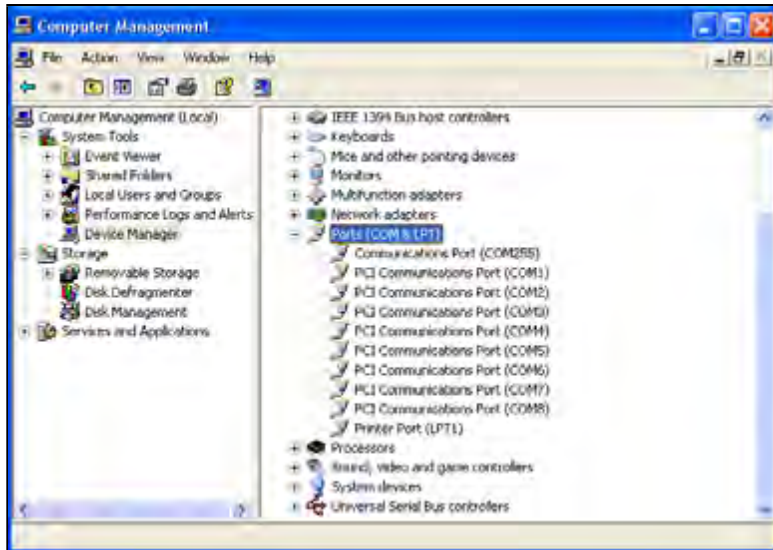


Figure 7.3: Ports in the Device Manager List

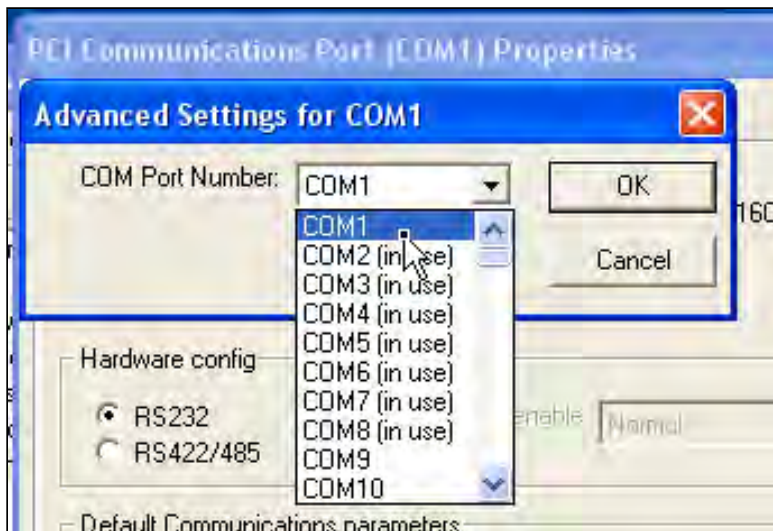


Figure 7.4: Changing the COM Port assignment.



Don't bother setting any options in the “**Settings**” tab for any COM Ports, as they are completely ignored by the software and the system. This includes the “**RS232, RS422/485**” radio buttons, which have no effect on the hardware. See section 7.6 on page 71 for information on how to switch between 422 and 232 on PCI422-232-8PT cards.

When you are finished assigning ports, mark your COM Port numbers on a sheet of paper. To verify the COM Port number for a specific serial port, see section 7.5.

7.5 The Serial Port Tester Application

Tightrope has included a serial port loopback adaptor and a handy software utility for testing serial ports¹, which is useful when trying to identify COM port assignments for the serial ports on your server.

The software utility is located in the “**D:\TRMS\Tools**” directory and it is called “**Utilities.SerialPortTesting.exe**”.

The loopback adaptor was included in the Cablecast server's packaging.



If your system did not include this adaptor, you can make one by wiring a DB-9 Pin female adaptor as shown in figure 7.5 on the next page.

The operation of the tester program is extremely simple. Plug the loopback adaptor into the serial port that you are testing. Select the COM Port from the “**Port**” pop-down list. Click the “**Test**” button. If you have success, you will see something similar to that in figure 7.6 on page 70. If not, you'll see the dialog box in figure 7.7 on page 70.

A test will fail for three reasons:

1. You have the adaptor on the wrong port. Try switching the “**Port**” selection until the test passes.
2. You have a broken or improperly installed serial port. This is especially possible with third party USB-Serial adaptors and improperly installed drivers.
3. Your loopback tester is broken. Tightrope uses the included tester to burn-in new servers, so it is unlikely that the included loopback adaptor is not working. If you made your own, check your wiring and test it on a serial port that is known to be working.

¹You're welcome.

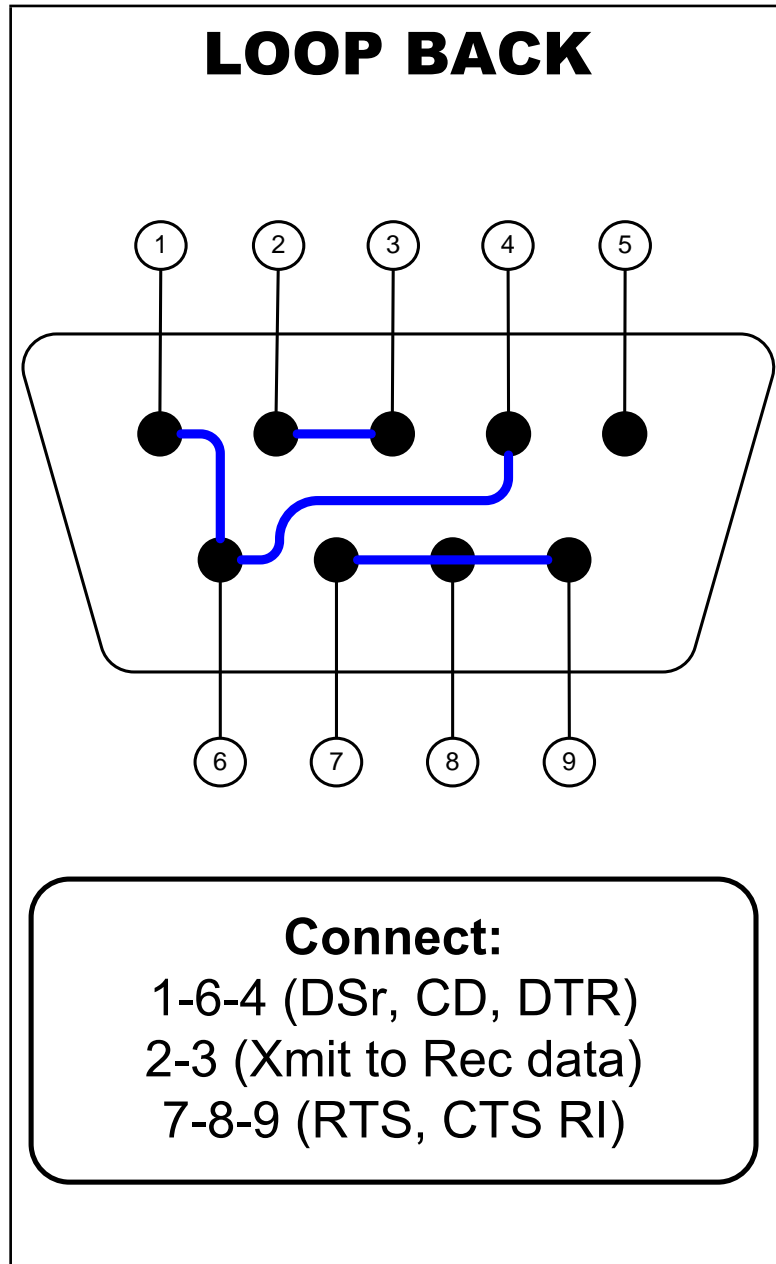


Figure 7.5: To make a serial port loopback adaptor, wire a DB-9 Pin female connector according to this illustration.

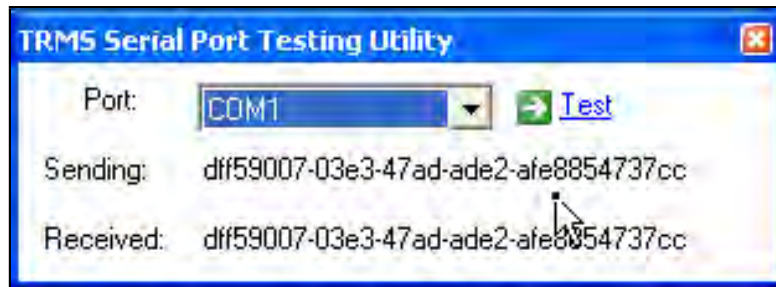


Figure 7.6: Successful Serial Port Test

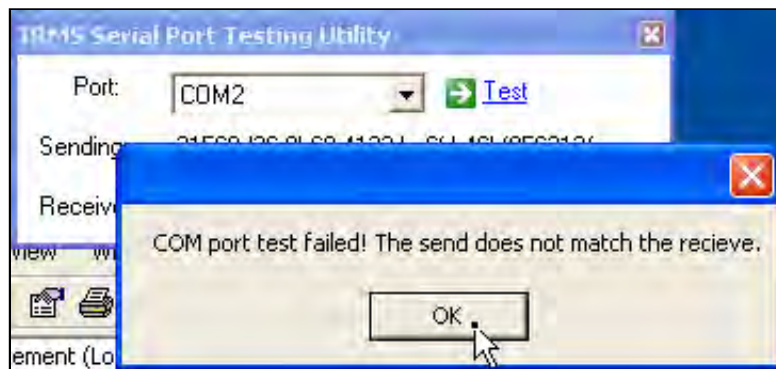


Figure 7.7: Failed Serial Port Test

As you verify each port, write its COM Port number and the device that will be attached to it on a sheet of paper. You will use this information when you configure Cablecast.

7.6 Changing the 422-232 Configuration on PCI422-232-8PT Cards

Check the information sheet that was included with your server for the default configuration of your 422/232 PCI cards. If you need to change this configuration, follow the steps in this section.

Open the Cablecast server's top cover, and remove the PCI card. If you have more than one card, note that by default the COM Ports will be numbered from right to left²: 1-8, 9-16, 17-24, etc.

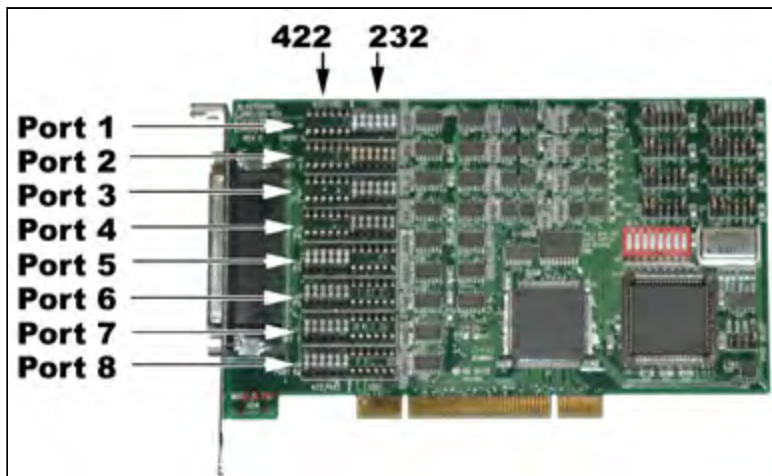


Figure 7.8: The PCI422-232-8PT. Note the shunts that determine each ports mode.



Be *extremely* careful during the next steps. The shunts described in the next paragraph are extremely fragile. Use great care when prying them out.

Study figure 7.8. The “422” and “232” columns both hold the shunts that determine the mode of each port. To change modes, pry out the shunt with a small flathead screwdriver and switch it to the other setting.

²With the computer's front closest to you it is right to left. If you look at it from the backside, it's left to right.



Do not change the jumpers at the back of the card. These are set correctly and will render the card inoperable if changed.

7.7 A Note About Serial Cables

For reasons of history and ego, not all devices use the same cable. Some are null. Some are straight-through. Some are something else.

If you are sure of your COM Port assignments and you've used the loopback adaptor to test the serial port's integrity, be sure that you have the correct cable³ before assuming that Cablecast is broken. See appendix [A](#) on page [95](#) for pin-out diagrams of most devices.

³...and test it!

Chapter 8

The CBL-IR4

8.1 Introduction



Figure 8.1: The IR4

The IR4 is a 4-port infrared (IR) transmitter that is controlled by Cablecast. It requires a single RS-232 serial port and is able to translate instruction from Cablecast into specified commands for up to 4 IR controlled devices, such as VCRs and DVD players.

Multiple IR4's can be connected to the server.

Devices that are controlled via IR use codes encoded in the infrared light emitting from the device's remote control. Programming the IR for involves capturing and recording those codes.

8.2 Installing the IR4

The IR4 is connected to the Cablecast machine through an available serial port¹.

1. Connect power to the IR4.
2. Connect the included RJ45 cable to the “RS232 AUX” port on the IR4.
3. Connect the other end of the RJ45 cable to the DB9-RJ45 adaptor, then into an available serial port on the server.
4. Connect each of the four included IR emitter cables to the 1/8th inch mini-plugs labeled “EMITTER OUTPUTS”.
5. Do *not* attach the other end of the IR emitter cable to your device at this time. You will want to test for the optimal placement before sticking it on to your device.

8.3 Learning IR Commands

Once the IR4 is connected you will need to learn each device’s IR codes from the device’s remote control.

1. Launch the “Utilities.IRLearner” application from the “D:\TRMS \Tools” directory on the server.
2. Set the “**Serial Port**” field to the COM port number that the IR4 is plugged into.
3. Select the first output in the “**IR Output**” field.
4. Click “**Play**” under the learn column.
 - (a) After clicking the button, you will be prompted to learn the IR command.
 - (b) Point the device’s remote at the front of the IR4.
 - (c) Click the “**OK**” button.
 - (d) Press the play button on the remote control.
 - (e) You should see the “**REC**” light turn solid and the ‘XMIT’ light flash when it successfully learns the command.
5. To test the command, click the “**Play**” button under the “**Test**” column.
6. Repeat steps four and five for each command and all four IR ports.

¹You may install the IR4 on any server that has the Cablecast Control Module Pack installed on it. This includes VS4-Series video servers, ENC-Series encoders, STRM-LIVE servers and STRM-VOD-Series servers. Carousel Players may also have this package installed by purchasing CBL-CMPack.

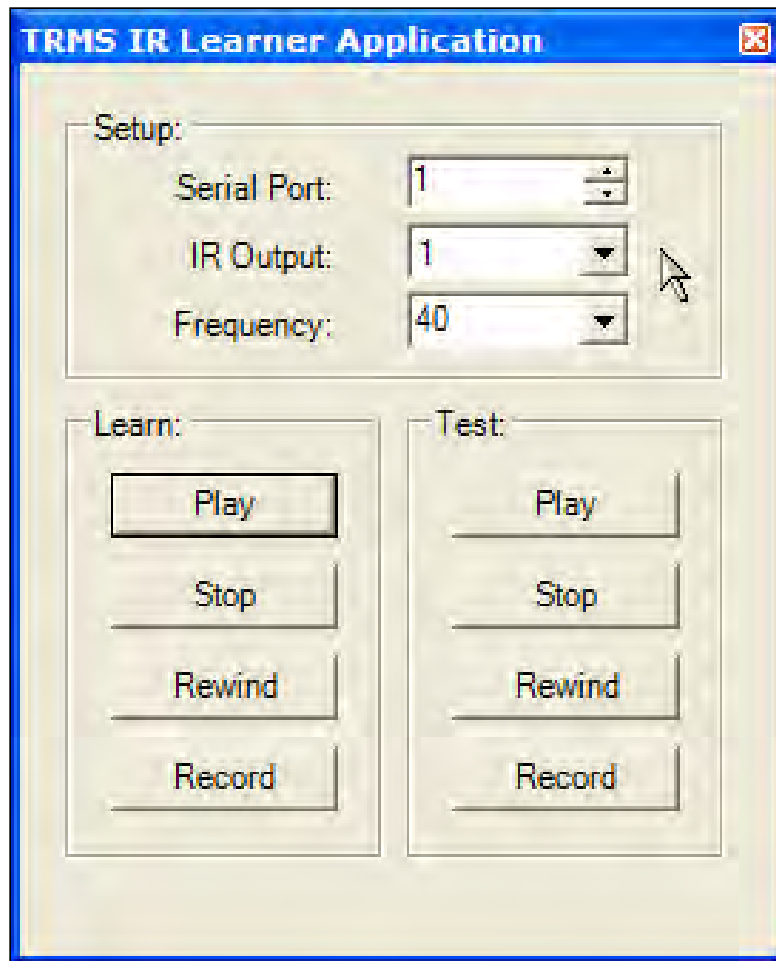


Figure 8.2: The learning application for the IR4.



Even if you have four identical devices plugged into the unit you will still have to program all four IR ports separately.

If you are unable to successfully capture commands for a particular device, it could be that the device needs a different frequency than the default setting, which is "40". Retry capturing codes using one of the options from the "**Frequency**" pop-down list. It is possible to enter your own value into this field, but it is highly unlikely that your device uses a frequency other than one of the pre-entered ones that are provided.

8.4 Configuring Cablecast

The following steps are done in the Cablecast web user interface.

Control Module Set:

1. Navigate to "**Location Settings : I/O : Control Module Sets**".
2. Click the "**New**" button.
3. Set the "**CMS Name**" field to "TRMSIR4".
4. Set the "**Control Module**" field to "TRMSIR4CM".
5. Enter the COM port that the IR4 is plugged into in the "**Port/Setting**" field.
6. Click the "**Save**" button.
7. Repeat steps two through six for each IR4 device, choosing a unique name in step three.

Configure the devices:

1. Navigate to the "**Location Settings : I/O : Devices**" menu.
2. Create a new device by clicking the "**New**" button.
3. Set the "**Device CMS**" field to "TRMSIR4²".
4. Set the "**Device Address**" field to the IR output on the IR4, which will be "1", "2", "3" or "4".
5. Configure the rest of the device parameters according to the instructions in the Cablecast Guide.
6. Click the "**Save**" button.

²If you have multiple IR4's connected, choose the CMS name for the specific IR4 that you are addressing.

8.5 Testing the Control

The best way to test an IR device is with Cablecast's force menu. Once you have established that you can control the device with the force menu, create a schedule and verify that the device is playing back properly. You may have to adjust the device's pre-roll setting for proper routing switcher coordination.

Chapter 9

The VS4 and ENC Series Video Servers

9.1 Introduction

This Chapter will walk you through the installation and software configuration of the VS4-Series video servers and ENC-Series encoders.



VS4-Series video servers include MPEG-2 encoders. ENC and VS4 servers share the same hardware and software platform for encoding and therefore have many of the same setup procedures.

9.2 Environmental Considerations

Your video server is a high performance computer system that requires proper environmental control.

- Make sure that the air surrounding the video server never exceeds 78° Fahrenheit.
- Make sure the server has ample ventilation in the front and from the rear. Be sure that cabinet drawers are not blocking airflow.
- Make sure that stable power is provided and that the server is plugged into a surge protector and UPS system.



Be sure to heed these environmental constraints! Failure to do so will result in repeated drive failure that is not covered under your Tightrope Media Systems Limited Warranty.

9.3 How does Cablecast Communicate with the Server?

VS4-Series video servers and ENC-Series encoders are controlled by Cablecast through the network using the built in Ethernet adaptor. A software control module that is on the video server and encoders manages commands from Cablecast in realtime or on a schedule formatted into an event table from the Cablecast server.

These video servers and encoders work semi-independently from Cablecast in that rebooting the Cablecast machine will have no effect on the video server's ability to execute the event list or play programming.

Generally, it is best to have the Cablecast machine, video servers and encoders in close 'network proximity' to each other—no gateways or network segments between them. This is especially important when working between the encoder and the video server, as the MPEG-2 files that are transferred between these servers are very large.

It is important to understand that Cablecast does not transfer MPEG-2 files to or from any encoder or video server. The amount of traffic between these servers and Cablecast is minimal, but it is nevertheless important to have as little lag as possible to facilitate responsive control during force operations.

9.4 Cablecast Setup for the VS4 and ENC Servers

Physical installation is covered in chapter 3 on page 17.

When you are ready to start configuring Cablecast's device control, follow the steps in this section to properly configure it to control the VS4 and ENC series encoders.



This section assumes a basic understanding of the Cablecast web user interface. See the Cablecast guide for more detailed information about its operation.

1. Log into Cablecast and navigate to “**System Settings : Control Module Hosts**”.
2. Check to see if there is an entry for your video server. If there is, you will see an entry for the Cablecast server called “localhost” and one each video server or encoder in your installation, which will be named something like “VS4500E-1006”. If there is no entry for your encoders or video server, add them by following these steps for each server or encoder:
 - (a) Click the “**new**” button.
 - (b) Type a descriptive name for your video server or encoder in the “**Name**” field. Example: “VS4-500” or “ENC-110-Studio”.



If there is more than one server, it's helpful to include its physical location in the name, so that when your addressing it in later setup procedures it will be simple to select the correct control module host.

- (c) Enter the network name or IP address in the “**Address**” field.



The “**Control Modules**” field has no effect on the settings of Cablecast. It only sets the target for the “**details**” link. That is, if you select a control module and click “**details**”, the system will retrieve a history on that control module on that server.

- (d) Enter the address of the video server. It may be a name or an IP address.
- (e) If you have more than one server, return to step ‘a’. Otherwise. . .
- (f) Click the “**save**” button.
- (g) When the software returns you to the “**System Settings**” menu, click on the “**Control Module Hosts**” button again. If it returns you to the menu and you can see the “**Control Modules**” pop-down list for the servers that you added, then the system was able to find them. If not, then you will see a “**No such host is known**” message. Check the address and your network configuration.



3. From the main menu, navigate to “**Location Settings : I/O : Control Module Host**”.
4. If there are no entries for your video servers and encoders, click the “**new**” button for each server. You will need 2 entries for each VS4-Series server¹ and one for each ENC-Series encoder.

¹This is because two control modules are used on VS4-Series servers—one for the decoders and one for the encoder.



As an example, if you had a VS4-Series video server and an ENC-Series encoder, you will need three entries.

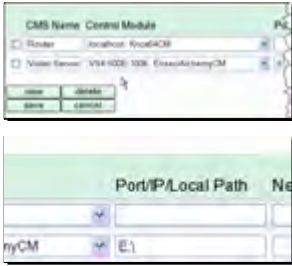
5. If there was an existing entry, you may need to edit it. Whether it is a new entry or one that you are editing:

(a) For VS4-Series video servers:

i. Enter a name for your video server in the “Name” field.



It is helpful to include the physical location or the specific purpose in the “Name” field if there is more than one server.



ii. Select the “**EnseoAlchemyCM**” control module from the video server’s control module host that you setup earlier. Be sure that you do **not** pick the Cablecast server’s version of this ². Pick the one that is located on the video server!

iii. The video server has to know where to find its content. When it is shipped from the factory, that path is “E:\”. You may change it to another path if necessary. Enter this information into the “**Port/IP/Local Path**” field.

iv. Check the “**Sync Time**” checkbox so that the video server and Cablecast are kept in sync.

(b) For the encoder on each VS4-Series video server *and* each ENC-Series encoder:

i. Enter a name for the encoder in the “Name” field.



If you only have one video server with an encoder, “Encoder” may be appropriate. If you have more than one, then “Encoder-Studio” or “VS4-Encoder” might make more sense.

ii. Select the “**OptibaseMovimakerCM**” control module from the video server or encoder’s control module host that you setup earlier.

iii. The encoder control module needs to know where to save its MPEG files. This is usually the encoder’s “E:\” directory. If this is a video server’s encoder, *be sure* it is the same path as the video server’s content directory! Enter the path into the “**Port/IP/Local path**” field.

²Do not pick “localhost : EnseoAlchemyCM”!



If you are setting up an ENC-Series encoder, this path will be the encoder's local hard drive and the system will automatically copy this file to your video server once it is done being recorded.

iv. Check the **“Sync-Time”** checkbox so that the encoder and Cablecast are kept in sync.

(c) Click the **“save”** button.

6. Navigate to **“Location Settings : Shows : Formats”**.

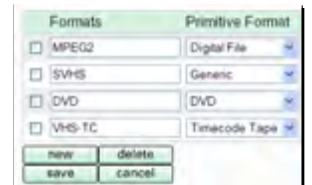
7. If there isn't a format called “MPEG”, add one by:

(a) Click the **“add”** button.

(b) Enter “MPEG” into the **“Name”** field.

(c) Select **“Digital File”** from the **“Primitive Format”** field.

(d) If you have more than one video server or need to distinguish between specific encoders, enter additional formats by repeating steps ‘a’ - ‘c’, naming each format a descriptive name that designates the target equipment, such as “MPEG-County Server” or “MPEG-Studio Encoder”.



If you have multiple video servers, you will almost certainly have to designate a format for each server. Otherwise, Cablecast will arbitrarily record and and play from either server, regardless of where the content is actually located.



If you have multiple encoders and one video server, it may not be necessary to establish multiple formats because each encoder will automatically copy its content to the video server after it is finished encoding the file. Since Cablecast will always replay from a single video server and is able to switch any device to either encoder, there is usually no reason to create a distinction between encoders.

(e) Click the **“save”** button.

8. Navigate to **“Location Settings : I/O : Devices”**. This is where you will tell Cablecast about the input for your encoder and/or each output of your video server.



If you purchased the video server/encoder with Cablecast, chances are that there are some entries already in this list. You will want to modify them for your installation. If your server has devices that are established for the video server, then you can modify these using the steps that you take to add new device entries.

9. To add device entries for the video server's *decoders*:

The screenshot shows a web-based configuration interface with four tabs: 'Shows', 'Schedule', 'I/O', and 'Autopilot'. The 'I/O' tab is selected. The form contains the following fields and values:

- Name: VS4-500 Output 1
- Router Address: 4
- Device Function: Playback only (dropdown)
- Device Type: Digital File (dropdown)
- Take Delay: 0 seconds
- Post Roll: 0 seconds
- Device CMS: Video Server (dropdown)
- Device Address: 0
- Device Formats: MPEG2 (dropdown)
- Device End Action: Stop (dropdown menu is open showing options: None, Stop, Rewind, Eject)

At the bottom of the form are two buttons: 'save' and 'cancel'. A mouse cursor is pointing at the 'save' button.

Figure 9.1: The "Device Edit" form for video server *encoders*.

- (a) If your creating a new device, click the "new" button. If you're editing an existing device, click the name of the device in the list and skip to step 'c'.
- (b) Click on the new device within the list in order to edit it. It will be called "New Input".
- (c) The video server has four decoders. Name this entry some thing like "Video Server 1", where "1" is the number of the decoder output, 1-4.



You do not need to define all four inputs. Many people choose only to incorporate one input for each channel on their Cablecast system, plus one extra for a preview output.

- (d) You should have plugged the output of the decoder into an input on your routing switcher. Enter that number into the “**Router Address**” field.
- (e) Select “**Playback only**” from the “**Device Function**” pop-down list.
- (f) Select “**Digital File**” from the “**Device Type**” pop-down list.
- (g) Enter “0” in the “**Take Delay**” field. This is telling Cablecast that the video server requires no time between the time that it receives the command and when it will actually start to play.
- (h) Enter “0” in the “**Post Delay**” field.
- (i) Select the control module set that you established in step ‘5’ from the “**Device CMS**” list.
- (j) In the “**Device Address**” field, enter the decoder output number, 0-3. That is, if you are working with the first output, enter “0”, second output “1” and so on.
- (k) Select the MPEG format that you created in step ‘6’ from the first “**Device Formats**” pop-down list. Leave the second two pop-downs blank.



If you created more than one format in order to distinguish between multiple servers, be sure you select the format for this server.

- (l) Set the “**Device End Action**” to “**Stop**”.
 - (m) Click the “**save**” button.
 - (n) Repeat these steps for each output of the video server that you wish to connect.
10. To add a new device entry for the video server's encoder or for an ENC-Series server, perform the following steps:
- (a) Click the “**new**” button, as necessary.
 - (b) Edit the new entry by clicking on its title.
 - (c) Enter a name for the encoder. If there is only one, “Encoder” might be appropriate. Otherwise, a more descriptive name will be necessary.

| | |
|---|--|
| Name: | VS4-Encoder |
| Device Function: | Record only |
| Device Type: | Digital File |
| Take Delay: | 0 seconds |
| Post Roll: | 0 seconds |
| Device CMS: | VS4-500-ENC |
| Device Address: | |
| Device Formats: | MPEG2 |
| Device End Action: | <ul style="list-style-type: none"> None Stop Rewind Eject Move File |
| Router Output: | 4 |
| Record Quality: | 6 mb/sec |
| Record Copy UNC: | |
| <input type="button" value="save"/> <input type="button" value="cancel"/> | |

Figure 9.2: This example illustrates setting up a device entry for a VS4-Series encoder. It is only slightly different for a stand-alone ENC-Series encoder.

- (d) Change the “Device Function” pop-down to “**Record Only**”. You will notice that the “**Input**” field disappears and the “**Output**” field appears at the bottom.
- (e) Change the “Device Type” pop-down to “**Digital File**”.
- (f) Leave “**Take Delay**” and “**Post Roll**” set at “0”.
- (g) Leave the “**Device Address**” field blank.
- (h) Choose the correct format for this device in the first “**Device Formats**” field. This is usually “**MPEG**” but you may have specified a unique format in step ‘6’.
- (i) *If this is the encoder included with a VS4-Series video server, then click on the “**Stop**” item in the “**Device End Action**” multi-select list and skip to step ‘k’. Otherwise...*
- (j) *If this is an ENC-Series stand-alone encoder, then hold down the ‘shift’ key and select both “**Stop**” and “**Move File**” from the “**Device End Action**” multi-select list.*
- (k) Enter the output on the routing switcher that this encoder is attached to into the “**Router Output**” field.
- (l) Select the desired recording quality for this encoder in the “**Record Quality**” field.



ENC-106 encoders and VS4-Series servers without the VS4-ENC10 option have a maximum quality of “**6mb/sec**”.

- (m) *If you are setting up a stand-alone ENC-Series encoder, enter the network path of the video server’s content share into the “**Record Copy UNC**” field. Example: “\\ServerName\ServerShare” or “\\192.168.1.3\ServerShare”. Make sure that this address leads the encoder into copying the file into the same directory that you established in step ‘5.a.iii’.*
- (n) Click the “**save**” button.

This concludes the configuration of the ENC-Series and VS4-Series servers within the Cablecast system. For information on how to test your setup, see the Cablecast Guide.

9.5 Maintaining the Video Server Storage RAID

All VS4-Series video servers employ a Redundant Array of Inexpensive Drives (RAID) storage system. RAID storage configurations use multiple hard drives, which are represented as one large hard disk to the server's operating system. There may be eight drives in your video server, but the server sees it as just one large hard disk.

The 'R' in RAID is for *redundant*. This means that one, *and only one*, of the drives in the disk array can fail without any loss of data. When the system detects a potential loss of data on one of the hard disks, it changes the status of the array to *degraded*.

A RAID may become degraded for any number of reasons: broken hard disk, computer reset, power spike or loss, loose cable, etc. . . A degraded RAID does not necessarily require a drive replacement.

Use this section to determine the most appropriate actions to take if your RAID has become degraded and .

9.5.1 Determining if Your RAID Has Been Degraded

The 3ware software that manages the RAID on your server will sound an audible alarm and flash a message on its VGA display that says, "Warning: The RAID is no longer fault tolerant."

If you close this dialog box and double click on the 3ware icon in the server's system tray, you will see a screen that looks similar to that in figure 9.3 on the next page. If your RAID has degraded, you'll see one of the drives listed as "**Not In Service**".

9.5.2 Configuring Email for 3ware controllers

In addition to the audio and visual alarms, the 3ware software may be configured to send you an email when it has an important message. To configure email notification:

1. Double-click on the 3ware icon in the server's system tray.
2. Click the "**Open Browser**" button.
3. Click the "**Settings**" button from the top menu bar.
4. Enter email setup information into the provided form.
5. Click the "**Enabled**" radio button to activate the feature.
6. Click the "**Save Email Settings**" button.



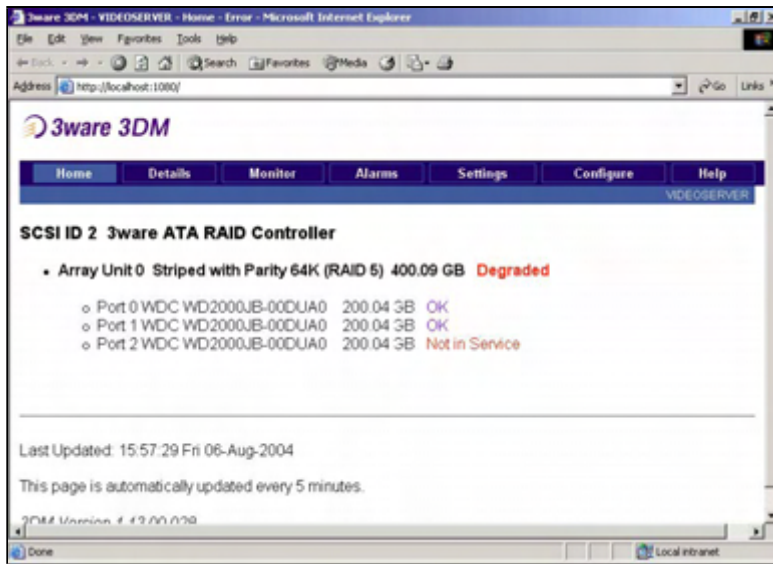


Figure 9.3: In this demonstration, you'll notice that the drive on "Port 2" has failed.

| | |
|----------------------------|---|
| Email Notification: | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| Sender: | <input type="text" value="VideoServer"/> |
| Recipient: | <input type="text" value="support@trms.com"/> |
| Server: | <input type="text" value="mail.myorg.org"/> |
| | <input type="button" value="Save Email Settings"/> |
| Email Test: | <input type="button" value="Send Test Message"/> |

Figure 9.4: The Email form in 3ware's web interface.

7. Click the **“Send Test Message”** button and check that you got a test email.
8. Edit as necessary, clicking the **“Save Email Settings”** button as you make changes.

9.5.3 Rebuilding the Array

Read through all of these steps before attempting to rebuild the array. There are some steps that require key combinations to be performed in a timely manner and it will help if you know that they are coming.

1. Double-click on the 3ware icon in the server’s system tray.
2. Each drive will be listed with a port number, as seen in figure 9.3 on the preceding page.
3. Note the port that is listed as **“Not In Service”**.
4. Note the number of drives that are listed as part of the array.
5. Reboot the server.
6. When the 3ware BIOS screen appears (figure 9.5), type ‘Alt-3’.



Figure 9.5: This is the BIOS screen for the 3ware controller. When you see it, type ‘Alt-3’ to enter the BIOS menu.

7. You will enter the **“3ware Disk Array Configuration”** screen. (figure 9.6 on the facing page)
8. You need to verify that all the drives are present before you attempt to rebuild the array. Look at the front of the server and count the number of drive bays that have power lights active on them. Cross check this with the number of drives listed in the BIOS screen, as shown in figure 9.6 on the next page. If you are missing a drive, skip to section 9.5.4 on page 93.
9. Highlight **“Array Unit-0”** using the arrow keys, as shown in figure 9.7 on the next page.
10. Hit the *‘enter’* key to select the array. Your selection will be noted by an **“*”**.

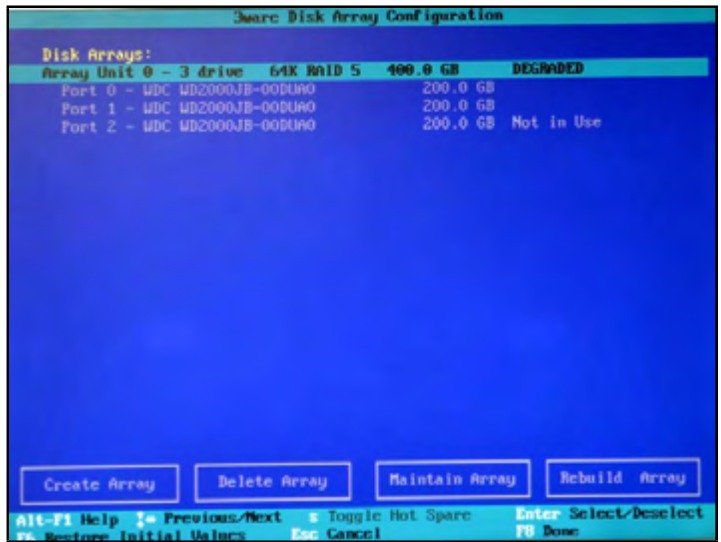


Figure 9.6: The 3ware Disk Array Configuration Screen.

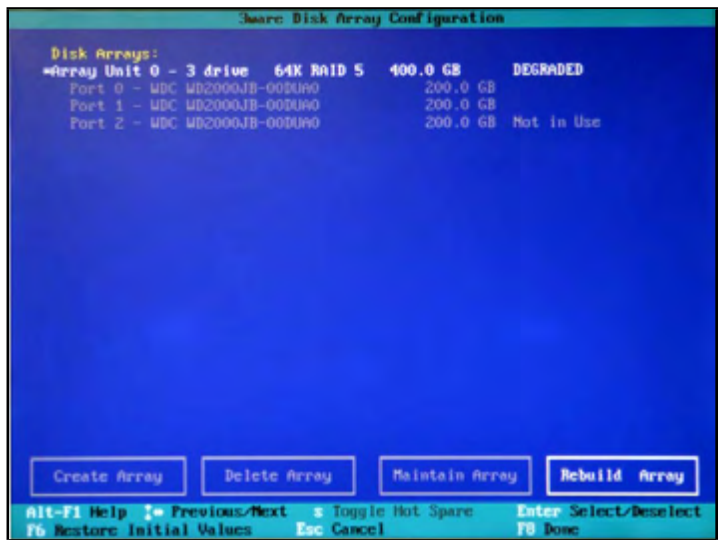


Figure 9.7: Select "Array Unit-0".

11. Use the arrow keys to highlight the **"Rebuild Array"** button and press 'enter'.
12. Confirm by pressing 'enter' again. (figure 9.8)
13. When you return to the main menu, press the 'F8' key and select **"Done"**.
14. You will be prompted to confirm that you want to begin the rebuilding process when the computer reboots. Press the 'y' key to confirm.
15. When the machine reboots, the rebuilding process will begin. The server will be sluggish during this process.

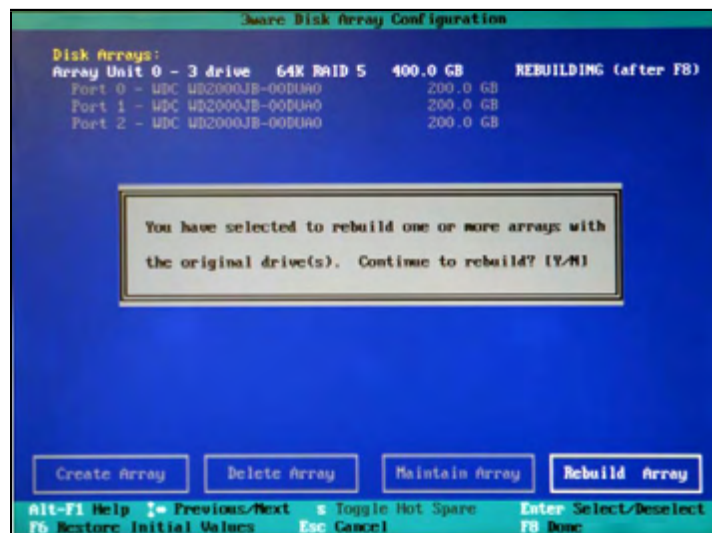


Figure 9.8: Confirming that you want to rebuild the array.

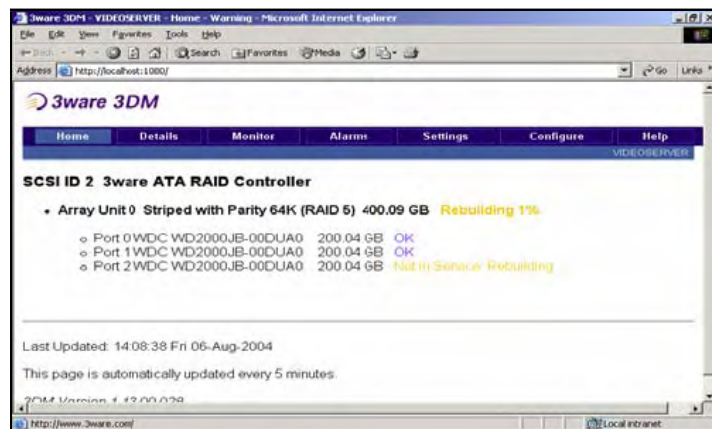


Figure 9.9: If you open the 3Ware interface, you'll notice that its status will now be set to "Rebuilding".

9.5.4 Checking Drive Connections

If one of the drives in the array does not appear in the web interface (figure 9.6 on page 91), the drive is either not responding or there is a bad connection. The first step is to reseal all of the drive and power connection to make sure that nothing has come loose.

If you are comparing a drive to a port number found in the 3Ware software, you can match the port number to the drive by counting from the top-most drive on the left side and going down, repeating top down for each row. The port number will begin with "0".

To reseal a hard disk:

1. If your system utilized drive caddies that are locked, use the included, round drive key to unlock the hard disk.
2. Remove the drive by pulling on the handle of the drive caddy. On some systems this handle will be purple, others it will be black.
3. Reseat the drive by applying equal pressure to the caddy as you insert it back into its slot. Make sure that the handle for the caddy is opened slightly before you apply pressure.
4. Open the top cover of the server
5. The back of the caddy housings will include connectors. Examine these connectors for any problems.
6. Follow the steps in section 9.5.1 on page 88 to see if the drive reappears. If it does not, then see the next section on replacing a bad hard drive.

9.5.5 Replacing Bad Drives

If rebuilding your array fails or you cannot get a drive to reappear, then you will need to replace the bad drive with a new one. Please contact Tightrope Media Systems' support for information on replacing your broken hard drive.

Appendix A

Cablecast Device Control List

This section includes information about all of the devices that Cablecast controls as of the date of this publication. Almost every month, a new device is added to Cablecast's control library. Be sure to check with Tightrope before you assume we cannot control a device that didn't make it on this list.

For a small engineering fee, Tightrope may be able to accommodate a device that is required for your installation.

A.1 Denon DVD2900

- **Physical Connections**

- This device requires an open RS-232 port.
- This device requires a *straight-through* cable. See Section [A.25.1](#) on page [105](#) for pin-out diagram.
- The device has a 9-pin **female** connector.

A.2 For Digital Rapids Encoders

- **Physical Connections**

- **The software that enables control of this device is optional.**
To purchase this software control module interface, order part number: "CBL:CM-DRStream".

- This device communicates using Telnet (port 23).
- The control module communicates with the server in real-time. Therefore the connection between it and the server must be reliable and fast. No more than a single Ethernet switch should separate the two.

A.3 VS4 Series Video Servers

- **Physical Connections**

- This device uses an Ethernet connection.

A.4 Extron MAV Series Routing Switchers

- **Physical Connections**

- This device requires an open RS-232 port.
- This device requires a *straight-through* cable. See Section [A.25.1](#) on page [105](#) for pin-out diagram.
- The device has a 9-pin **female** connector.

A.5 JVC SR-S365U SVHS VTR

- **Physical Connections**

- This device requires an open RS-232 port.
- This device requires a *null-modem* cable. See Section [A.25.2](#) on page [106](#) for pin-out diagram.
- The device has a 9-pin **male** connector.

- **Important notes about this device:**

- This control module also works with RS-232 controlled JVC Edit Desk Series machines.
- If this deck has the RS-422 card installed, use the RS422CM control module instead of this one.

A.6 8 I/O and Lower Knox RS Series Routing Switcher

- **Physical Connections**

- This device requires an open RS-232 port.
- This device requires a *straight-through* cable. See Section [A.25.1](#) on page [105](#) for pin-out diagram.
- The device has a 9-pin **female** connector.

- **Important notes about this device:**

- Do not use for routing switchers above eight inputs or eight outputs. Instead use the Knox64CM control module for routing switchers above 8 inputs or 8 outputs.

A.7 16 I/O and Higher Knox RS Series Routing Switchers

- **Physical Connections**

- This device requires an open RS-232 port.
- This device requires a *straight-through* cable. See Section [A.25.1](#) on page [105](#) for pin-out diagram.
- The device has a 9-pin **female** connector.

- **Important notes about this device:**

- Do not use for routing switchers below 16 inputs or 16 outputs. Instead use the Knox8CM control module.

A.8 Knox Pro Switch Series Routing Switchers

- **Physical Connections**

- This device requires an open RS-232 port.
- This device requires a *straight-through* cable. See Section [A.25.1](#) on page [105](#) for pin-out diagram.
- The device has a 9-pin **female** connector.

A.9 Leitch Routers (Terminal and Passthru Protocols)

- **Physical Connections**

- This device requires an open RS-232 port.
- This device requires a *null-modem* cable. See Section [A.25.2](#) on page [106](#) for pin-out diagram.
- The device has a 9-pin **male** connector.

- **Important notes about this device:**

- This control module description is valid for all Leitch Routers, regardless of protocol.

A.10 Leightronix Mini-T Pro

- **Physical Connections**

- **The software that enables control of this device is optional.**
To purchase this software control module interface, order part number: “CBL:CM-Lgx”.
- This device requires an open RS-232 port.
- This device requires a *straight-through* cable. See Section [A.25.1](#) on page [105](#) for pin-out diagram.
- The device has a 9-pin **male** connector.

- **Important notes about this device:**

- Even though the Mini-T Pro only has 8 inputs, you can use all 16 addresses on its ProBus.
- It is not required that your location use the Mini-T Pro’s routing switcher. Many stations connect a routing switcher directly to the Cablecast machine.
- If you are having trouble communicating with the Mini-T Pro and you are certain that you have the correct type of cable, check that the unit is set to 9600 baud and in “no modem” mode.

A.11 Leightronix MVP-2000

- **Physical Connections**

- **The software that enables control of this device is optional.**

To purchase this software control module interface, order part number: “CBL:CM-Lgx”.

- This device uses an Ethernet connection.

- **Important notes about this device:**

- It is not required that your location use the MVP’s routing switcher. Many stations connect a routing switcher directly to the Cablecast machine.
- This control module does not support any of the features in “**Autopilot: Digital File Management**”. Also, you will not see a status in the “**Autopilot: Force**” screen.

A.12 Leightronix Pro 8

- **Physical Connections**

- **The software that enables control of this device is optional.**

To purchase this software control module interface, order part number: “CBL:CM-Lgx”.

- This device requires an open RS-232 port.

- Leightronix ships the Pro 8 with the adaptor and cable needed to connect to the server. If you require a new cable, see Section [A.25.7](#) on page [111](#). A straight-thru 9-Pin cable with a 9-Pin to 25-Pin adaptor should work.

The device has a 25-pin **male** connector.

- **Important notes about this device:**

- Even though the Pro 8 only has 8 inputs, you can use all 16 addresses on its ProBus.
- It is not required that your location use the Pro 8’s routing switcher. Many stations connect a routing switcher directly to the Cablecast machine.
- If you are having trouble communicating with the Pro 8 and you are certain that you have the correct type of cable, check that the unit is set to 9600 baud and in “no modem” mode.

A.13 Leightronix Pro 16

- **Physical Connections**

- **The software that enables control of this device is optional.**

To purchase this software control module interface, order part number: "CBL:CM-Lgx".

- This device requires an open RS-232 port.
- Leightronix ships the Pro 16 with the adaptor and cable needed to connect to the server. If you require a new cable, see Section [A.25.7](#) on page [111](#). A straight-thru 9-Pin cable with a 9-Pin to 25-Pin adaptor should work.

The device has a 25-pin **male** connector.

- **Important notes about this device:**

- It is not required that your location use the Pro 16's routing switcher. Many stations connect a routing switcher directly to the Cablecast machine.
- If you are having trouble communicating with the Pro 16 and you are certain that you have the correct type of cable, check that the unit is set to 9600 baud and in "no modem" mode.

A.14 Leightronix TCD-1000

- **Physical Connections**

- **The software that enables control of this device is optional.**

To purchase this software control module interface, order part number: "CBL:CM-Lgx".

- This device requires an open RS-232 port.
- Leightronix ships the TCD-1000 with the adaptor and cable needed to connect to the server. If you require a new cable, see Section [A.25.7](#) on page [111](#). A straight-thru 9-Pin cable with a 9-Pin to 25-Pin adaptor should work.

The device has a 25-pin **male** connector.

- **Important notes about this device:**

- It is not required that your location connect the routing switcher to the TCD-1000. Many stations connect a routing switcher directly to the Cablecast machine.

- If you are having trouble communicating with the TCD-1000 and you are certain that you have the correct type of cable, check that the unit is set to 38400 baud and in “no modem” mode.

A.15 Leightronix TCD-IP

- **Physical Connections**

- **The software that enables control of this device is optional.**

To purchase this software control module interface, order part number: “CBL:CM-Lgx”.

- This device requires an open RS-232 port.
- This device uses an Ethernet connection.

- **Important notes about this device:**

- It is not required that your location connect the routing switcher to the TCD/IP. Many stations connect a routing switcher directly to the Cablecast machine.
- Before you upgrade the BIOS on your TCD/IP, check with Tightrope support staff for compatibility issues.
- Keeping a copy of WinTCD handy is a good idea, as the program is useful for troubleshooting and maintenance.

A.16 Panasonic 232 Protocol Devices (AG7100, 7150, etc.)

- **Physical Connections**

- This device requires an open RS-232 port.
- This device requires a *straight-through* 9-pin to 25-pin cable. See Section [A.25.7](#) on page [111](#) for pin-out diagram.
- The device has a 9-pin **male** connector.

- **Important notes about this device:**

- No Special notes for this device.

A.17 Pioneer DVDV7400 and V5000

- **Physical Connections**

- This device requires a *straight-through* cable. See Section [A.25.1](#) on page [105](#) for pin-out diagram.
- The device has a 9-pin **male** connector.

A.18 Pioneer DVDV7400 and V5000

- **Physical Connections**

- This device requires a *straight-through* cable. See Section [A.25.1](#) on page [105](#) for pin-out diagram.
- The device has a 9-pin **male** connector.

A.19 Pioneer DV-F07

- **Physical Connections**

- This device requires an open RS-232 port.
- This device uses a custom cable, illustrated in Section [A.25.6](#) on page [110](#).
- This device has a 15-pin male connector.

- **Important notes about this device:**

- Rumor has it that this changer is more reliable when DVD-R's are used.
- Sticker labels are problematic with this device.

A.20 Sierra SVS Series Routing Switchers

- **Physical Connections**

- This device requires an open RS-232 port.
- This device uses a special cable which is illustrated in Section [A.25.3](#) on page [107](#).
- The device has a 9-pin **female** connector.

- **Important notes about this device:**

- Sierra routers that support the SVS protocol. NOTE: the router must be in command mode by setting !!HOST1**

A.21 Sigma Routing Switchers

- **Physical Connections**

- This device requires an open RS-232 port.
- This device requires a *null-modem* cable. See Section [A.25.2](#) on page 106 for pin-out diagram.
- The device has a 9-pin **female** connector.

A.22 Sony DVP-CX777ES

- **Physical Connections**

- This device requires an open RS-232 port.
- This device requires a *null-modem* cable. See Section [A.25.2](#) on page 106 for pin-out diagram.
- The device has a 9-pin **male** connector.

- **Important notes about this device:**

- Sticker DVD labels do not work well with this changer.

A.23 Tascam DVD6500 DVD Player

- **Physical Connections**

- This device requires an open RS-232 port.
- This device requires a *null-modem* cable. See Section [A.25.2](#) on page 106 for pin-out diagram.
- The device has a 9-pin **male** connector.

A.24 Tightrope 422 Control

- **Physical Connections**

- **The software that enables control of this device is optional.**
To purchase this software control module interface, order part number: “CBL:CM-422”.
- Devices using this control module will need an open RS-422 Port.
- This device requires an open RS-422 port.
- This device requires a *422-video* cable, unless it is used with Tightrope’s internal 422 adapters. When used with Tightrope’s internal 422 adapters, use a *straight-through* cable. This does not include Tightrope’s USB-422 adapter, which require the specially wired *422-video* cable. For pin-outs, see Section [A.25.4](#) on page [108](#) for internal serial cards and Section [A.25.5](#) on page [109](#) for external USB to Serial adaptors.
- Generally, the devices will have a 9-Pin Male connector. Check your specific device to be sure.

- **Important notes about this device:**

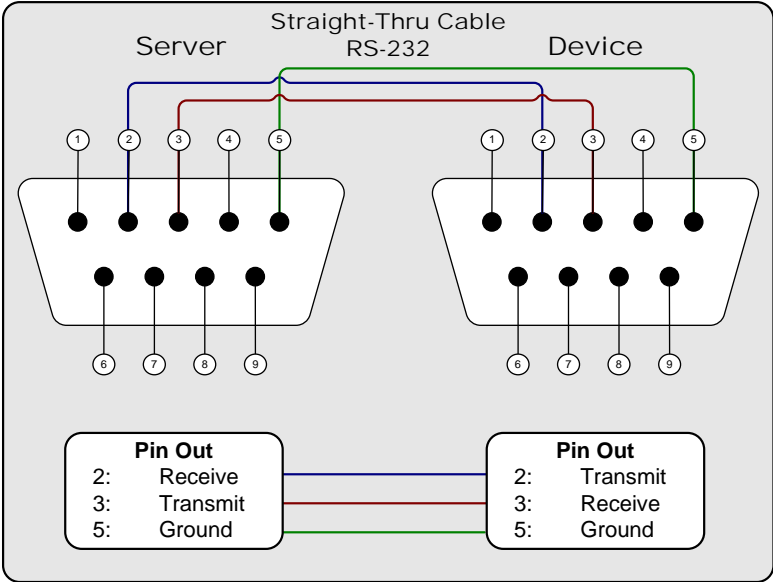
- This control module supports Sony Protocol devices and VDCP compatible servers.
- If you are having trouble communicating with your 422 device, be sure of two things:

First, check the cabling. Be sure you read the notes at the top of this section.

Second, check that the device is set for 422 control and not local mode.

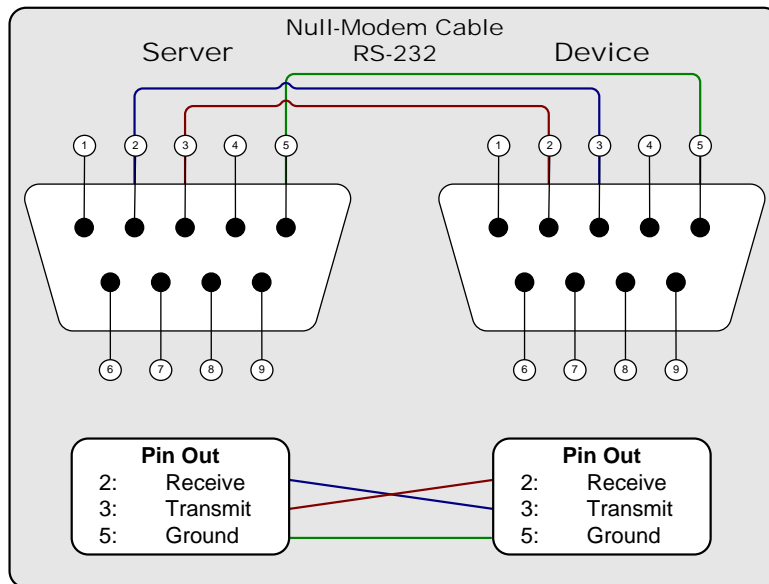
A.25 Cable Pin-Out Diagrams

A.25.1 RS-232 9-Pin Serial Cable: Straight-Thru



Use cables:
ACC:9P-FF-6FT
ACC:9P-FF-10FT
ACC:9P-FM-6FT
ACC:9P-FM-10FT

A.25.2 RS-232 9-Pin Serial Cable: Null-Modem



Use cables:

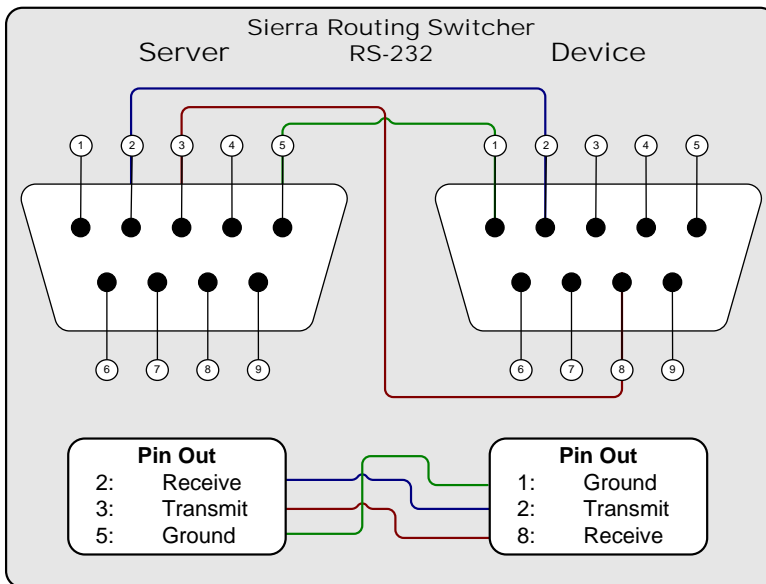
ACC:9P-FF-6FT-NULL

ACC:9P-FF-10FT-NULL

ACC:9P-FM-6FT-NULL

ACC:9P-FM-10FT-NULL

A.25.3 RS-232 9-Pin Serial Cable: Sierra Routers



Use cables:

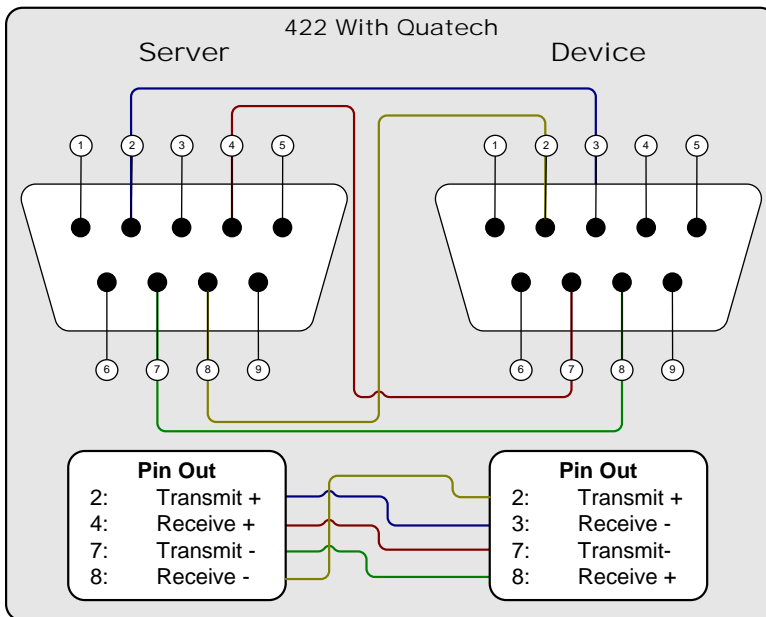
ACC:9P-FF-6FT

ACC:9P-FF-10FT

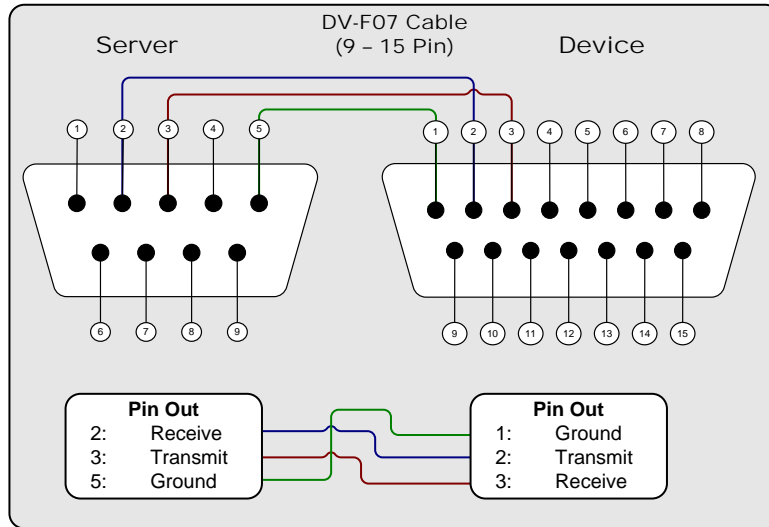
ACC:9P-FM-6FT

ACC:9P-FM-10FT

A.25.5 RS-422 9-Pin Serial Cable: With Multi-Port USB-Serial Converters

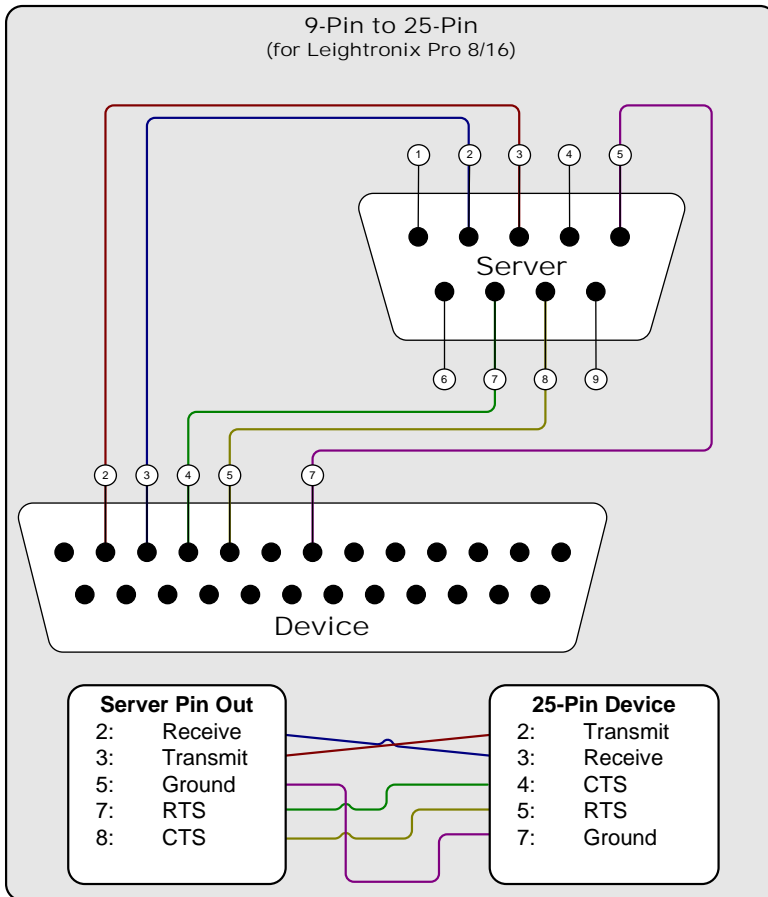


A.25.6 RS-232 9-Pin to 15-Pin Serial Cable: For Most Pioneer



Use cables:
ACC:PIO-6FT
ACC:PIO-10FT

**A.25.7 RS-232 9-Pin to 25-Pin Serial Cable:
 For Leightronix Pro 8/16**



Appendix B

A Not-So-Short Introduction to Networking

B.1 Introduction

If you are not a network person by profession or hobby, this paper may serve as a helpful guide in understanding some basic concepts. We overview networking rules, conventions and issues. This guide was written with Tightly installations in mind, but the basic concepts are universally applicable.

None of the information in this paper should be considered complete. Many difficult concepts are glossed over and oversimplified. Our goal is to provide you with useful information that may lead you to accomplishing your goals—or at the very least communicate those goals to someone who can do it for you.

B.2 The Basics: What is a Network?

A computer network is a group of computers connected by hardware and software that are able to *directly* communicate with each other.

The word 'directly' is emphasized in our opening paragraph because it is possible for computers to communicate even when they are on two different networks, but that ability does not make their networks into a single entity—they are two different networks. It is important to limit the definition to "direct communication" because we need to differentiate between the meaning of a single network and a group of networks. Often, people say 'network' when they mean "wide area network"

(WAN), which is a term used to describe several networks that are interconnected and under the control of a single organization. Computers can communicate with any other computer on the WAN, but they must do so through the use of networking equipment that is able to route traffic *between* networks within the WAN. This is not the same as “one big network”. Some will try to emphasize that you are speaking about a single network by using the term “local area network” (LAN), but this is no more precise than just using the word ‘network’. In this document, “local area network” and ‘network’ mean the same thing. Much of the text clarifies the mechanics of these difference, so if you don’t “get it”, that’s ok; you can come back to this later. :)

On most networks, all computers are considered peers. That is, there is nothing inherently special about a server in the network closet that makes it different than the computer sitting on your desk. It is the roles that we assign these computers that make them special.

These ‘roles’ are called *services*. They include web servers, email, file servers, time synchronization, security authentication and many others. There are thousands of services that may be provided on any network.

99% of local area networks are using Ethernet hardware and a software networking package¹, which is usually included with the computer’s operating system.

The key to understanding a network is to see it as one group of computers that is wired together both:

physically All of the computers are wired together with network cabling and can electrically ‘get’ to each other.

logically All of the computers are configured so that their network software represents them as “on the same network”.

Physical connections are straightforward. In most networks today, you have Ethernet cables (CAT5e) that connect computers to an Ethernet switch, which is a box that is able to send networking signals between computers in an efficient way. When everything is connected to the same switch, you have a simple network that is just begging for the connected computers to be configured in such a way that they can communicate with each other.

The logical side of networking refers to the protocols, software and configuration that make up a network. In the post Internet Boom, almost every network in existence runs on an Internet Protocol (IP) network. IP networks have four basic components that are within the scope of this article². The rest of this section is devoted to those components.

¹... which is called a *stack*...

²...and a million that lie outside it. :)

B.2.1 IP Address

If you know one thing about networks, it is probably the concept of the IP address. On any network, every network interface³ must have a unique IP address⁴. An IP address is a number that, for the sake of readability, is broken up into four numbers separated by a period (.). Example: “192.168.1.1”.

Each of the four numbers must be between 0 and 255. When we speak of a computer’s IP address, it’s important to understand that there are many addresses that are not considered valid because they are reserved for special purposes. That is, “0.0.0.0” and “255.255.255.255” are examples of addresses that are not considered valid. “127.0.0.1” is another special address called the *loopback address*. It represents the local computer and is effectively saying, “go to me and ask myself for something⁵”.

Another important concept to understand is that in an IP network, the IP address serves two purposes. The first purpose is to identify the network and the second is to identify a specific network interface on that network.

When we say “identify the network”, we are alluding to the fact that the complete range of possible IP addresses are always segmented into smaller networks. That is, no valid network has an IP address range of 0.0.0.1 to 255.255.255.254⁶. We break them up into smaller chunks for manageability reasons.

How do we determine the part of the IP address that signifies the network and the part that identifies a specific computer on that network? We do that with the...

B.2.2 Subnet Mask

Put simply, the subnet mask’s job is to split an IP address into a network address and a host address. This helps networking software determine when an address falls within the local network and when it does not.

Like an IP address, a subnet mask is a group of four numbers separated by a period. Each of the four numbers must always be between 0 and 255.

The subnet mask is a bit mask. Since computers think in “0’s” and “1’s”, it can quickly take this number and *mask* it over the IP address. Whenever there is a “1”

³The term *network interface* is more precise than saying *computer*, because a computer might have more than one network card or the connecting device might not be a computer. *Network Interface* covers any host on a network.

⁴This is probably true for every scenario that you will come across. There are special cases where a computer might have the same IP address on the same computer, usually for redundancy or performance reasons in high capacity installations. We mention it in a footnote so that when a network nerd corrects you on this point, you can say, “Yeah, I know.”

⁵One of my close friends, and one of the biggest nerds that I know, has a bumper sticker that reads, “*There’s no place like 127.0.0.1*”. It is at Thinkgeek.com if you want your own.

⁶255.255.255.255 is special, so we don’t include it in the standard IP address range.

in the mask, it associates the corresponding bit in the IP address as a “network address”. When it sees a “0” in the subnet mask, the computer thinks “computer’s address”.

Examine the table below. We can see how a computer is able to separate the network address from a specific computer’s address by using a subnet mask.

| | Decimal | Binary |
|------------------------|---------------|---|
| IP Address | 192.168.1.1 | 11000000.10101000.00000001.00000001 |
| Subnet Mask | 255.255.255.0 | 11111111.11111111.11111111.00000000 |
| Network Portion | 192.168.1.X | 11000000.10101000.00000001.XXXXXXXXXX |
| Address Portion | XXX.XXX.XXX.1 | XXXXXXXX.XXXXXXXXXX.XXXXXXXXXX.00000001 |

After reading the last four paragraphs, you should be very confused. If not, you probably don’t need to read this paper. :) So let’s explain things a little further.

As an example, that is technically illegal, a subnet mask of “0.0.0.0” would define any computer IP address as being within your network. Generally this is not a number that you will ever see. Conversely, “255.255.255.255” would define a network with exactly one computer on it⁷. As the example in the previous table shows us, “255.255.255.0”⁸ would mean that all computers that shared the first 3 numbers of their IP address would be on the same network.



If you are interested in the math, networking software performs a bitwise AND operation on the IP address of the local network interface and the subnet mask. It then performs the same operation using the destination’s IP address to determine if they are within the same network. If not, the network communication is sent to the network’s router. For a detailed explanation of subnet masks, see [Wikipedia.org](https://en.wikipedia.org).

The bottom line is that the purpose of the network’s subnet mask is to help computers decide if a communication request is within the network by separating an IP address into two parts: a network address and a host address. If a communication request does not fall within a computer’s network, we involve the...

B.2.3 Network Router

A network router, also known as the *default gateway*, sits on the edge of your network and handles traffic *between* networks. When you are at your computer and you ask for a computer that’s not in your local network, that request is sent to

⁷Sometimes this value is used when you are using an old-time modem.

⁸All of our examples are with either “255” or “0”. Other numbers are possible, but not any number. Specifically, if you read a subnet mask in binary from left to right, all of the “1’s” would be packed together followed by all of the “0’s”. There may be no “0’s” before any “1’s” in a valid subnet mask.

your router. Using magic⁹, your router figures out how to get to the computer that you are asking for and the connection is complete. If it cannot, then you get an error.

Incidentally, if your network did not have a router then any request that didn't fall within your subnet would be considered unreachable.

B.2.4 Domain Name System (DNS) Address

When you type an address into your web browser, you typically type a name, such as "www.trms.com". Imagine if we had to remember the IP address for every site that we wanted to visit!

DNS is a service that is able to resolve names to IP addresses. When your computer gets a name instead of an IP address, the computer listed as the DNS server will be asked to translate it.

If you have spent any time with your web browser, you'll notice that all of the names that you type end in a common suffix, like '.com', '.org', '.uk', etc. These are called *top level domains* and are governed by various organizations, depending on the specific domain in question.

The name that comes directly before the last dot (.) is called the *second level domain*. Examples of these would be "whitehouse.gov" or "trms.com". Second level domains are managed by various domain name registration companies including [Network Solutions](#) and [Register.com](#). If you want to reserve one for your organization, you simply go to one of these companies, search for an available name and pay them some money. When you're picking a name, you can choose the top level domain that is most appropriate for you, naming yourself "myfantasticname.org" or "myfantasticname.com". You can even be both, if the names are available.



Some top level domains work differently than standard ones like ".org" and ".com". For example, not just anyone can get a ".mil" address as those are reserved for the United States Military. In the United States the ".us" works a bit differently for schools in that second, third level and fourth level domains are used to drill down to a specific district. For example, the Bloomington school district in Minnesota is at "bloomington.k12.mn.us". The fifth level domain is managed by the school for internal domains, computers and services.

If you have your own domain name, you or your organization is responsible for managing it. You have the responsibility to designate a DNS server that will manage any requests that are sent to your new domain. Your DNS server tells the world, "When people look for www.myfantasticname.org, it is at *this* IP address."

⁹There is a lot of 'magic' in this document, because we can't cover everything.

Most often, when you type an address into a web browser, there are three parts to an address, like “www.trms.com”. The “www” in that address is the *third level* domain. Any domain beyond the second level domain is managed by the organization. They are used to designate specific services or computers within an organization’s network. As an example, your computer on your desk is most likely named with a third and possibly fourth level domain, depending on the complexity of your network.

Domain levels are like a tree where the top level is the trunk and each subsequent level is a branch that comes off of the previous level. The highest level domain might be considered the leaf, which represents a service or a specific computer. There can be any number of levels to a domain. See figure B.1 for an illustration of domain levels.

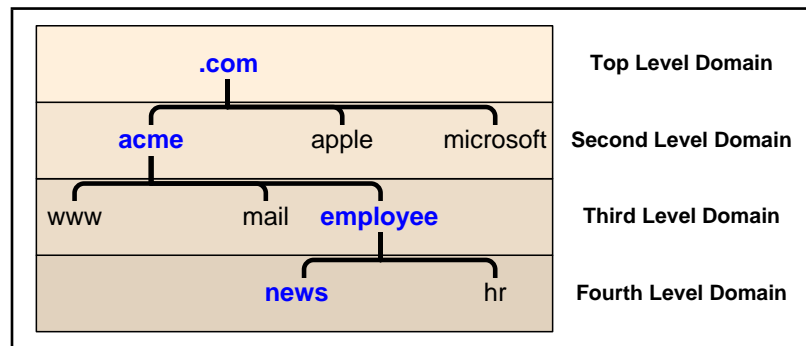


Figure B.1: The above example illustrates how domain names are structured, where each level drills down into a specific service or computer. To get to the “news” computer, you would use the “news.employee.acme.com” domain name.



When you refer to a computer’s name, you might say “news” or be more specific and say “news.employee.acme.com”. The full name is known as the *fully qualified domain name*.

Domain levels higher than the second are particularly interesting to Tightrope customers who are operating within an established network, as they may provide a means of addressing your server even if there is already an existing one. In fact, this is how Tightrope operates its demonstration site, which is a full-blown Cablecast and Carousel system. If you go to “www.trms.com” you get our corporate web site. If you go to “demo.trms.com” our network hardware and configuration is able to redirect you to the demonstration system. We will explore this topic further when we talk about firewalls and port forwarding.

B.2.5 Summary of Basic Network Concepts

All computers on a network must have an IP address that is unique so that other computers can find them. All computers on a network will have the same subnet mask, which is just a number that defines the size of the network. Using math, the networking software on your computer is able to figure out if an IP address is inside or outside your network based on this subnet mask. If it is outside the network, your computer will forward your request to the router on your network that will, using magic, forward it off to the computer with which you are trying to communicate. If there is no router defined, then you can only communicate with computers within your network.

DNS servers interpret friendly names that humans understand, like “www.trms.com”, into numbers that computers understand, like “64.122.237.46”. If there is no DNS server defined, then you will have to use IP addresses and not names.

B.3 Dynamic Addresses and DHCP

Imagine that you are a network administrator for a new organization that just received 500 desktop computers. Your first task is to get these computers on your network. You begin assigning each computer an IP address, subnet mask, DNS and router information. This would be extremely time consuming, but you get it done thanks to your hard work and dedication to repetitive tasks.

Now imagine that it is a year later. Some of these computers have broken and been replaced. Thirty of them got a virus and needed to be rebuilt. You added another 100 computers to one department and got rid of 30 from another. . .

You can see how time consuming network administration can become when you have to manually enter the networking information into a large number of computers! Enter a magic technology: Dynamic Host Configuration Protocol or DHCP.

DHCP is a service that runs on a network. If a computer is configured to use DHCP, it will seek out this service and automatically configure its network settings using the DHCP service’s instructions.

Typically, if your computer uses DHCP it leases an IP address. This means that your IP address can change after a predetermined amount of time. We call these addresses *dynamic IP addresses*. If your computer is sitting on your desk and you use it for email and surfing the web, this is fine. Nobody cares about your IP address because nobody relies on your computer for any network services.

Dynamic IP addresses are a problem if your computer does have services that people need to find. For example, a web server¹⁰ needs to be at a fixed IP address because people need to know where they can find it.

¹⁰ . . .like Tightrope’s Cablecast or Carousel computers. . .



Using DHCP does not have to mean a dynamic address. DHCP can be configured to make a specific computer's address static. There are other features of DHCP that are worth exploring. Check out [Wikipedia.org](https://en.wikipedia.org) for detailed information about it.

The bottom line is: DHCP is a service that automatically configures networking on a computer and usually gives it a dynamic IP address. Desktop computers are generally configured with DHCP and servers, like those from Tightrope, can only use this service if the address it gets is static and not dynamic.

B.4 TCP and UDP Glossed Over

Within a network, communication is happening. Computer A is saying something to computer B and they both must agree on how that communication is established and negotiated. There is a protocol to it all, like a handshake when you meet someone new.

There are two primary methods for communicating on IP networks that are within the scope of this paper: TCP and UDP.

TCP stands for Transmission Control Protocol. We don't care why it's called that, but we do care that TCP is the most common way that two computers will communicate on a network. It is the TCP in TCP/IP networks. TCP is a connection-based protocol that is able to guarantee proper communication between two computers. It is a reliable stream of data that is guaranteed to reach the destination with the same data in the same order¹¹.

We say that TCP communication is *connection-based* because before data is transmitted, a connection is established. Just like picking up a telephone to call your neighbor, communicating with TCP means that you establish the connection first, then you begin communicating. When you're done 'talking', you hang up, or drop the connection. Because there is a constant connection, the two communicating computers are able to monitor the packets of information, ensuring their correctness and that they arrived. The down side is that these connections have a significant amount of overhead that each communicating computer must deal with.

By contrast, imagine that you are leaving your office and before you shut the door you yell out, "Bye! Lock up before you leave!" Did anyone hear you? Who knows?! You left before you got a response.

UDP is much like yelling in the dark. It stands for User Datagram Protocol and using this method, the computer sending the data packages the information into a datagram and sends it into the network. You have to rely on *hope* that it will get

¹¹But not necessarily immediately, as it uses retransmission to achieve those guarantees.

to its final destination¹² because Unlike TCP, UDP does not require a connection before communication can occur. Furthermore, it does not make any promises about “if”, “when” or “in what order” each UDP message will arrive. If a UDP datagram doesn't make it to its destination, your networking software will not return an error.

UDP datagrams usually contain a return address so, if a response is expected, the computer that receives the datagram knows where to send it.

UDP has very low overhead and is therefore very popular to use for services where success does not need to be guaranteed, like synchronizing your computer's clock or streaming audio on a Voice over IP (VoIP) call¹³.

We talk about these two communication types because there are important limitations when dealing with UDP and network address translation, a topic we explore in section B.7 on page 123.

B.5 Network Ports

As we learned a couple of sections ago, every computer on a network must have a unique IP address. It is kind of like a temporary serial number in that it identifies one specific computer on one specific network.

But there are many things to do on a network and they can all happen at the same time! We may know where a computer is, but how do we address the service that is on the computer that we want?

Think of a cable box. A cable box sits on top of your television and it is addressed by your cable company using its serial number (IP address). When you turn your TV on and flip through the channels on your cable box, you receive different television shows (services) from the channels (ports) that your cable company provides.

Networks are similar in that communications are handled on ports, which are like a channel. When you ask for a web page, you basically say, “Hey computer, I need to ask port 80 to give me your home page and send it back to me at IP address 208.40.80.2 on port 51,589”, where 51,589 is any arbitrary port number that your computer has available. The server responds back with, “Hey, so you want to talk?” Your computer says, “Yup!”. The connection is then established¹⁴.

Some port number assignments are governed by The Powers That Be¹⁵. Port 80 is

¹²Most services that use UDP, such as DNS, implement their own retransmission strategy, so it's a bit more complicated than “yelling in the dark”. :)

¹³If a chunk of audio doesn't arrive in the right order, the receiver can buffer it or drop it since there is no time to retransmit. In VoIP, low latency is much more important than complete accuracy.

¹⁴Nerds call this process *The Three Way Handshake* or *SYN-SYN/ACK-ACK*, which reminds this author of the movie “*Mars Attacks!*”

¹⁵[The Internet Assigned Numbers Authority](#)

HTTP (a.k.a. the web), port 21 (both UDP and TCP) is FTP, mail is port 25—there are thousands of services that are available on a network. Some are famous and are always expected on a specific port. Others are arbitrarily assigned by their designer and may conflict with someone else's choice.

There is a lot more to ports and how they work. For our purposes, it's enough to know that IP addresses are used to locate computers while ports are used to locate services on those computers and to facilitate multiple connections between different computers at the same time.

It is important to understand ports because the topic will come up when we explore NAT and firewalls in later sections.

B.6 Private and Public IP Addresses

There are hundreds of millions of computers and hundreds of thousands (if not millions) of networks in operation throughout the world. The geniuses that invented the Internet back in the 70's never imagined that everyone and their mom would be using it. The result is that there are not nearly enough IP addresses to accommodate the number of devices that are using the Internet.

To alleviate this problem, The Powers That Be¹⁶ decided to reserve three blocks of addresses for private networks:

10.0.0.1 - 10.255.255.255

172.16.0.1 - 172.31.255.255

192.168.0.1 - 192.168.255.255



History dictates that not only are these private address blocks differently sized, they are also segmented differently. For example, the "192.168.x.x" block is most often represented as 256 different networks with 255 IP addresses each, with a subnet of "255.255.255.0". Since these addresses are private, there is nothing written in stone about how you segment your network. It's just what other networking types would expect to see when they look at your network configuration.

Someone that decides to use these IP addresses can do so without any coordination with an outside organization. That is because by their very definition, routers on the Internet will not view these as addresses that they can route. That is why they are called *non-routable* or *private* IP addresses.

Addresses that are outside the range of those listed above are considered *route-able* or *public*. If you arbitrarily choose a public IP address and then connect it to a router

¹⁶Again, [The Internet Assigned Numbers Authority](#)

which is connected to the Internet, you will create problems and your network will not work correctly.

People creating networks in their own organization almost universally use private IP addresses. Back in the early days of the Internet, this was thought of as a second-class solution. Now reality has set in, addresses are scarce, security concerns abound and we all have private IP addresses on our desktop computers¹⁷.

The trouble with a private address is that you cannot communicate with anyone outside your network. If I try to go to “www.trms.com” and my computer uses a private IP address, the remote computer will not know where to respond to because the routers that are in between our two computers will not allow traffic to go back to a private IP address.

If this is true, then how is it that we all have private IP addresses and we are still able to communicate on the Internet? That question leads us to our next section...

B.7 Network Address Translation

Network Address Translation (NAT) is a magic technology that makes our Internet possible. Without it, there would be a lot fewer computers on the Internet and that would be a Bad Thing. But what is NAT?

NAT is a feature of a router¹⁸ that enables computers inside your network that are using private IP addresses to communicate with computers on the Internet.

When you ask for something that is outside your network, your computer goes to the router. A router using NAT, in turn, completes the request *on your behalf*. The destination computer then establishes a connection with your router and your router is responsible for marshalling the packets back to you.

Your computer thinks that it is communicating directly with the destination computer and the destination computer thinks that it is talking to you from your router's address¹⁹.

Because TCP communications are based on a connection and that connection is basically established by information that is stored in the packets of data that are a part of that communication, NAT works²⁰.

¹⁷For fun, open up a command prompt on your desktop computer. Type “ipconfig”. Chances are that your address falls within one of the ranges listed above!

¹⁸You'll remember that a router routes IP traffic to remote computers. A router is at the edge of your network and links it to other networks.

¹⁹Incidentally, the destination computer sees you as your router, but if they're aggressive enough, they can mine your private IP address out of the packet. That's how online poker games know if you're cheating! :)

²⁰... mostly. :) There are times when NAT fails even with TCP. Examples include certain kinds of FTP, MSN messenger file transfers and others.

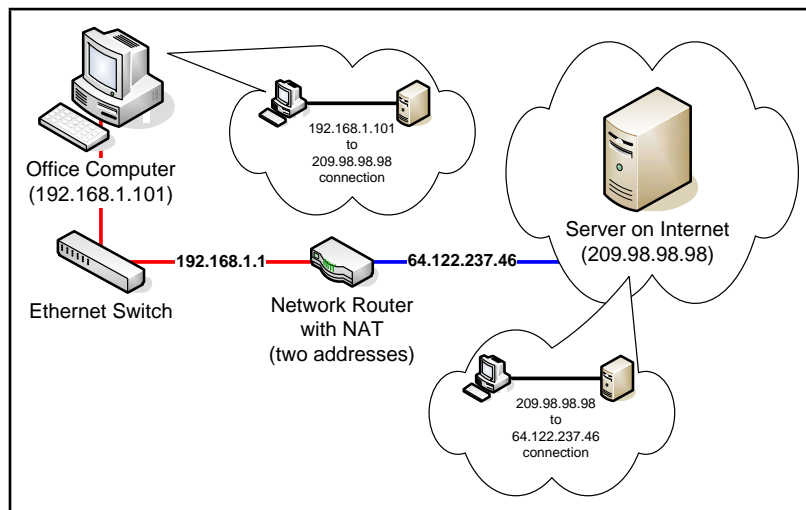


Figure B.2: A router with NAT will use at least two addresses. In this example they are (“192.168.1.1”) for the local address and (“64.122.237.46”) for the public IP address. Local computers address it from the “192. . .” address. Computers on the Internet ‘see’ your computer as though it has the “64. . .” address. When you communicate with a computer outside of your network, your router uses NAT to make the connection on your behalf.

NAT does not work very well with UDP communication because there is no connection, and thus no handshake with which to base future communications upon. Fortunately, some newer routers are able to make educated guesses about where incoming UDP datagrams should be sent²¹ based on outgoing UDP datagrams that your computer recently sent. Educated guesses and occasional failures are an accepted part of UDP-over-NAT because the spirit of UDP is to be unreliable.



Despite the modern UDP-enabling features of NAT equipped routers, there are many administrative and protocol headaches associated with NAT. Since NAT came after the design of the Internet, it wasn't a part of the underlying design of IP networking. As a result, it violates basic assumptions embedded into the design of the Internet to accomplish its amazing feats.

It is for this reason that we all look forward to a day when a new version of IP networking, called IPv6, is able to finally retire the current one.

The key thing to remember about NAT is that there are two connections: you with the router and the router with the destination. The router makes a connection *on your behalf* and forwards all return packets back to your computer. For the most part, it works just like if your computer were directly connected to the destination computer.

B.8 Firewalls

A firewall is a device or a feature on a router that is able to block specific IP traffic based on a set of rules. Firewalls were traditionally installed on the edge of your network, but have become an important feature of operating systems and software firewalls are now found on many desktop computers.

To understand the significance of firewalls, we need to acknowledge a troubling fact: *all non-trivial computer systems have bugs*. It doesn't matter what platform you operate on or if you are up to date with your "Microsoft Patches". There are bugs in your system and many of them can be exploited to gain access to your network resources.

One of the central purposes of a firewall is to block access on your network so that bad people can exploit fewer bugs. :) Why expose a service to the Internet that might be a "way in" when you are not even using it? In fact, it doesn't even need to be a bug to allow access. What happens if you have a web server running on your computer that isn't configured properly? It is just waiting for someone to "configure it for you".

²¹... using a feature called UDP NAT Traversal

Firewall rules may be set for incoming traffic and outgoing traffic. Incoming traffic refers to traffic from outside the network coming into your network. Outgoing traffic refers to requests made from within your network to the outside. Incoming rules help protect your computer from attacks. Outgoing rules help protect everyone else from your computer should it fall victim to a virus or hacker.

The most common type of rule that a firewall will follow is a port rule. These rules simply block traffic, either incoming or outgoing, on a specified port. For example, your firewall may block all traffic on TCP port 23, which is commonly used for the telnet service.

Other rules might be based on traffic that comes from specific IP addresses. Your firewall may be configured to block all incoming traffic on port 23, except when it comes from an IP address that is from a remote location within your organization.

B.8.1 Dire Warning About Firewalls

Many people view a firewall as *the answer* to their security issues. They are not. In fact, firewalls are really just a small (but important) part of an overall security strategy.

Firewalls do not address the human elements of security, like 'phishing' scams and viruses that come through email attachments. Furthermore, they do not stop attacks on the services that you do expose on the Internet.

Also, there is something called the "chewy middle" of your network that can completely negate a firewall's effectiveness. This is where someone within your network shows some initiative by installing a \$40 wireless access point and provides anyone within a reasonable proximity to your network full and un-encrypted access to the inside.

B.9 Port Forwarding

Port forwarding is a feature of a router that is typically used in conjunction with NAT and firewalls. This feature forwards incoming traffic on specified ports to addresses that are inside the network. An example of port forwarding might be, "Forward all incoming traffic on TCP port 80 to the computer at "192.168.1.3".

Port forwarding is at the heart of many networks that provide services on the Internet. It is a fantastic way to partially shield a computer behind a firewall while allowing specific traffic through to services that are running on that computer.

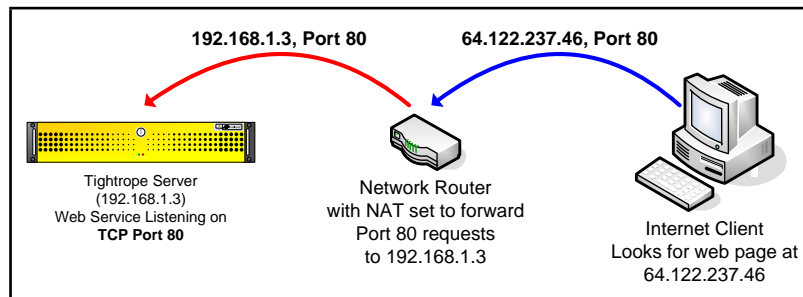


Figure B.3: In this example, a computer on the Internet is looking for a web site that you are hosting behind a router configured with NAT and port forwarding. It looks for the site at your router's external IP address and the router forwards that request to your web server.

B.10 Virtual Private Network

A Virtual Private Network (VPN) is a method of extending a private network to computers that are located on a remote network through the use of a public networking infrastructure. When you use a VPN from home to get into your work's network, you are making a connection *on top of* your Internet connection. You are, in effect, dialing into your work's network over the Internet.

This new connection is an encrypted link that effectively joins your home computer to your work's network. This connection includes its own IP address, subnet mask, DNS address, etc. It is a new connection in every sense of the word. Your home computer now has all of the rights and privileges that you would normally have if you were on your computer at work. Typically, this means that you can print to a printer at work, see all of the network resources that are normally available, etc.

Incidentally, we say that VPN is a tunneling protocol, in that you tunnel through the Internet and into a remote network. VPN wraps all of your communications into encrypted packets and unwraps them at the "front door" of the network that you are accessing.

B.11 How Do I Access Cablecast or Carousel From Home?

This is the most common sales and support question that we get at Tightrope Media Systems. Because our products are web based, people assume that they will be able to access them from home. This assumption is correct, provided the network is configured to let it happen!

There are three ways to gain access to your Cablecast or Carousel system from the Internet, each with their own security and accessibility tradeoffs.

B.11.1 Option 1: Hang It Out On the Internet

If you give your computer a public IP address, people will be able to access your Tightrope server. Using this method, you will not only be able to update your system, but others will be able to access the public web interface of Cablecast and Carousel, giving them the ability to view messages and see your Cablecast system's schedule.

The down side is that your server is hanging out on the Internet, ready to be infected with the latest worm or controlled by the next bored teenager.

Because of the insecurity of this option and the relative ease of the alternatives, security professionals suggest that you seek alternatives to exposing your servers directly to the Internet.

B.11.2 Option 2: Use Port Forwarding

The most popular method of putting your Tightrope server on the Internet is to use port forwarding. Your server sits inside your network on a private IP address and traffic that comes in on a specific port is forwarded to your server.

The upside to this configuration is that any type of access that you need on your Tightrope server can be accommodated, including anonymous access to the system's public web interfaces.

On an existing network, this configuration might be difficult to accomplish because of security concerns and existing configurations. Specifically, if your network administrator forwards a port to your Tightrope server, there is still no guarantee that the server will not become infected or compromised. Once it is compromised, the rest of the computers on your network are in jeopardy.

The most effective way past this obstacle is to place your Tightrope server inside your network's DMZ, which actually does stand for Demilitarized Zone. A DMZ is a tiny network with a firewall on either side. One firewall separates the DMZ from the Internet and the other separates the DMZ from the internal network. That way, if your Tightrope server is infected, only the computers within the DMZ are at risk.

The second obstacle is that your network may be using the port that you need. There are three ways around this problem:

1. Use a new public IP address for your Tightrope servers. This will eliminate the port conflict because your server will be the only computer using that port on that address.

2. Use a firewall that supports named forwarding and add a DNS entry for your Tightrope system's web server. That way, if someone is looking for "carousel.mydomain.org" the firewall/NAT server will forward them to the Carousel machine instead of your main web server.
3. Use a different port on your Tightrope server by changing it in Internet Information Server. Instead of using port "80" for web access, you could use port "8080". See section [B.12.2](#) on page [131](#) for information about how to do this.

B.11.3 Option 3: Use VPN

This is a limiting option because all of the public web features of Tightrope's system will be unusable, given that there is no anonymous access from the Internet to your Tightrope server. It is secure, however, because you are simply using the same VPN access that you would use for your regular network access. If your organization already uses VPN, you don't even need to involve your IT department.

B.11.4 The "Forget the IT Department" Option

Instead of fighting your network administrators, you may be able to buy an inexpensive connection of your own.

DSL or cable modem connection might cost you only 30 to 80 dollars per month and provide a method to access your computer from outside your network.

Using this method, you would access your system from your desk at work by going out on the Internet through your regular network and back into your building through the new connection that you purchased for your Tightrope System. You access your Tightrope servers as you would any other computer on the Internet.

The biggest limitation is that you cannot connect any machine within your building's network to any Tightrope server. For Carousel machines, this is not a significant limitation unless you are uploading large video files. For Cablecast installations with video servers, this is a problem because you will not be able to transfer video files into the server using Windows Networking.

Another consideration has to do with the type of Internet connection that you purchase. It is very common for cable companies to block certain ports on your network. Also, obtaining a static IP address is often difficult or expensive to accomplish.

For ways around these limitations, see the next section. . .

B.12 Avoiding The Tyranny of Cable Modem Providers

If you are on your own or find it impossible to put your Tightrope system on the Internet through your IT department, getting your own connection might be the best option.

When an organization wants to put out a web presence, they will purchase a connection that is designed for the task. Traditionally this has meant a T1 connection, which is very expensive.

A great alternative to a T1 is a DSL or cable modem connection, which can be had for less than 40 dollars per month, in some cases. Unfortunately, these connections are designed for consumers and as such lack static IP addresses. In some cases the Internet Service Provider (ISP) will even block incoming access to common ports, like TCP port 80, in an attempt to stop you from hosting web sites with your connection.

Sometimes your provider will have a business version of their services which will provide you with everything that you need to host a web site. If your ISP does not offer business class service or it is cost prohibitive, you have one last option.



Many Tightrope customers have a working relationship with their cable provider. The policies in place might be more applicable to high traffic sites than it is to your situation and you may be in a position to ask for some flexibility.

BEFORE YOU CONTINUE READING THIS SECTION:

Call your cable provider and ask them if the following steps are acceptable to them. You do not want to circumvent their policies only to suffer their wrath when you find they've canceled your account and you are facing possible legal action. Get any negotiated exceptions to their policies *in writing!*

Tightrope Media Systems does not condone nor advocate wanton violation of your ISP's acceptable use policies!

B.12.1 Dynamic DNS

The first order of business is figuring out how to find your Tightrope server from outside your network. To do this, you use a technology called Dynamic Domain Name Service (DDNS). DDNS providers offer the same services as DNS except that they are able to track your dynamic IP address using special software that you install on your Tightrope server. This service is generally very inexpensive.

The down side to this service is that if your IP address changes, your site may be down for a short period of time. This is because the software might not discover the switch right away.

To find a dynamic DNS service provider, simply 'Google' the term *dynamic DNS*. You'll find many from which to choose. :)

B.12.2 Change Your Port Number

Your ISP may choose to block incoming data packets on specific ports. You can get around this by changing the port on which your Tightrope system's web server is listening.

1. Right-click on **"My Computer"** on your Tightrope server's desktop.
2. Select **"Manage"**
3. Expand the **"Services and Applications"** Branch. Expand the **"Internet Information Services"** and **"Web Sites"** branches.
4. Right-click on **"Default Web Site"** and click properties. (figure B.4 on the next page)
5. Under the **"Web Site"** tab, find the **"TCP Port"** field. (figure B.5 on page 133)
6. Enter a port that is higher than 50,000. These are called *unregistered* or *user ports* and are unlikely to conflict with another application on your computer.
7. When you access your Tightrope server, you will have to designate the port number by entering a ":" then the number after the address. Example: "carousel.mydomain.org:8080" or "192.168.1.3:8080".

B.13 Time Synchronization, UDP and NAT

We spent so much time talking about NAT, UDP and TCP in this guide because there are situations where you will want to use UDP through your router and will have problems doing so. The most common situation is where you want to synchronize a Tightrope server's clock to "Internet Time" using a service called Network Time Protocol (NTP).

NTP uses UDP port 123. Some organizations will have an NTP server running within their network and configuring a Tightrope server to use it is trivial. (section 6.5.4 on page 58)

If there is no NTP service available, you will have to configure your router to forward all NTP traffic to your Tightrope server, or enable UDP-NAT Traversal, which is

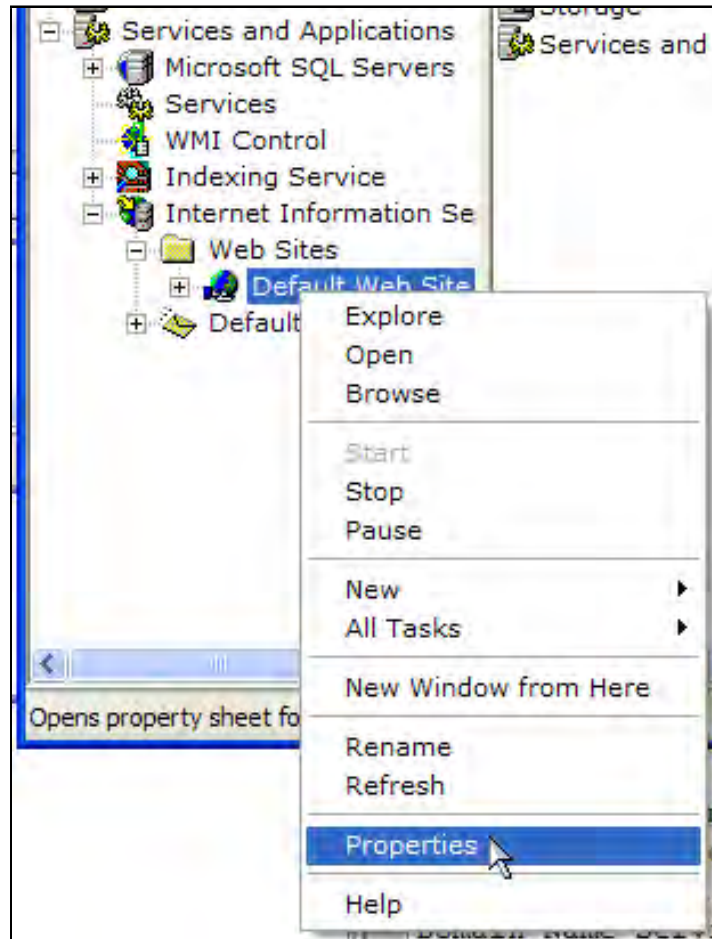


Figure B.4: Navigating to Internet Information Services

able to guess at the destination of incoming UDP packets based on recent outgoing traffic.

On inexpensive consumer cable modem routers, simple versions of UDP-NAT Traversal are often enabled by default. More expensive router/firewall/NAT combinations require some configuration.

B.14 Summary

In this paper we were able to cover quite a bit of ground. You should now have a basic grasp on the following concepts:

- IP addresses, subnet masks, routers and DNS
- DHCP and Dynamic IP addresses
- The difference between TCP and UDP and why it matters
- A basic understanding of network ports
- Understand private and public IP addresses
- Network Address Translation

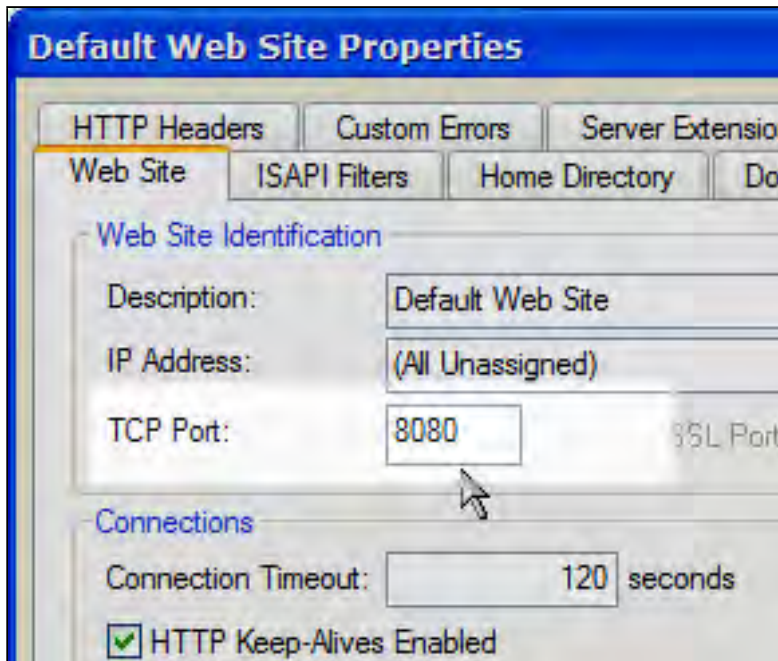


Figure B.5: Changing your port number.

- Firewalls and port forwarding
- Virtual Private Networking
- The various options for getting your system on the Internet